

FR

FR

FR



COMMISSION EUROPÉENNE

Bruxelles, le 2.2.2011
COM(2011) 32 final

2011/0023 (COD)

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

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

{SEC(2011) 132 final}
{SEC(2011) 133 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Motivation et objectifs de la proposition

Durant la dernière décennie, l'Union européenne (UE) et d'autres régions du monde ont connu une hausse de la grande criminalité et de la criminalité organisée, et notamment de la traite des êtres humains¹ et du trafic de drogue². Selon le recueil de statistiques relatives à la criminalité et à la justice pénale, quelque 14 000 infractions pénales par tranche de 100 000 habitants ont été dénombrées en 2007 dans les États membres de l'UE (à l'exception de l'Italie et du Portugal pour lesquels des données n'ont pas été communiquées), ce nombre allant de 14 465 en Suède à 958 à Chypre. L'évaluation de la menace que représente la criminalité organisée dans l'UE, effectuée en 2009 par Europol (OCTA 2009), révèle que la plupart des infractions relevant de la criminalité organisée impliquent des déplacements internationaux, qui ont généralement pour but de faire entrer clandestinement des personnes, des stupéfiants ou d'autres marchandises illicites dans l'Union.

Parallèlement, les terroristes et les organisations terroristes sont établis tant dans l'UE qu'en dehors de celle-ci. Les attentats perpétrés aux États-Unis en 2001, le projet d'attentat déjoué en août 2006 qui visait à faire exploser plusieurs avions en vol entre le Royaume-Uni et les États-Unis et la tentative d'attentat à bord du vol Amsterdam-Detroit en décembre 2009 ont prouvé que les terroristes sont capables de monter des attaques ciblant des vols internationaux dans tous les pays. S'il constate une régression du terrorisme dans l'UE en 2009, le rapport 2010 d'Europol sur la situation et les tendances du terrorisme en Europe indique que cette menace demeure réelle et sérieuse. Puisque la plupart des activités terroristes sont de nature transnationale et impliquent des déplacements internationaux³, entre autres vers des camps d'entraînement situés en dehors de l'Union, une coopération accrue entre les services répressifs est indispensable.

Les formes graves de criminalité (ci-après les «infractions graves») et les infractions terroristes causent des préjudices considérables aux victimes, ainsi que des dommages économiques de grande ampleur, tout en sapant le sentiment de sécurité sans lequel les citoyens ne peuvent jouir effectivement de leur liberté et de leurs droits individuels.

D'après les estimations d'une étude publiée en 2009⁴ pour l'Organisation internationale du travail, le coût de la coercition dû au sous-paiement de la main-d'œuvre résultant de la traite des êtres humains s'élevait à 2 508 368 218 USD en 2007 dans les économies industrialisées, tandis que le coût total au niveau mondial était de 19 598 020 343 USD.

Le rapport 2010 sur l'état du phénomène de la drogue en Europe, publié par l'Observatoire européen des drogues et des toxicomanies, souligne la nature mondiale de ce phénomène ainsi que les dommages croissants et graves qu'il cause. Parce qu'il sape le développement social et

¹ Évaluation de la menace que représente la criminalité organisée dans l'UE, effectuée en 2009 par Europol.

² Eurostat 36/2009.

³ Rapport 2010 d'Europol sur la situation et les tendances du terrorisme en Europe.

⁴ Measuring the costs of coercion to workers in forced labour - Vinogradova, De Cock, Belser (disponible seulement en anglais).

alimente la corruption et la criminalité organisée, il représente une véritable menace pour l'Union européenne. Quelque 1 000 décès liés à la consommation et au trafic de cocaïne sont recensés chaque année dans l'UE. Des estimations prudentes indiquent que 1,35 million de personnes consomment des opiacés en Europe. Quant aux incidences économiques et sociales de la drogue, 22 États membres de l'UE ont indiqué en 2008 que les dépenses liées aux drogues illicites se montaient au total à 4,2 milliards d'EUR.

Une autre étude, réalisée par le ministère britannique de l'intérieur⁵, a mesuré les coûts supportés pour prévenir la criminalité, tels que les dépenses défensives, les coûts des répercussions de la criminalité, tels que les impacts physique et émotionnel sur la victime et la valeur du patrimoine volé, ainsi que les dépenses engagées pour apporter une réponse à la criminalité, dont les coûts supportés par le système de justice pénale. Ces coûts ont été évalués à 36 166 000 000 de GBP en 2003.

Parallèlement, quatre Européens sur cinq réclament une action plus ferme au niveau de l'UE contre la criminalité organisée et le terrorisme⁶.

Pour contrer la menace que représentent la grande criminalité et le terrorisme et par suite de la suppression des contrôles aux frontières intérieures en application de la convention de Schengen, l'UE a adopté des mesures organisant la collecte de données à caractère personnel et l'échange de celles-ci entre les services répressifs et d'autres autorités. Si elles s'avèrent utiles, ces mesures sont surtout axées sur l'information relative aux personnes déjà suspectées, c'est-à-dire les individus «connus» des services de police. Le système d'information Schengen (SIS)⁷, le système d'information Schengen de deuxième génération (SIS II)⁸, le système d'information sur les visas⁹ et le futur système d'entrée/sortie en sont des exemples.

Dans sa «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice»¹⁰, la Commission a analysé ces mesures et souligné la nécessité d'accroître la coopération entre les services répressifs à l'égard des passagers de vols internationaux au départ et en provenance des États membres, et notamment d'utiliser plus systématiquement les données des dossiers de ces passagers (*Passenger Name Record* – données PNR) à des fins répressives. Le «programme de Stockholm - Une Europe ouverte et sûre qui sert et protège les citoyens»¹¹ demande également à la Commission de présenter une proposition concernant l'utilisation des données PNR aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière.

Les données PNR sont des informations non vérifiées communiquées par les passagers, qui sont recueillies et conservées dans le système de réservation et de contrôle des départs des transporteurs aériens pour leur propre usage commercial. Le dossier ainsi constitué comporte divers éléments, tels que les dates du voyage, l'itinéraire, les informations figurant sur le

⁵ The economic and social costs of crime against individuals and households 2003/04.

⁶ Eurobaromètre standard 71, p. 149 de l'annexe.

⁷ Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO L 239 du 22.9.2000, p. 19.

⁸ Règlement (CE) n° 1987/2006, décision 2007/533/JAI, règlement (CE) n° 1986/2006.

⁹ Décision 2004/512/CE du Conseil, règlement (CE) n° 767/2008, décision 2008/633/JAI du Conseil. Voir aussi la déclaration sur la lutte contre le terrorisme, Conseil européen, 25.3.2004.

¹⁰ COM(2010) 385.

¹¹ Document n° 17024/09 du Conseil du 2.12.2009.

billet, les coordonnées du passager, le nom de l'agent de voyages auprès duquel le vol a été réservé, le moyen de paiement utilisé, le numéro du siège et des données relatives aux bagages.

Les services répressifs peuvent utiliser les données PNR de plusieurs manières:

en mode réactif: dans le cadre d'enquêtes, de poursuites, du démantèlement de réseaux après qu'une infraction a été commise. Pour permettre aux services répressifs de remonter suffisamment loin dans le temps, il est nécessaire de prévoir une durée de conservation des données par ces services qui soit proportionnée;

en temps réel: avant l'arrivée ou le départ de passagers dans le but de prévenir une infraction ou de surveiller ou d'arrêter des personnes avant qu'une infraction soit commise ou parce qu'une infraction a été commise ou est en train de l'être. Dans de tels cas, les données PNR sont nécessaires pour pouvoir établir des comparaisons, d'une part, avec des critères d'évaluation préétablis afin d'identifier les suspects jusqu'alors «inconnus» et, d'autre part, avec diverses bases de données relatives aux personnes et objets recherchés;

en mode réactif: pour l'analyse et la définition de critères d'évaluation qui peuvent ensuite être appliqués afin d'évaluer le risque que représentent les passagers avant leur arrivée et avant leur départ. Pour effectuer cette analyse de la pertinence aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière, il est nécessaire de prévoir une durée de conservation des données par les services répressifs qui soit proportionnée.

Une collecte, une utilisation et une conservation plus systématiques des données PNR relatives aux vols internationaux, sous réserve de garanties strictes pour leur protection, permettraient d'intensifier la prévention et la détection des infractions terroristes et des infractions graves, ainsi que les enquêtes et les poursuites en la matière, outre le fait qu'elles sont nécessaires, comme expliqué ci-dessous, pour contrer les menaces qui pèsent sur la sécurité et pour réduire les dommages causés.

L'utilisation des données PNR n'est toutefois pas réglementée au niveau de l'UE. Si quelques États membres ont déjà mis en place un système PNR, la plupart utilisent les données PNR pour la prévention et la détection des infractions terroristes et des infractions graves, ainsi que pour les enquêtes et les poursuites en la matière, mais pas systématiquement ou en vertu de compétences générales dévolues à la police ou à d'autres autorités. Au sein de l'Union, le Royaume-Uni dispose déjà d'un système PNR, tandis que la France, le Danemark, la Belgique, la Suède et les Pays-Bas ont adopté la législation correspondante ou utilisent les données PNR à titre expérimental. Plusieurs autres États membres étudient la possibilité de mettre en place un système PNR. Ces mesures nationales se distinguent à plusieurs égards, notamment sous l'angle de la finalité du système, de la durée de conservation des données, de la structure du système, de la portée géographique et des modes de transport concernés. Il est également très vraisemblable que lorsque le cadre réglementaire complet relatif à l'utilisation des données PNR sera adopté dans ces États membres, des règles divergentes s'appliqueront en matière de protection des données et de garantie de la sécurité des transferts de données. Par conséquent, jusqu'à 27 systèmes sensiblement différents pourraient voir le jour. Cette situation se traduirait par des degrés inégaux de protection des données à caractère personnel dans l'Union, des lacunes en matière de sécurité, des hausses de coûts et une insécurité juridique tant pour les transporteurs aériens que pour les passagers.

