CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 22 septembre 2010 (24.09)
(OR. en)

13954/10

JAI 764
DATAPROTECT 67
AVIATION 134
RELEX 789

NOTE DE TRANSMISSION

Origine:	Pour le Secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, Directeur
Date de réception:	21 septembre 2010
Destinataire:	Monsieur Pierre de BOISSIEU, Secrétaire général du Conseil de l'Union européenne
Objet:	Communication de la Commission relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers

Les délégations trouveront ci-joint le document de la Commission - COM(2010) 492 final.

p.j.: COM(2010) 492 final

COMMISSION EUROPÉENNE

Bruxelles, le 21.9.2010
COM(2010) 492 final

COMMUNICATION DE LA COMMISSION

relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers

COMMUNICATION DE LA COMMISSION

relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers

1. INTRODUCTION

Les attentats terroristes perpétrés aux États-Unis en 2001, à Madrid en 2004 et à Londres en 2005 ont conduit à définir une nouvelle approche des politiques en matière de sécurité intérieure. Des événements récents, tels que la tentative d'attentat terroriste survenue dans un avion le jour de Noël en 2009, et celle déjouée à Times Square, à New York, en 2010, indiquent que la menace terroriste est toujours présente. Parallèlement, on note une progression de la criminalité organisée, en particulier du trafic de drogue et de la traite des êtres humains[1].

En réponse à ces menaces persistantes, l'UE et certains pays tiers ont adopté de nouvelles mesures, dont la collecte et l'échange de données à caractère personnel. Une vue d'ensemble de ces mesures a été fournie par la Commission dans sa présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice[2]. Parmi celles-ci figure l'utilisation des données des dossiers passagers (*Passenger Name Record* – PNR) à des fins répressives.

Le 16 janvier 2003, la Commission a publié une communication au Conseil et au Parlement intitulée «Transfert des données des dossiers passagers (*Passenger Name Record* - PNR): une démarche globale de l'Union européenne»[3] qui visait à définir les éléments d'une démarche globale de l'UE concernant les données PNR. Cette communication préconisait la définition d'un cadre juridiquement sûr pour les transferts des dossiers passagers vers le ministère de la sécurité intérieure des États-Unis et l'adoption d'une politique intérieure relative aux dossiers passagers. Elle prônait également la mise au point par les transporteurs aériens d'un système de transfert de données de type «push»[4] et la présentation d'une initiative internationale sur les transferts de données PNR par l'Organisation de l'aviation civile internationale (OACI).

Les conclusions de cette communication ont déjà été mises en œuvre dans une large mesure, ou sont en passe de l'être. L'UE a notamment signé avec le ministère de la sécurité intérieure des États-Unis un accord relatif au transfert de données PNR dans l'intérêt de la lutte contre le terrorisme et les formes graves de criminalité transnationale et qui garantit la protection des données à caractère personnel lors du transfert de données PNR[5]. En outre, la Commission a adopté une proposition de décision-cadre relative à l'utilisation des données PNR à des fins répressives[6]. La Commission examine actuellement, en s'appuyant sur une analyse d'impact, la possibilité de remplacer cette décision-cadre par une proposition de directive relative à l'utilisation des données PNR à des fins répressives. Le système de transfert de données de type «push» a été mis en place comme il se doit par la plupart des transporteurs, tandis que

---

1 Eurostat 36/2009.
2 COM(2010) 385.
3 COM(2003) 826.
4 Selon ce système, le transporteur transmet les données au pays tiers plutôt que d'accorder à ce dernier l'accès à ses bases de données.
5 JO L 204 du 4.8.2007, p. 16.
6 COM(2007) 654.

l'OACI a élaboré une série de lignes directrices pour les transferts de données PNR aux autorités publiques.

Outre l'accord avec les États-Unis, l'UE a conclu des accords similaires avec le Canada[7] et l'Australie[8]. La Nouvelle-Zélande, la Corée du Sud et le Japon utilisent également les données PNR, mais n'avaient pas conclu d'accord avec l'UE à la date de rédaction du présent rapport. Au sein de l'Union, le Royaume-Uni a mis en place un système PNR, tandis que d'autres États membres ont adopté la législation nécessaire ou utilisent les données PNR à titre expérimental.

Ces évolutions témoignent que l'utilisation des données PNR s'étend et qu'elle est de plus en plus considérée comme un aspect normal et nécessaire du travail des services répressifs. Or cette utilisation implique le traitement de données à caractère personnel qui soulève d'importantes questions quant au respect de deux droits fondamentaux, la protection de la vie privée et la protection des données à caractère personnel.

L'Union est dès lors confrontée à de nouveaux défis en ce qui concerne les transferts internationaux de données PNR. Il est en effet très probable que l'on assiste, au cours des années à venir, à une augmentation du nombre de pays qui mettront en place des systèmes PNR partout dans le monde. En outre, l'UE a acquis une connaissance approfondie de la structure et de la valeur des systèmes PNR dans le cadre des réexamens conjoints des accords conclus avec les États-Unis et le Canada.

La Commission estime donc nécessaire de revoir sa démarche globale relative aux transferts des données PNR aux pays tiers. La révision de cette démarche devrait prévoir des garanties solides en matière de protection des données, assurer le plein respect des droits fondamentaux et être conforme aux principes d'élaboration des politiques définis dans la présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice[9]. Il importe tout particulièrement, dans le cadre de la révision de la démarche relative aux dossiers passagers, de recueillir les points de vue des principaux acteurs, tels que les États membres, le Parlement européen, le contrôleur européen de la protection des données et le groupe de travail article 29 sur la protection des données, concernant les questions générales que soulève l'utilisation de ce type de données.

L'objectif premier de la présente communication est d'établir, pour la première fois, un ensemble de critères généraux qui servirait de base aux futures négociations relatives aux accords PNR à conclure avec les pays tiers. L'UE pourra ainsi mieux répondre aux tendances actuelles et expliquer aux pays tiers, aux États membres et aux citoyens comment la Commission européenne souhaite définir sa politique extérieure relative aux dossiers passagers. Les recommandations qui seront formulées par la Commission en ce qui concerne la négociation d'accords PNR avec les pays tiers devraient désormais respecter au minimum les critères généraux énoncés dans la présente communication, tandis que des critères supplémentaires pourraient être établis dans chaque recommandation.

---

7 OJ L 91, 29.3.2006, p. 53, OJ L 91, 29.3.2006, p. 49 and OJ L 82, 21.3.2006, p. 15.

8 OJ L 213, 8.8.2008 p. 49.

9 COM(2010) 385.

2. TENDANCES INTERNATIONALES RELATIVES AUX DOSSIERS PASSAGERS

2.1. Les données PNR et leur utilisation

Les données PNR