L'objectif de la proposition est donc d'harmoniser les dispositions des États membres faisant obligation aux transporteurs aériens assurant des vols entre un pays tiers et le territoire d'au moins un État membre de transmettre aux autorités compétentes les données PNR aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière. La présente proposition n'exige pas des transporteurs aériens qu'ils recueillent des données supplémentaires auprès des passagers ou qu'ils conservent certaines données; elle ne requiert pas non plus que les passagers communiquent d'autres données que celles qui sont déjà transmises aux transporteurs aériens.

Les obligations légales susmentionnées doivent être imposées aux transporteurs aériens pour les raisons exposées ci-après.

Premièrement, les données PNR permettent aux services répressifs d'identifier des personnes auparavant «inconnues» d'eux, c'est-à-dire jusque-là non soupçonnées de participation à une infraction grave ou à un acte de terrorisme, mais dont l'analyse des données indique qu'elles peuvent être impliquées dans une infraction de cette nature et qu'elles devraient donc être soumises à un examen approfondi par les autorités compétentes. L'identification de ces personnes aide les services répressifs à prévenir et à détecter les infractions graves, y compris les actes de terrorisme. À cet effet, lesdits services doivent utiliser les données PNR, d'une part, en temps réel, pour les analyser au regard de critères d'évaluation préétablis, qui indiquent les personnes jusque-là «inconnues» devant faire l'objet d'un examen approfondi et, d'autre part, d'une manière proactive aux fins de l'analyse et de la définition de critères d'évaluation.

Par exemple, une analyse de données PNR peut donner des indications sur les itinéraires les plus empruntés pour la traite des êtres humains ou le trafic de drogue, autant d'éléments qui peuvent être intégrés dans les critères d'évaluation. La confrontation en temps réel des données PNR à ces critères permet de prévenir ou de détecter des infractions. Un État membre a fourni un exemple concret concernant une affaire dans laquelle l'analyse des données PNR a permis de démasquer un groupe de passeurs qui empruntaient toujours le même itinéraire. Produisant des documents falsifiés pour procéder aux formalités d'enregistrement sur un vol intérieur, ils utilisaient des documents authentiques pour procéder, simultanément, aux formalités d'enregistrement sur un autre vol à destination d'un pays tiers. Une fois dans la salle d'attente de l'aéroport, ils embarquaient sur le vol intérieur. Sans les données PNR, il aurait été impossible de démanteler ce réseau de traite des êtres humains.

Une utilisation à la fois proactive et en temps réel des données PNR permet donc aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent, par rapport à ce que permet le traitement d'autres catégories de données à caractère personnel. Comme expliqué ci-dessous, le traitement de données à caractère personnel accessibles aux services répressifs dans le cadre d'instruments de l'UE actuels et futurs, tels que la directive relative aux informations préalables sur les passagers¹², le système d'information Schengen (SIS) et le système d'information Schengen de deuxième génération (SIS II), ne donne pas aux services répressifs la possibilité d'identifier des suspects «inconnus» comme le permet l'analyse de données PNR.

Deuxièmement, après la commission d'une infraction, les données PNR aident les services répressifs à prévenir et à détecter d'autres infractions graves, dont des actes de terrorisme, et à

¹² Directive 2004/82/CE du 29 avril 2004.

enquêter sur celles-ci et à poursuivre leurs auteurs. À cet effet, les services répressifs doivent utiliser les données PNR en temps réel, pour les confronter à diverses bases de données de personnes «connues» et d'objets recherchés. Ils doivent également en faire un usage réactif, pour rassembler des preuves et, au besoin, trouver d'éventuels complices et démanteler des réseaux criminels.

Par exemple, les informations liées à une carte de crédit qui font partie des données PNR peuvent permettre aux services répressifs d'identifier une personne et d'établir l'existence de liens entre celle-ci et un délinquant ou une organisation criminelle qu'ils connaissent. Un État membre a cité l'exemple d'un vaste réseau de traite des êtres humains et de trafic de drogue entre un État membre et des pays tiers. Des cartels importaient de la drogue dans plusieurs régions d'Europe. Ils faisaient appel à des personnes, elles-mêmes victimes de la traite, qui avalaient la drogue. Les données PNR ont permis leur identification car ils avaient acheté leurs billets avec des cartes de crédit volées. Des arrestations ont ensuite eu lieu dans l'État membre concerné. Un critère d'évaluation a été défini sur cette base, qui a à son tour permis plusieurs arrestations dans d'autres États membres et dans des pays tiers.

Enfin, **l'examen des données PNR avant l'arrivée** des passagers permet aux services répressifs de procéder à une évaluation et de ne contrôler étroitement que les personnes les plus susceptibles de représenter une menace pour la sécurité, sur la base de critères d'évaluation objectifs et de l'expérience acquise. Cela facilite le déplacement de tous les autres passagers et réduit le risque qu'ils soient soumis, à leur entrée dans l'UE, à un contrôle fondé sur des critères illégaux, tels que la nationalité ou la couleur de peau, que les services répressifs, et notamment les douaniers et gardes-frontières, peuvent à tort associer à un risque pour la sécurité.

Les mesures proposées impliquent la collecte et le traitement de données PNR par les services répressifs et ont donc une incidence sur le droit au respect de la vie privée et le droit à la protection des données. Afin d'assurer le respect du principe de proportionnalité, la proposition a par conséquent une portée soigneusement limitée, comme expliqué ci-après, et contient des garanties strictes en matière de protection des données.

La nécessité de restreindre l'utilisation des données PNR et de la soumettre à ces garanties strictes est corroborée par certains éléments factuels, ainsi qu'il ressort de l'analyse d'impact accompagnant la présente proposition. En l'absence de dispositions harmonisées régissant la collecte des données PNR et leur traitement au niveau de l'UE, il n'existe pas de statistiques précises indiquant dans quelle mesure ces données contribuent à la prévention et à la détection de la grande criminalité et du terrorisme, ainsi qu'aux enquêtes et aux poursuites en la matière. Cependant, l'utilisation indispensable des données PNR est confirmée par des informations provenant de pays tiers et d'États membres qui les utilisent déjà des fins répressives.

L'expérience acquise dans ces pays montre que l'utilisation de données PNR a fait sensiblement progresser la lutte contre la drogue, la traite des êtres humains et le terrorisme notamment et permet de mieux comprendre la composition et le fonctionnement des réseaux terroristes et des autres réseaux criminels. En ce qui concerne la drogue, des États membres ont indiqué que la majorité des saisies intervenaient grâce à une utilisation en temps réel et proactive des données PNR. La Belgique a signalé que 95 % de l'ensemble des saisies de drogue effectuées en 2009 sur son territoire résultaient exclusivement ou essentiellement du traitement de données PNR. La Suède a déclaré que 65 à 75 % de l'ensemble des saisies de drogue effectuées en 2009 sur son territoire résultaient exclusivement ou essentiellement du

traitement de données PNR, soit 278,9 kilos de cocaïne, plus de l'héroïne et d'autres drogues. Le Royaume-Uni a indiqué qu'au cours d'un semestre en 2010, 212 kilos de cocaïne et 20 kilos d'héroïne avaient été saisis exclusivement ou essentiellement grâce au traitement de données PNR.

- **Contexte général**

Le 6 novembre 2007, la Commission a adopté une proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* - PNR) à des fins répressives¹³ (ci-après la «proposition de 2007»). Cette proposition a fait l'objet de discussions approfondies au sein des groupes de travail du Conseil, et le Conseil «Justice et affaires intérieures» a avalisé les progrès réalisés, en janvier, juillet et novembre 2008. Les discussions que les groupes de travail ont consacrées à la proposition ont permis de dégager un consensus sur la plupart de ses dispositions¹⁴.

Lors de l'entrée en vigueur du traité sur le fonctionnement de l'Union européenne (TFUE) le 1^{er} décembre 2009, la proposition de la Commission, non encore adoptée par le Conseil, est devenue obsolète. La présente proposition remplace celle de 2007 et repose sur les dispositions du TFUE. Elle tient compte des recommandations que le Parlement européen a formulées dans sa résolution de novembre 2008¹⁵ et elle traduit le dernier état d'avancement des discussions au sein des groupes de travail du Conseil en 2009. Elle prend également en considération les avis du contrôleur européen de la protection des données¹⁶, du groupe «Article 29» sur la protection des données¹⁷ et de l'Agence des droits fondamentaux¹⁸.

- **Dispositions en vigueur dans le domaine de la proposition**

Les données PNR se distinguent des informations préalables sur les passagers (*Advance Passenger Information* – API), et il y a lieu de ne pas les confondre. Les données API sont les informations biographiques extraites de la partie d'un passeport lisible par machine et contenant le nom, le lieu de naissance et la nationalité du titulaire, le numéro du passeport et sa date d'expiration. Elles se distinguent donc des données PNR et sont de portée plus limitée.

Dans l'Union, l'utilisation des données API est réglementée par la directive API¹⁹. Celle-ci prévoit que les données API doivent être transmises aux autorités chargées d'effectuer les contrôles aux frontières, sur demande de chaque État membre, pour les vols atterrissant sur le territoire de l'UE, aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration illégale. Si leur utilisation à des fins répressives est autorisée par la directive, elle ne l'est qu'à condition que des critères spécifiques soient remplis. Ainsi, bien que les données API soient parfois utilisées par les services répressifs pour identifier des suspects ou des personnes recherchées, elles servent essentiellement d'outil de vérification des identités et de gestion des frontières. En outre, les données API ne permettent pas aux services répressifs de procéder à une évaluation du risque que représentent les passagers et ne facilitent donc pas le dépistage de criminels ou de terroristes jusque-là «inconnus».

¹³ COM(2007) 654.

¹⁴ Document 5618/2/09 REV 2 du Conseil du 29.6.2009.

¹⁵ P6_TA (2008)0561.

¹⁶ JO C 110 du 1.5.2008.

¹⁷ Avis n° 145 du 5.12.2007.

¹⁸ http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf (en anglais uniquement).

¹⁹ Directive 2004/82/CE du 29 avril 2004.

Le **système d'information Schengen (SIS)** a pour objet de maintenir la sécurité publique, y compris la sécurité nationale, à l'intérieur de l'espace Schengen. Le SIS est un système d'information centralisé doté d'une composante nationale dans chaque État participant et d'une fonction de support technique située en France. Les États membres peuvent signaler les personnes recherchées pour l'arrestation aux fins d'extradition; les étrangers non admissibles; les personnes disparues; les témoins ou personnes citées à comparaître devant les autorités judiciaires; les personnes et véhicules soumis à des vérifications complémentaires; les armes à feu, documents et véhicules perdus ou volés; et les billets de banque suspects.

Le **système d'information sur les visas (VIS)** a pour but de répondre à deux préoccupations: il vise à soutenir la mise en œuvre d'une politique commune des visas en simplifiant l'examen des demandes de visa et les contrôles aux frontières extérieures tout en contribuant à la prévention des menaces à la sécurité intérieure des États membres. Il s'agit d'un système d'information centralisé qui se compose d'un élément national par État participant et d'une fonction d'appui technique établie en France. Le VIS aura recours à un système de correspondance biométrique destiné à garantir la fiabilité des comparaisons d'empreintes digitales, lequel sera également déployé aux frontières extérieures de l'UE pour vérifier l'identité des titulaires de visas. Il comprendra des données concernant les demandes de visas, des photographies, des empreintes digitales, des décisions connexes des services de visas et des liens entre demandes connexes.

Par conséquent, à l'instar des API, le SIS et le VIS servent essentiellement d'outils de vérification des identités et de gestion des frontières et ne sont utiles que lorsque l'identité du suspect est connue. Ces instruments ne présentent donc pas d'intérêt pour l'évaluation des personnes ni pour le dépistage des délinquants ou terroristes «inconnus».

Des accords en matière de transfert de données PNR dans le cadre de la lutte contre la grande criminalité transnationale et le terrorisme, limités aux transports aériens, ont été signés entre l'UE et les États-Unis, le Canada et l'Australie. Ils font obligation aux transporteurs aériens qui recueillent des données PNR pour leur propre usage commercial de les transmettre aux autorités compétentes américaines, canadiennes et australiennes. Ces trois accords devraient être renégociés en 2011. D'autres pays, notamment la Corée du Sud et le Japon, ont également demandé à pouvoir négocier des accords de ce type. La Commission a décrit les principaux volets d'une politique de l'UE sur cette question dans sa communication du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers²⁰. La présente proposition s'accorde parfaitement avec la politique présentée dans cette communication.

• **Cohérence avec les autres politiques et objectifs de l'Union**

Le système d'information Schengen (SIS)²¹, le système d'information Schengen de deuxième génération (SIS II)²², le système d'information sur les visas²³ et les futurs système

²⁰ COM(2010) 492.

²¹ Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO L 239 du 22.9.2000, p. 19.

²² Règlement (CE) n° 1987/2006, décision 2007/533/JAI, règlement (CE) n° 1986/2006.

²³ Décision 2004/512/CE du Conseil, règlement (CE) n° 767/2008, décision 2008/633/JAI du Conseil. Voir aussi la déclaration sur la lutte contre le terrorisme, Conseil européen, 25.3.2004.

d'entrée/sortie et système d'enregistrement des voyageurs sont des mesures prises par l'UE pour régir directement des processus qui se déroulent physiquement aux frontières.

Bien que les données PNR soient des données relatives aux passagers liées à leurs déplacements, elles sont essentiellement utilisées en tant qu'outil de renseignement en matière criminelle, plutôt que comme instrument de contrôle aux frontières. On y a recours avant le franchissement de la frontière et non lors de celui-ci. Leur utilisation s'inscrit principalement dans le cadre de la lutte contre le terrorisme et la grande criminalité, plutôt que dans celui de la lutte contre l'immigration illégale et de la facilitation des contrôles aux frontières.

La proposition ne modifie ni n'affecte les règles de l'UE actuelles définissant les modalités des contrôles aux frontières, pas plus que les règles de l'UE applicables aux entrées sur le territoire de l'Union et aux sorties de celui-ci. Elle coexisterait plutôt avec ces règles, qui resteraient intactes.

- **Incidence sur les droits fondamentaux**

La proposition s'inscrit dans le droit fil de l'objectif global visant à créer un espace européen de liberté, de sécurité et de justice. Vu la nature des dispositions envisagées, la présente proposition a fait l'objet d'un examen approfondi, comme l'indique l'analyse d'impact qui l'accompagne, pour garantir que ses dispositions sont compatibles avec les droits fondamentaux, et notamment le droit à la protection des données à caractère personnel consacré par l'article 8 de la charte des droits fondamentaux de l'UE. Elle est également conforme à l'article 16 du TFUE, qui confère à toute personne le droit à la protection des données à caractère personnel la concernant.

La proposition est compatible avec les principes de la protection des données, et ses dispositions sont conformes à la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale²⁴ (ci-après la «décision-cadre 2008/977/JAI»). Il s'agit notamment de conférer aux citoyens les droits d'accès, de rectification, d'effacement et de verrouillage, ainsi que le droit à réparation et le droit à un recours juridictionnel. En outre, pour satisfaire au principe de proportionnalité, elle introduit dans certains domaines des règles de protection des données plus strictes que celles de la décision-cadre 2008/977/JAI.

En particulier, le champ d'application de la proposition est strictement limité et n'autorise les services répressifs à utiliser les données PNR que pour lutter contre des certaines infractions graves, dont une liste exhaustive est dressée et qui doivent en outre être passibles d'une peine d'emprisonnement d'au moins trois ans dans l'État membre concerné. Par ailleurs, pour veiller à ce que le traitement des données de personnes innocentes et non soupçonnées reste aussi limité que possible, certains aspects du champ d'application de la proposition ayant trait à la définition et à l'application de critères d'évaluation ont en outre été limités aux infractions graves qui sont aussi transnationales par nature, c'est-à-dire intrinsèquement liées à des déplacements, et donc au type de données traitées. La proposition autorise la conservation des données PNR pendant une période n'excédant pas cinq ans, au terme de laquelle les données doivent être effacées. De plus, les données doivent être rendues anonymes après un bref délai de 30 jours car, au terme de celui-ci, l'utilisation proactive des données PNR est permise pour autant que celles-ci aient été anonymisées. La collecte et l'utilisation de données sensibles révélant, directement ou indirectement, la race ou l'origine ethnique d'une personne, ses

²⁴ JO L 350 du 30.12.2008, p. 60.

convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle sont interdites. En outre, la proposition prévoit que toute décision d'un État membre qui produit des effets juridiques préjudiciables à une personne ou l'affecte gravement ne doit pas être prise sur la seule base du traitement automatisé des données PNR la concernant. Par ailleurs, une telle décision ne peut en aucun cas reposer sur la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle. De plus, les transporteurs doivent transmettre les données PNR en recourant exclusivement à la méthode dite «push», ce qui signifie que les États membres n'auront pas directement accès aux systèmes informatiques des transporteurs. Les États membres ne seront autorisés à transmettre des données PNR à des pays tiers que dans des situations très limitées et qu'au cas par cas. 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 (autorité chargée de la protection des données) ait la responsabilité de surveiller les modalités de traitement des données PNR et joue un rôle consultatif à cet égard. Ils doivent également instituer une seule unité désignée (unité de renseignements passagers) pour assurer le traitement et la protection des données. Tout traitement de données PNR doit être journalisé ou faire l'objet d'une trace documentaire conservée par cette unité de renseignements passagers à des fins de vérification de la licéité du traitement, d'autocontrôle et de garantie de l'intégrité des données et de la sécurité du traitement des données. Les États membres doivent également veiller à ce que les passagers reçoivent une information claire et précise sur la collecte des données PNR et sur leurs droits.

Par conséquent, outre qu'elle observe les règles et principes actuels en matière de protection des données, la proposition contient un certain nombre de garanties permettant de respecter pleinement le principe de proportionnalité et d'assurer un degré élevé de protection des droits fondamentaux.

2. CONSULTATION DES PARTIES INTERESSEES ET ANALYSE D'IMPACT

• Consultation des parties intéressées

Méthodes de consultation utilisées, principaux secteurs ciblés et profil général des répondants

Lors de l'élaboration de la proposition de 2007, la Commission a consulté toutes les parties intéressées par l'intermédiaire d'un questionnaire envoyé en décembre 2006. Ce dernier a été adressé à tous les États membres, à leurs autorités de protection des données, au contrôleur européen de la protection des données, à l'association des compagnies européennes de navigation aérienne (Association of European Airlines - AEA), à l'association des transporteurs aériens des États-Unis (Air Transport Association of America - ATA), à l'association internationale des charters aériens (International Air Carrier Association - IACA), à l'association européenne des compagnies d'aviation des régions d'Europe (European Regions Airline Association - ERA) et à l'association internationale du transport aérien (International Air Transport Association - IATA). Leurs réponses ont été synthétisées dans l'analyse d'impact de 2007 accompagnant la proposition de 2007. Par la suite, la Commission a invité les États membres à une réunion durant laquelle leurs représentants ont pu faire connaître leurs avis.

Une fois la proposition de 2007 adoptée, toutes les parties intéressées ont pris position sur celle-ci. Le Parlement européen a adopté une résolution sur cette proposition le 20 novembre 2008²⁵. Les États membres ont exprimé leur opinion dans le cadre des discussions tenues au sein des groupes de travail du Conseil²⁶. Le contrôleur européen de la protection des données²⁷, le groupe «Article 29» sur la protection des données²⁸ de l'Agence des droits fondamentaux²⁹ ont également publié un avis.

Synthèse des réponses

La principale critique formulée dans la résolution du Parlement européen était que la nécessité des mesures envisagées n'avait pas été suffisamment démontrée. Le Parlement doutait que la proposition remplisse le critère requis pour justifier une atteinte au droit à la protection des données. La résolution exprimait l'inquiétude du Parlement quant au fait que la valeur ajoutée de la proposition au regard d'autres initiatives de protection des frontières n'avait pas été évaluée. En ce qui concerne la protection des données, le Parlement demandait que les finalités soient clairement limitées et qu'on insiste sur le fait que seules certaines autorités devraient avoir accès aux données PNR. Enfin, le Parlement craignait que la méthode proposée d'évaluation automatique des données PNR à l'aide de critères d'évaluation factuels préétablis ne donne lieu à une utilisation très large de ces données; il a en outre souligné que cette évaluation ne devrait jamais conduire à l'établissement de profils sur la base de données sensibles.

Le groupe «Article 29» sur la protection des données a estimé que la proposition était disproportionnée et qu'elle pourrait entraver le droit à la protection des données. Il a mis en question le régime de protection des données car la décision-cadre 2008/977/JAI ne couvre pas l'ensemble des traitements de données nationaux. Il était d'avis que la nécessité d'une telle proposition n'avait pas été démontrée à suffisance, que la durée de conservation (13 ans) était disproportionnée et que seule la méthode «push» de transfert des données devait être utilisée.

Le contrôleur européen de la protection des données doutait que la nécessité et le caractère proportionné de la proposition aient été démontrés, sachant que celle-ci porte sur la collecte de données relatives à des personnes innocentes. Il a déploré le fait que la proposition contribue à l'émergence d'une société de la surveillance, mettant également en cause le régime de protection des données car les traitements de données nationaux ne sont pas régis par la décision-cadre 2008/977/JAI. Le contrôleur européen de la protection des données a plus précisément suggéré de mieux définir les autorités qui auraient accès aux données PNR, ainsi que les conditions applicables aux transferts de données vers des pays tiers.

L'Agence des droits fondamentaux était également d'avis que la nécessité et le caractère proportionné de la proposition n'avaient pas été démontrés et estimait que des garanties supplémentaires devaient figurer dans la proposition pour empêcher l'établissement de profils sur la base de données sensibles.

²⁵ P6_TA (2008)0561.

²⁶ Document n° 17024/09 du Conseil du 2.12.2009.

²⁷ JO C 110 du 1.5.2008.

²⁸ Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives, présentée par la Commission le 6 novembre 2007 (WP 145 du 5.12.2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_fr.pdf.

²⁹ http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf (en anglais uniquement).

Certaines associations de compagnies aériennes, notamment l'IATA et l'AEA, ont également publié un avis sur la proposition, critiquant essentiellement la structure décentralisée évoquée dans la proposition et soulignant que la collecte centralisée des données présenterait des avantages financiers pour les transporteurs. Elles ont également déploré le choix de la méthode «push» et demandé que le choix du mode de transfert soit laissé à l'appréciation des transporteurs.

Le processus de consultation a grandement influencé l'élaboration de la proposition législative. Si plusieurs parties prenantes n'étaient pas convaincues de la nécessité d'avoir recours aux données PNR, toutes s'accordaient sur le fait qu'il était préférable de légiférer au niveau de l'Union plutôt que de voir naître des systèmes PNR nationaux divergents. Les consultations ont également eu pour effet de limiter la finalité de l'utilisation des données à la lutte contre les infractions terroristes et les infractions graves, ainsi que de limiter le champ d'application de la proposition au transport aérien. Un régime fort de protection des données a été privilégié, assorti d'une durée de conservation spécifique et de l'interdiction d'utiliser des données sensibles, telles que celles qui révèlent les origines raciales ou ethniques d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle. La méthode «push» a été préférée, de même que des restrictions sévères aux transferts ultérieurs de données vers des pays tiers.

- **Obtention et utilisation d'expertise**

Il n'a pas été nécessaire de faire appel à des experts externes.

- **Analyse d'impact**

La Commission a effectué l'analyse d'impact prévue dans le programme de travail³⁰.

Quatre options principales ont été examinées dans l'analyse d'impact, chacune comportant deux variables.

Option A: s'abstenir de réglementer la question au niveau de l'UE et maintenir le statu quo.

Option B: établir la structure d'un système de collecte et de traitement des données PNR, selon l'option B.1: collecte et traitement décentralisés des données par les États membres, ou selon l'option B.2: collecte et traitement centralisés des données au niveau de l'UE.

Option C: limiter la finalité des mesures proposées, selon l'option C.1: accès aux données aux seules fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière, ou selon l'option C.2: accès aux données aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière, et aux fins d'autres objectifs stratégiques.

Option D: déterminer les modes de transport qui seront concernés par les mesures proposées, selon l'option D.1: les transporteurs aériens uniquement, ou selon l'option D.2: transporteurs aériens, maritimes et ferroviaires.

³⁰ SEC(2011) 132.

Chaque option a été évaluée au regard des critères suivants: sécurité dans l'UE, protection des données à caractère personnel, coûts pour les pouvoirs publics, coûts pour les transporteurs, concurrence dans le marché intérieur et promotion d'une approche globale.

L'analyse d'impact a permis de conclure que la meilleure option (une combinaison des options B1, C1 et D1) consisterait en une proposition législative applicable aux déplacements aériens, prévoyant une collecte décentralisée des données PNR pour la prévention et la détection des infractions terroristes et autres infractions graves, ainsi que pour les enquêtes et les poursuites en la matière. La sécurité au sein de l'Union s'en trouverait renforcée, l'impact sur la protection des données à caractère personnel étant limité au strict minimum et les coûts maintenus à un niveau acceptable.

3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

• Résumé des mesures proposées

L'objectif de la proposition est d'harmoniser les dispositions des États membres faisant obligation aux transporteurs aériens assurant des vols entre un pays tiers et le territoire d'au moins un État membre de transmettre aux autorités compétentes les données PNR aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites y afférentes. Tous les traitements de données PNR effectués en vertu de la présente proposition seront conformes aux règles de protection des données énoncées dans la décision-cadre 2008/977/JAI.

• Base juridique

Le TFUE, et notamment son article 82, paragraphe 1, point d), et son article 87, paragraphe 2, point a).

• Principe de subsidiarité

Les services répressifs doivent disposer d'outils efficaces de lutte contre le terrorisme et la grande criminalité. Étant donné que la plupart des infractions graves et des actes de terrorisme comportent des déplacements internationaux, les autorités doivent utiliser les données PNR pour préserver la sécurité intérieure de l'Union. En outre, les investigations menées par les autorités compétentes des États membres aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière, dépendent dans une large mesure de la coopération internationale et transfrontière.

Vu la libre circulation des personnes dans l'espace Schengen, il est indispensable que tous les États membres recueillent, traitent et échangent des données PNR pour éviter toute faille dans la sécurité. Par l'action collective et cohérente qu'elle prévoit, la présente proposition contribuera au renforcement de la sécurité de l'Union.

Cette action au niveau de l'Union permettra d'harmoniser les dispositions relatives à la protection des données dans les États membres. Les différents régimes des États membres qui ont déjà mis en place des mécanismes similaires, ou comptent en instaurer à l'avenir, risqueraient de nuire aux transporteurs aériens car ceux-ci pourraient devoir se conformer à diverses exigences nationales potentiellement contradictoires, par exemple en ce qui concerne les types d'information à transmettre et les conditions dans lesquelles ces informations doivent être communiquées aux États membres. Ces divergences peuvent nuire à une coopération

efficace entre les États membres aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière.

Étant donné les objectifs de la présente proposition ne peuvent être réalisés de manière suffisante par les États membres et peuvent donc être mieux réalisés au niveau de l'Union, il est permis de conclure que l'Union est à la fois habilitée à prendre des mesures et mieux placée pour le faire que les États membres agissant isolément. Par conséquent, la proposition est conforme au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne.

- **Principe de proportionnalité**

Une collecte, une analyse et une conservation systématiques des données PNR relatives aux vols à destination de l'UE en provenance de pays tiers, sous réserve de garanties strictes pour leur protection, permettraient d'intensifier la prévention et la détection des infractions terroristes et des infractions graves, ainsi que les enquêtes et les poursuites en la matière et sont nécessaires pour contrer les menaces qui pèsent sur la sécurité.

Le champ d'application de la proposition se limite aux seuls éléments qui requièrent une approche harmonisée au niveau de l'UE, à savoir la définition des modes d'utilisation des données PNR par les États membres, les données qui doivent être recueillies, les buts dans lesquels l'information peut être utilisée, la communication des données entre les unités PNR des États membres, ainsi que les conditions techniques de cette communication.

L'instrument proposé est une directive. Le choix d'un système décentralisé suppose que les États membres peuvent déterminer les modalités de mise en place de leur système PNR et décider eux-mêmes des aspects techniques.

Conformément au principe de proportionnalité tel qu'énoncé à l'article 5 du traité sur l'Union européenne, la présente proposition n'excède pas ce qui est nécessaire et proportionné pour atteindre ses objectifs.

- **Choix des instruments**

Instrument proposé: une directive.

D'autres moyens ne seraient pas appropriés pour le motif suivant:

la mesure proposée visant à harmoniser les législations des États membres, un instrument autre qu'une directive ne serait pas adéquat.

4. INCIDENCE BUDGETAIRE

La proposition n'a pas d'incidence sur le budget de l'UE.

5. INFORMATIONS SUPPLEMENTAIRES

- **Simulation, phase pilote et période de transition**

La proposition fera l'objet d'une période transitoire sous la forme d'un délai de mise en œuvre de deux ans. La collecte provisoire des données PNR sera également prévue, dans la

perspective d'une collecte de ces données pour l'ensemble des vols dans un délai de six ans à compter de l'entrée en vigueur de la directive.

- **Application territoriale**

Les États membres seront destinataires de la directive proposée. L'application de la directive au Royaume-Uni, à l'Irlande et au Danemark sera décidée conformément aux dispositions des protocoles (n° 21 et 22) annexés au traité sur le fonctionnement de l'Union européenne.

- **Clause de réexamen/de révision/de caducité**

La proposition contient une clause prévoyant le réexamen du fonctionnement de la directive quatre ans après sa date de transposition, ainsi qu'un réexamen spécial en vue de l'éventuelle extension de son champ d'application aux données des dossiers de passagers de vols intérieurs au sein de l'Union.

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

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

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,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen³¹,

vu l'avis du Comité des régions³²,

après consultation du contrôleur européen de la protection des données,

statuant conformément à la procédure législative ordinaire,

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 (*Passenger Name Record* - PNR) à des fins répressives³³. Cependant, n'ayant pas encore été adoptée par le Conseil lors de l'entrée en vigueur du traité de Lisbonne le 1^{er} 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»³⁴ demande à la Commission de 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 (ci-après les «infractions graves»), 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 tiers³⁵, la

³¹ JO C du , p. .

³² JO C du , p. .

³³ COM(2007) 654.

³⁴ Document n° 17024/09 du Conseil du 2.12.2009.

³⁵ COM(2010) 492.

Commission a décrit certains éléments essentiels d'une politique de l'Union dans ce domaine.

- (4) La directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers³⁶ régit le transfert préalable aux autorités nationales compétentes, par les transporteurs aériens, de données relatives aux passagers, en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration clandestine.
- (5) Les données PNR sont indispensables pour prévenir et détecter efficacement les infractions terroristes et les infractions graves, ainsi que pour enquêter sur celles-ci et poursuivre leurs auteurs, et donc pour renforcer la sécurité intérieure.
- (6) Les données PNR aident les services répressifs à prévenir et à détecter les infractions graves, dont les actes de terrorisme, à enquêter sur celles-ci et à poursuivre leurs auteurs, ces services pouvant les confronter à diverses bases de données de personnes ou d'objets recherchés, afin de rassembler des preuves et, au besoin, de trouver d'éventuels complices et de démanteler des réseaux criminels.
- (7) Les données PNR permettent aux services répressifs d'identifier des personnes auparavant «inconnues» d'eux, c'est-à-dire jusque-là non soupçonnées de participation à une infraction grave ou à un acte de terrorisme, mais dont l'analyse des données indique qu'elles peuvent être impliquées dans une infraction de cette nature et qu'elles devraient donc être soumises à un examen approfondi par les autorités compétentes. L'utilisation des données PNR permet aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent, par rapport au traitement d'autres catégories de données à caractère personnel. Cependant, pour veiller à ce que le traitement de données de personnes innocentes et non soupçonnées reste aussi limité que possible, les aspects de l'utilisation des données PNR ayant trait à la définition et à l'application de critères d'évaluation devraient en outre être limités aux infractions graves qui sont transnationales par nature, c'est-à-dire qui sont intrinsèquement liées à des déplacements et donc au type de données traitées.
- (8) Le traitement des données à caractère personnel doit être proportionné à l'objectif de sécurité spécifiquement poursuivi par la présente directive.
- (9) L'utilisation des données PNR, ainsi que des données préalables sur les passagers dans certains cas a conféré une valeur ajoutée à l'assistance apportée aux États membres pour la vérification de l'identité des personnes, renforçant ainsi la valeur de leur action répressive.
- (10) Pour prévenir et détecter les infractions terroristes et les infractions graves et pour enquêter sur celles-ci et poursuivre leurs auteurs, il est donc essentiel que tous les États membres adoptent des dispositions imposant des obligations aux transporteurs aériens assurant des vols internationaux à destination ou en provenance du territoire des États membres de l'Union européenne.
- (11) Les transporteurs aériens procèdent déjà à la collecte et au traitement des données PNR de leurs passagers pour leur propre usage commercial. La présente directive ne

³⁶ JO L 261 du 6.8.2004, p. 24.

devrait pas leur imposer l'obligation de recueillir des données supplémentaires auprès des passagers ou de les conserver et ne devrait pas non plus contraindre les passagers à communiquer d'autres données que celles qui sont déjà transmises aux transporteurs aériens.

- (12) La définition des infractions terroristes devrait être reprise des articles 1^{er} à 4 de la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme³⁷. La définition des infractions graves devrait être reprise de l'article 2 de la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres³⁸. Toutefois, les États membres peuvent exclure les infractions mineures pour lesquelles, compte tenu de leurs systèmes respectifs de justice pénale, le traitement de données PNR en vertu de la présente directive ne serait pas conforme au principe de proportionnalité. La définition des infractions transnationales graves devrait être reprise de l'article 2 de la décision-cadre 2002/584/JAI du Conseil et de la convention des Nations unies contre la criminalité transnationale organisée.
- (13) Il convient que les données PNR soient transmises à une seule unité désignée (unité de renseignements passagers) dans l'État membre correspondant, de manière à garantir la transparence et à réduire les coûts supportés par les transporteurs aériens.
- (14) Les listes de données PNR demandées, à transmettre aux unités de renseignements passagers, devraient être établies dans le but de refléter les exigences légitimes des pouvoirs publics visant à prévenir et à détecter les infractions terroristes ou les infractions graves et à enquêter sur celles-ci et à poursuivre leurs auteurs, afin de renforcer ainsi la sécurité intérieure de l'Union et de protéger les droits fondamentaux des citoyens, notamment le droit au respect de leur vie privée et à la protection des données à caractère personnel les concernant. Ces listes ne devraient pas contenir de données à caractère personnel susceptibles de révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat ni de données qui concernent la santé ou la vie sexuelle de l'intéressé. Les données PNR devraient inclure des informations détaillées relatives à la réservation et à l'itinéraire de voyage des passagers, qui permettent aux autorités compétentes d'identifier les passagers représentant une menace pour la sécurité intérieure.
- (15) Actuellement, deux méthodes de transfert des données sont possibles: la méthode «pull» par laquelle les autorités compétentes de l'État qui demandent les données peuvent accéder au système de réservation du transporteur aérien et en extraire («pull») une copie des données requises, et la méthode «push» par laquelle les transporteurs aériens transmettent («push») les données PNR requises à l'autorité qui les demande, ce qui permet aux transporteurs aériens de garder le contrôle sur les types de données transmis. La méthode «push» est réputée offrir un degré plus élevé de protection des données et devrait être obligatoire pour tous les transporteurs aériens.
- (16) La Commission soutient les travaux entrepris dans le cadre de l'initiative multilatérale de l'OACI, qui a abouti à l'élaboration des lignes directrices de l'OACI relatives aux données PNR. Il convient donc que ces lignes directrices servent de base pour

³⁷ JO L 164 du 22.6.2002, p. 3. Décision modifiée par la décision-cadre 2008/919/JAI du Conseil du 28 novembre 2008 (JO L 330 du 9.12.2008, p. 21).

³⁸ JO L 190 du 18.7.2002, p. 1.

l'adoption des formats de données reconnus pour les transferts des données PNR par les transporteurs aériens vers les États membres. Il est donc justifié que ces formats de données reconnus, ainsi que les protocoles correspondants applicables au transfert des données provenant des transporteurs aériens, soient adoptés conformément à la procédure consultative prévue dans le règlement (UE) n° du Parlement européen et du Conseil [.....].

- (17) Les États membres devraient adopter toutes les mesures nécessaires pour permettre aux transporteurs aériens de remplir les obligations qui leur incombent en vertu de la présente directive. Il y a lieu que les États membres prévoient des sanctions dissuasives, efficaces et proportionnées, y compris des sanctions financières, à infliger aux transporteurs aériens qui ne se conforment pas à leurs obligations en matière de transfert de données PNR. En cas d'infractions graves répétées susceptibles de nuire aux objectifs fondamentaux de la présente directive, ces sanctions pourraient comprendre, à titre exceptionnel, des mesures telles que l'immobilisation, la saisie ou la confiscation du moyen de transport, ou la suspension temporaire de la licence d'exploitation, voire son retrait.
- (18) Chaque État membre devrait être responsable de l'évaluation des menaces potentielles liées aux infractions terroristes et aux infractions graves.
- (19) Pour respecter pleinement le droit à la protection des données à caractère personnel et le droit à la non-discrimination, aucune décision susceptible de produire des effets juridiques préjudiciables à une personne ou de l'affecter gravement ne peut être prise sur la seule base du traitement automatisé des données PNR la concernant. Par ailleurs, aucune décision de cette nature ne devrait être fondée sur la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle.
- (20) Les États membres devraient, au besoin, partager avec les autres États membres les données PNR qu'ils reçoivent, lorsqu'un transfert est nécessaire aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière. Les dispositions de la présente directive ne devraient en rien porter atteinte à d'autres instruments de l'Union relatifs à l'échange d'informations entre les services de police et les autorités judiciaires, et notamment la décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol)³⁹ et la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne⁴⁰. Il conviendrait que les échanges de données PNR entre les services répressifs et les autorités judiciaires soient régis par les règles de la coopération policière et judiciaire.
- (21) La durée de conservation des données PNR devrait être proportionnée aux objectifs poursuivis, c'est-à-dire la prévention et la détection des infractions terroristes et des infractions graves, ainsi que les enquêtes et les poursuites en la matière. En raison de la nature et des usages des données PNR, il est indispensable qu'elles soient conservées pendant une période suffisamment longue pour permettre la réalisation

³⁹ JO L 121 du 15.5.2009, p. 37.

⁴⁰ JO L 386 du 29.12.2006, p. 89.

d'analyses et leur utilisation dans le cadre d'enquêtes. Pour éviter toute utilisation disproportionnée, il est nécessaire de les anonymiser après un délai initial et d'en subordonner l'accès à des conditions très strictes et limitées.

- (22) Lorsque des données PNR spécifiques ont été transférées à une autorité compétente et servent dans le cadre d'enquêtes ou de poursuites pénales particulières, leur durée de conservation par cette autorité devrait être fixée par le droit interne de l'État membre concerné, indépendamment des délais de conservation prévus dans la présente directive.
- (23) Dans chaque État membre, les traitements de données PNR effectués au plan national par l'unité de renseignements passagers et par les autorités compétentes devraient être soumis à une norme de protection des données à caractère personnel, en vertu de la législation nationale, qui soit conforme à la 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 pénale⁴¹ (ci-après la «décision-cadre 2008/977/JAI»).
- (24) Compte tenu du droit à la protection des données à caractère personnel, il conviendrait que les droits des personnes dont les données PNR sont traitées, tels que les droits d'accès, de rectification, d'effacement et de verrouillage, ainsi que le droit à réparation et le droit à un recours juridictionnel, soient conformes à la décision-cadre 2008/977/JAI.
- (25) 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 qu'ils reçoivent une information précise sur la collecte des données PNR et sur le transfert de celles-ci à l'unité de renseignements passagers.
- (26) Les États membres ne devraient être autorisés à transférer des données PNR vers des pays tiers qu'au cas par cas et conformément à 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, à la qualité de l'autorité destinataire et aux garanties applicables aux données à caractère personnel transmises au pays tiers.
- (27) 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 quant aux dispositions de la présente directive et d'en surveiller l'application et la mise en œuvre.
- (28) La présente directive ne porte pas atteinte à la possibilité offerte aux États membres de prévoir, en vertu de leur législation nationale, un système de collecte et de traitement des données PNR à des fins autres que celles visées dans la présente directive, ou de collecter, auprès de transporteurs autres que ceux que la directive mentionne, des données relatives à des vols intérieurs et de les traiter, sous réserve du respect des règles de protection des données correspondantes et pour autant que cette législation nationale soit conforme à l'acquis de l'Union. Il conviendrait que la question de la

⁴¹ JO L 350 du 30.12.2008, p. 60.

collecte des données PNR relatives aux vols intérieurs fasse l'objet d'une réflexion particulière à l'avenir.

- (29) Comme les dispositions nationales relatives au traitement des données à caractère personnel, et notamment les 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 ainsi que les conditions dans lesquelles ces informations doivent être rendues accessibles 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 infractions graves, ainsi que des enquêtes et des poursuites en la matière.
- (30) Étant donné les objectifs de la présente directive ne peuvent être réalisés de manière suffisante par les États membres et peuvent donc être mieux réalisés au niveau de l'Union, l'Union peut adopter 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 cet objectif.
- (31) La présente directive respecte les droits fondamentaux et les principes énoncés dans la charte des droits fondamentaux de l'Union européenne, 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 les articles 8, 7 et 21 de la charte et doit 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 satisfaire au principe de proportionnalité, elle introduit, pour certaines questions, des règles de protection des données plus strictes que celles de la décision-cadre 2008/977/JAI.
- (32) En particulier, le champ d'application de la présente directive est aussi limité que possible: la conservation des données PNR est autorisée pendant une période n'excédant pas cinq ans, au terme de laquelle les données doivent être effacées; les données doivent être anonymisées après un très court délai; la collecte et l'utilisation des données sensibles sont interdites. 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 ait la responsabilité de surveiller les modalités de traitement des données PNR et joue un rôle consultatif à cet égard. Tout traitement de données PNR doit être journalisé ou faire l'objet d'une trace documentaire à des fins de vérification de la licéité du traitement, d'autocontrôle et de garantie de l'intégrité des données et de la sécurité du traitement des données. Les États membres doivent également veiller à ce que les passagers reçoivent une information claire et précise sur la collecte des données PNR et sur leurs droits.
- (33) [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, le Royaume-Uni et l'Irlande ont notifié leur souhait de participer à l'adoption et à l'application de la présente directive] OU [Sans préjudice de l'article 4 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, le Royaume-Uni et l'Irlande ne participeront pas à l'adoption de la présente directive et ne seront donc pas liés par celle-ci ni soumis à son application].

- (34) Conformément aux articles 1^{er} et 2 du protocole (n° 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 donc pas lié par celle-ci ni soumis à son application,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. La présente directive prévoit le transfert, par les transporteurs aériens, des données des dossiers des passagers de vols internationaux à destination et en provenance des États membres, ainsi que le traitement de ces données, notamment leur collecte, leur utilisation et leur conservation par les États membres, et leur échange entre lesdits États.
2. Les données PNR recueillies conformément à la présente directive ne peuvent être traitées qu'aux fins suivantes:
 - (a) la prévention et la détection d'infractions terroristes et d'infractions graves, ainsi que la réalisation d'enquêtes et de poursuites en la matière conformément à l'article 4, paragraphe 2, points b) et c); et
 - (b) la prévention et la détection d'infractions terroristes et d'infractions transnationales graves, ainsi que la réalisation d'enquêtes et de poursuites en la matière conformément à l'article 4, paragraphe 2, points a) et d).

Article 2

Définitions

Aux fins de la présente directive, on entend par:

- a) «transporteur aérien»: une entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent, qui lui permet de transporter des passagers par voie aérienne;
- b) «vol international»: tout vol régulier ou non, effectué par un transporteur aérien devant atterrir sur le territoire d'un État membre en provenance d'un pays tiers ou

devant quitter le territoire d'un État membre à destination finale d'un pays tiers, y compris, dans les deux cas, tout vol de transfert ou de transit;

- c) «Passenger Name Record» ou «PNR»: le dossier de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens adhérents qui assurent les réservations pour chaque voyage réservé par une personne ou en son nom, que le dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs ou des systèmes équivalents offrant les mêmes fonctionnalités;
- d) «passager»: toute personne, à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef, avec le consentement du transporteur;
- e) «système de réservation»: le système interne d'inventaire du transporteur aérien, dans lequel les données PNR sont recueillies pour le traitement des réservations;
- f) «méthode push»: la méthode par laquelle les transporteurs aériens transfèrent les données PNR requises vers la base de données de l'autorité requérante;
- g) «infractions terroristes»: les infractions en droit national visées aux articles 1^{er} à 4 de la décision-cadre 2002/475/JAI du Conseil;
- h) «infractions graves»: les infractions en droit national visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil, si elles sont passibles, dans le droit interne de l'État membre, d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans; les États membres peuvent néanmoins exclure les infractions mineures pour lesquelles, compte tenu de leurs systèmes respectifs de justice pénale, le traitement des données PNR conformément à la présente directive serait contraire au principe de proportionnalité;
- i) «infractions transnationales graves»: les infractions en droit national visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil, si elles sont passibles, dans le droit interne de l'État membre, d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans, et si:
 - i) elles sont commises dans plus d'un État;
 - ii) elles sont commises dans un seul État, mais une part importante de leur préparation, de leur planification, de leur conduite ou de leur contrôle a lieu dans un autre État;
 - iii) elles sont commises dans un seul État mais impliquent un groupe criminel organisé qui est engagé dans des activités criminelles dans plus d'un État;
 - iv) elles sont commises dans un seul État mais ont des incidences considérables dans un autre État.

CHAPITRE II

RESPONSABILITÉS INCOMBANT AUX ÉTATS MEMBRES

Article 3

Unité de renseignements passagers

1. Chaque État membre crée ou désigne une autorité compétente en matière de prévention et de détection d'infractions terroristes et d'infractions graves, ainsi que d'enquêtes et de poursuites en la matière, ou crée ou désigne un département d'une telle autorité pour exercer la fonction d'«unité de renseignements passagers» nationale, chargée de la collecte des données PNR auprès des transporteurs aériens, de leur conservation et de leur analyse et de la transmission des résultats des analyses aux autorités compétentes visées à l'article 5. Les membres de son personnel peuvent être des agents détachés par les autorités publiques compétentes.
2. Deux ou plusieurs États membres peuvent instituer ou désigner la même autorité en tant qu'unité de renseignements passagers. Cette unité est établie dans l'un des États membres participants et est considérée comme l'unité nationale de renseignements passagers de tous les États membres participants. Ces derniers acceptent les règles détaillées de fonctionnement de l'unité de renseignements passagers et respectent les dispositions de la présente directive.
3. Chaque État membre informe la Commission dans un délai d'un mois à compter de la mise en place de l'unité de renseignements passagers et peut à tout moment actualiser sa déclaration. La Commission publie cette information, et notamment toute mise à jour, au *Journal officiel de l'Union européenne*.

Article 4

Traitement des données PNR

1. Les données PNR, transférées par les transporteurs aériens conformément à l'article 6, qui concernent des vols internationaux ayant pour point d'arrivée ou de départ le territoire de tout État membre sont recueillies par l'unité de renseignements passagers de l'État membre concerné. Si les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées en annexe, l'unité de renseignements passagers efface ces données supplémentaires dès leur réception.
2. L'unité de renseignements passagers ne traite les données PNR qu'aux fins suivantes:
 - (c) procéder à l'évaluation du risque représenté par les passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes qui peuvent être impliquées dans une infraction terroriste ou une infraction transnationale grave et pour lesquelles un examen plus approfondi par les autorités compétentes visées à l'article 5 est requis. Lors de cette évaluation, l'unité de renseignements passagers peut traiter les données PNR au regard de critères préétablis. Les États membres s'assurent que tout résultat positif obtenu par un tel traitement automatisé est contrôlé individuellement par des moyens non automatisés, afin de vérifier si l'intervention de l'autorité compétente visée à l'article 5 est nécessaire;

- (d) procéder à l'évaluation du risque représenté par les passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes qui peuvent être impliquées dans une infraction terroriste ou une infraction grave et pour lesquelles un examen plus approfondi par les autorités compétentes visées à l'article 5 est requis. Lors de cette évaluation, l'unité de renseignements passagers peut confronter les données PNR aux bases de données pertinentes, notamment des bases de données internationales ou nationales ou des bases de données de l'Union mises en miroir au niveau national, lorsqu'elles sont créées, en vertu du droit de l'Union, pour recenser les personnes ou objets recherchés ou visés par un signalement, en conformité avec les dispositions de l'Union et les dispositions internationales et nationales applicables aux fichiers de cette nature. Les États membres s'assurent que tout résultat positif obtenu par un tel traitement automatisé est contrôlé individuellement par des moyens non automatisés, afin de vérifier si l'intervention de l'autorité compétente visée à l'article 5 est nécessaire;
 - (e) réagir, au cas par cas, aux demandes dûment motivées d'autorités compétentes visant à obtenir des données PNR et le traitement de celles-ci dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou d'infractions graves, ainsi que de la réalisation d'enquêtes et de poursuites en la matière, et communiquer aux autorités compétentes les résultats de ce traitement; et
 - (f) analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères pour la réalisation d'évaluations en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une infraction transnationale grave conformément au point a).
3. L'évaluation du risque représenté par les passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, visée au paragraphe 2, point a), est réalisée de façon non discriminatoire au regard des critères d'évaluation définis par l'unité de renseignements passagers. Les États membres veillent à ce que les critères d'évaluation soient fixés par les unités de renseignements passagers, en coopération avec les autorités compétentes visées à l'article 5. Lesdits critères ne sont en aucun cas fondés sur la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle.
4. L'unité de renseignements passagers d'un État membre transfère les données PNR ou les résultats du traitement des données PNR des personnes identifiées conformément au paragraphe 2, points a) et b), aux autorités compétentes de ce même État membre pour examen plus approfondi. Ces transferts ne sont effectués qu'au cas par cas.

Article 5

Autorités compétentes

1. Chaque État membre arrête une liste des autorités compétentes habilitées à demander ou à obtenir des données PNR ou le résultat du traitement de telles données auprès des unités de renseignements passagers, en vue d'un examen plus approfondi des informations ou de l'adoption des mesures requises aux fins de la prévention et de la

détection d'infractions terroristes et d'infractions graves, ainsi que d'enquêtes ou de poursuites en la matière.

2. Les autorités compétentes sont celles habilitées à intervenir en matière de prévention ou de détection d'infractions terroristes et d'infractions graves, ainsi que d'enquêtes ou de poursuites dans ce domaine.
3. Chaque État membre communique à la Commission la liste de ses autorités compétentes dans un délai maximal de douze mois à compter de l'entrée en vigueur de la présente directive et peut à tout moment actualiser sa déclaration. La Commission publie cette information, ainsi que toute mise à jour, au *Journal officiel de l'Union européenne*.
4. Les données PNR et le résultat du traitement de telles données communiqués par l'unité de renseignements passagers ne peuvent faire l'objet d'un traitement ultérieur par les autorités compétentes des États membres qu'aux fins de la prévention ou de la détection d'infractions terroristes ou d'infractions graves, ainsi que d'enquêtes ou de 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 indices d'infractions sont détectés lors d'actions répressives menées à la suite dudit traitement.
6. Les autorités compétentes s'abstiennent de prendre toute décision susceptible de produire des effets juridiques préjudiciables à une personne ou de l'affecter gravement sur la seule base du traitement automatisé de données PNR. Les décisions de cette nature ne peuvent pas être fondées sur la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle.

Article 6

Obligations imposées aux transporteurs aériens

1. Les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent (méthode push) les données PNR telles que définies à l'article 2, point c), et énumérées en annexe, pour autant qu'ils recueillent déjà ces données, vers la base de données de l'unité nationale de renseignements passagers de l'État membre sur le territoire duquel le vol international 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. Si le vol comporte une ou plusieurs escales dans les aéroports des États membres, les transporteurs aériens transfèrent les données PNR aux unités de renseignements passagers de tous les États membres concernés.
2. Les transporteurs aériens transfèrent les données PNR par voie électronique au moyen des protocoles communs et des formats de données reconnus qui doivent être adoptés selon la procédure définie aux articles 13 et 14 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 le départ programmé 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 que d'autres passagers ne peuvent plus embarquer.
3. Les États membres peuvent autoriser les transporteurs aériens à limiter les transferts visés au paragraphe 2, point b), aux mises à jour des transferts visés au paragraphe 2, point a).
4. Au cas par cas, à la demande d'une unité de renseignements passagers conformément au droit national, les transporteurs aériens transfèrent des données PNR lorsqu'il est nécessaire d'y avoir accès avant le moment indiqué au paragraphe 2, point a), pour réagir à une menace spécifique et réelle liée à des infractions terroristes ou à des infractions graves.

Article 7

Échange d'informations entre États membres

1. Les États membres veillent à ce que, s'agissant de personnes identifiées par une unité de renseignements passagers conformément à l'article 4, paragraphe 2, points a) et b), le résultat du traitement des données PNR soit transmis par ladite unité aux unités de renseignements passagers d'autres États membres, lorsque ladite unité considère ce transfert nécessaire pour prévenir ou détecter des infractions terroristes ou des infractions graves ou pour procéder à des enquêtes ou à des poursuites en la matière. Les unités de renseignements passagers des États membres destinataires transmettent ces données PNR ou le résultat du traitement de ces données aux autorités compétentes desdits États.
2. L'unité de renseignements passagers d'un État membre a le droit de demander, au besoin, à l'unité de renseignements passagers de tout autre État membre de lui communiquer des données PNR qui sont conservées dans sa base de données conformément à l'article 9, paragraphe 1, ainsi que, si nécessaire, le résultat du traitement de données PNR. Cette demande peut être viser un ou plusieurs éléments de données, selon ce que l'unité de renseignements passagers requérante estime nécessaire dans un cas précis de prévention ou de détection d'infractions terroristes ou d'infractions graves ou d'enquêtes ou de poursuites en la matière. Les unités de renseignements passagers communiquent les données demandées aussi rapidement qu'elles le peuvent et transmettent aussi le résultat du traitement des données PNR, s'il a déjà été entrepris conformément à l'article 4, paragraphe 2, points a) et b).
3. L'unité de renseignements passagers d'un État membre a le droit de demander, au besoin, à l'unité de renseignements passagers de tout autre État membre de lui communiquer des données PNR qui sont conservées dans sa base de données conformément à l'article 9, paragraphe 2, ainsi que, si nécessaire, le résultat du traitement de données PNR. L'unité de renseignements passagers ne peut demander l'accès à des données PNR précises, conservées par l'unité de renseignements passagers d'un autre État membre, dans leur intégralité et sans passages tronqués, que

dans des circonstances exceptionnelles, afin de réagir à une menace spécifique ou dans le cadre d'une enquête ou de poursuites spécifiques concernant des infractions terroristes ou des infractions graves.

4. Ce n'est que si la prévention d'une menace immédiate et grave à la sécurité publique le requiert que les autorités compétentes d'un État membre peuvent demander directement à l'unité de renseignements passagers d'un autre État membre de leur communiquer des données PNR qu'elle conserve dans sa base de données conformément à l'article 9, paragraphes 1 et 2. Ces demandes s'inscrivent dans le cadre d'une enquête spécifique ou de poursuites spécifiques concernant des infractions terroristes ou des infractions graves et sont motivées. Les unités de renseignements passagers accordent un traitement prioritaire à ces demandes. Dans tous les autres cas, les autorités compétentes transmettent leurs demandes par l'intermédiaire de l'unité de renseignements passagers de leur propre État membre.
5. À titre exceptionnel, si l'accès anticipé à des données PNR est nécessaire pour réagir à une menace spécifique et réelle ayant trait à des infractions terroristes ou à des infractions graves, l'unité de renseignements passagers d'un État membre a le droit de demander à l'unité de renseignements passagers d'un autre État membre de lui communiquer à tout moment les données PNR de vols à destination de son territoire ou en provenance de celui-ci.
6. L'échange d'informations en vertu du présent article peut avoir lieu par l'intermédiaire de n'importe quel canal de coopération internationale existant entre les services répressifs. La langue utilisée pour la demande et l'échange d'informations est celle applicable à l'utilisation du canal retenu. Lorsqu'ils procèdent aux notifications conformément à l'article 3, paragraphe 3, 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 aux États membres les notifications qu'elle reçoit.

Article 8

Transfert de données vers des pays tiers

Un État membre ne peut transférer à un pays tiers des données PNR et les résultats du traitement de telles données qu'au cas par cas et si:

- a) les conditions définies à l'article 13 de la décision-cadre 2008/977/JAI du Conseil sont remplies;
- b) le transfert est nécessaire aux fins de la présente directive précisées à l'article 1, paragraphe 2, et si
- c) Le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque c'est nécessaire aux fins précisées à l'article 1^{er}, paragraphe 2, de la présente directive et uniquement sur autorisation expresse de l'État membre.

Durée de conservation des données

1. Les États membres veillent à ce que les données PNR transmises par les transporteurs aériens à l'unité de renseignements passagers y soient conservées dans une base de données pendant une période de 30 jours à compter de leur transfert à l'unité de renseignements passagers du premier État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol international.
2. À l'expiration de la période de 30 jours à compter du transfert des données PNR à l'unité de renseignements passagers visée au paragraphe 1, les données y sont conservées pendant une période supplémentaire de cinq ans. Au cours de cette période, tous les éléments d'information pouvant servir à identifier le passager auquel se rapportent les données PNR sont masqués. Les données PNR ainsi anonymisées ne sont accessibles qu'à un nombre limité d'employés de l'unité de renseignements passagers, qui sont expressément autorisés à analyser les données PNR et à mettre au point des critères d'évaluation conformément à l'article 4, paragraphe 2, point d). L'accès à l'intégralité des données PNR n'est autorisé que par le responsable de l'unité de renseignements passagers aux fins de l'article 4, paragraphe 2, point c), et lorsqu'il est raisonnable de penser que cet accès est nécessaire pour mener une enquête ou pour réagir à une menace ou à un risque spécifique et tangible, ou pour donner suite à une enquête spécifique ou à des poursuites spécifiques.

Aux fins de la présente directive, les éléments d'information pouvant servir à identifier le passager auquel se rapportent les données PNR et devant être filtrés et masqués sont les suivants:

- le(s) nom(s), notamment les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;
 - l'adresse et les coordonnées;
 - les remarques générales, dans la mesure où elles comportent des informations pouvant servir à identifier le passager auquel le PNR se rapporte; et
 - toute information préalable sur les passagers qui a été recueillie.
3. Les États membres veillent à ce que les données PNR soient effacées à l'expiration du délai prévu au paragraphe 2. Cette obligation s'applique sans préjudice des cas où des données PNR spécifiques ont été transférées à une autorité compétente et servent dans le cadre d'enquêtes ou de poursuites pénales particulières, auquel cas la conservation de ces données par l'autorité compétente est régie par le droit interne de l'État membre.
 4. Le résultat de la mise en correspondance visée à l'article 4, paragraphe 2, points a) et b), n'est conservé par l'unité de renseignements passagers que le temps nécessaire pour informer les autorités compétentes d'un résultat positif. Lorsque, après réexamen individuel par des moyens non automatisés, le résultat d'une mise en correspondance automatisée s'est révélé négatif, il est néanmoins archivé de manière à éviter de futurs «faux» résultats positifs pendant une période maximale de trois ans, à moins que les données de base n'aient pas encore été effacées conformément au

paragraphe 3 à l'expiration de la période de cinq ans, auquel cas le journal est conservé jusqu'à l'effacement des données de base.

Article 10

Sanctions contre les transporteurs aériens

Les États membres veillent, conformément à leur législation nationale, à ce que des sanctions dissuasives, efficaces et proportionnées, notamment des sanctions financières, soient infligées aux transporteurs aériens qui ne transmettent pas les données requises en vertu de la présente directive, pour autant qu'ils les collectent déjà, ou ne les transmettent pas dans le format requis ou transgressent de quelque autre façon les dispositions nationales adoptées en application de la présente directive.

Article 11

Protection des données à caractère personnel

1. Chaque État membre veille à ce que, pour tout traitement de données à caractère personnel au titre de la présente directive, tout passager ait un droit d'accès, un droit de rectification, d'effacement et de verrouillage des données, un droit à réparation et un droit à un recours juridictionnel qui soient identiques à ceux adoptés en droit national en application des articles 17, 18, 19 et 20 de la décision-cadre 2008/977/JAI du Conseil. Les dispositions des articles 17, 18, 19 et 20 de la décision-cadre 2008/977/JAI du Conseil sont donc 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 du Conseil, qui concernent la confidentialité du traitement et la sécurité des données, soient également appliquées à tous les traitements de données à caractère personnel effectués conformément à la présente directive.
3. Tout traitement de données PNR révélant la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle est interdit. Au cas où l'unité de renseignements passagers recevrait des données PNR révélant de telles informations, elle les efface immédiatement.
4. Tout traitement de données PNR effectué par les transporteurs aériens, tout transfert de données PNR réalisé par les unités de renseignements passagers et toute demande formulée par les autorités compétentes ou les unités de renseignements passagers d'autres États membres et de pays tiers, même en cas de refus, est journalisé ou fait l'objet d'une trace documentaire conservée par l'unité de renseignements passagers et les autorités compétentes à des fins de vérification de la licéité du traitement des données, d'autocontrôle et de garantie de l'intégrité des données et de la sécurité du traitement des données, notamment par les autorités nationales de contrôle de la protection des données. Ces journaux sont conservés pendant une période de cinq ans, à moins que les données de base n'aient pas encore été effacées conformément à l'article 9, paragraphe 3, à l'expiration de ces cinq années, auquel cas les journaux sont conservés jusqu'à l'effacement des données de base.

5. Les États membres veillent à ce que les transporteurs aériens, leurs agents ou d'autres vendeurs de billets pour le transport de passagers sur des services aériens donnent aux passagers de vols internationaux, lors de la réservation d'un vol ou de l'achat d'un billet, des informations claires et précises sur la communication des données PNR à l'unité de renseignements passagers, la finalité du traitement desdites données, la durée de conservation des données, l'éventuelle utilisation de celles-ci en vue de prévenir et de détecter des infractions terroristes et des infractions graves ou de réaliser des enquêtes ou des poursuites en la matière, la possibilité d'échanger et de partager ces données et les droits des passagers en matière de protection des données, notamment le droit de déposer plainte auprès de l'autorité nationale de contrôle de la protection des données de leur choix. Ces mêmes informations mises à la disposition du public par les États membres.
6. Tout transfert de données PNR par les unités de renseignements passagers et les autorités compétentes à des personnes privées établies dans un État membre ou un pays tiers est interdit.
7. Sans préjudice de l'article 10, les États membres prennent les mesures appropriées pour assurer la pleine mise en œuvre des dispositions de la présente directive et définissent notamment les sanctions effectives, proportionnées et dissuasives à infliger en cas de violation des dispositions adoptées en application de la présente directive.

Article 12

Autorité de contrôle nationale

Chaque État membre prévoit que l'autorité de contrôle nationale mise en place en vertu de l'article 25 de la décision-cadre 2008/977/JAI est également chargée de conseiller et de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres conformément à la présente directive. Les autres dispositions de l'article 25 de la décision-cadre 2008/977/JAI sont applicables.

CHAPITRE IV

MESURES DE MISE EN ŒUVRE

Article 13

Protocoles communs et formats de données reconnus

1. Tous les transferts de données PNR effectués par des transporteurs aériens vers les unités de renseignements passagers aux fins de la présente directive se font par voie électronique ou, en cas de défaillance technique, par tout autre moyen approprié, pendant une période d'un an à compter de l'adoption des protocoles communs et des formats de données reconnus en application de l'article 14.

2. À l'issue de la période d'un an à compter de la date d'adoption des protocoles communs et des formats de données reconnus, tous les transferts de données PNR effectués par des transporteurs aériens vers les unités de renseignements passagers aux fins de la présente directive se font par voie électronique à l'aide de méthodes sécurisées utilisant des protocoles communs acceptés, qui sont identiques pour tous les transferts afin d'assurer la sécurité des données pendant le transfert, et un format de données reconnu afin d'assurer la lisibilité des données par toutes les parties concernées. Tous les transporteurs aériens sont tenus de choisir et de préciser à l'unité de renseignements passagers le protocole commun et le format de données qu'ils entendent utiliser pour leurs transferts.
3. La Commission dresse la liste des protocoles communs acceptés et des formats de données reconnus et, le cas échéant, l'adapte conformément à la procédure visée à l'article 14, paragraphe 2.
4. Tant que les protocoles communs acceptés et les formats de données reconnus visés aux paragraphes 2 et 3 ne sont pas disponibles, le paragraphe 1 reste applicable.
5. Chaque État membre veille à l'adoption des mesures techniques nécessaires pour pouvoir utiliser les protocoles communs et les formats de données dans un délai d'un an à compter de la date d'adoption des protocoles communs et des formats de données reconnus.

Article 14

Procédure de comité

1. La Commission est assistée par un comité («le comité»). Il s'agit d'un comité au sens du règlement [.../2011/UE] du 16 février 2011.
2. S'il est fait référence au présent paragraphe, l'article 4 du règlement [.../2011/UE] du 16 février 2011 s'applique.

CHAPITRE V

DISPOSITIONS FINALES

Article 15

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 deux ans après son entrée en vigueur. Ils communiquent immédiatement à la Commission le texte de ces dispositions ainsi qu'un tableau de correspondance entre ces dispositions et la présente directive.

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 couvert par la présente directive.

Article 16

Dispositions transitoires

À la date visée à l'article 15, paragraphe 1, c'est-à-dire deux ans après l'entrée en vigueur de la présente directive, les États membres veillent à ce que les données PNR d'au moins 30 % de l'ensemble des vols visés à l'article 6, paragraphe 1, soient recueillies. Dans un délai de deux ans à compter de la date visée à l'article 15, les États membres veillent à ce que les données PNR d'au moins 60 % de l'ensemble des vols visés à l'article 6, paragraphe 1, soient recueillies. Les États membres veillent à ce que, à compter de quatre ans après la date visée à l'article 15, les données PNR de l'ensemble des vols visés à l'article 6, paragraphe 1, soient recueillies.

Article 17

Réexamen

Sur la base des informations communiquées par les États membres, la Commission:

- a) réexamine la nécessité d'inclure des vols intérieurs dans le champ d'application de la présente directive ainsi que la faisabilité de cette inclusion, à la lumière de l'expérience acquise par les États membres qui recueillent des données PNR relatives à des vols intérieurs. La Commission présente un rapport au Parlement européen et au Conseil dans les deux ans qui suivent la date mentionnée à l'article 15, paragraphe 1;
- b) procède à un réexamen du fonctionnement de la présente directive et présente un rapport au Parlement européen et au Conseil dans les quatre ans qui suivent la date mentionnée à l'article 15, paragraphe 1. Ce réexamen couvre tous les éléments de la présente directive, une attention particulière étant accordée au respect du niveau de protection des données à caractère personnel, à la durée de conservation des données et à la qualité des évaluations. Il comporte aussi les statistiques recueillies conformément à l'article 18.

Article 18

Données statistiques

1. Les États membres compilent une série de statistiques sur les données PNR communiquées aux unités de renseignements passagers. Ces statistiques indiquent au moins, par transporteur aérien et par destination, le nombre d'identifications de personnes pouvant être impliquées dans une infraction terroriste ou une infraction

grave conformément à l'article 4, paragraphe 2, et le nombre d'actions de répression consécutives ayant comporté l'utilisation de données PNR.

2. Ces statistiques ne contiennent pas de données à caractère personnel. Elles sont transmises annuellement à la Commission.

Article 19

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 moment de l'adoption de la présente directive, dans la mesure où ils sont compatibles avec celle-ci.
2. La présente directive s'applique sans préjudice des obligations et engagements de l'Union qui découlent d'accords bilatéraux et/ou multilatéraux avec des pays tiers.

Article 20

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

Par le Parlement européen
Le président

Par le Conseil
Le président

ANNEXE

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

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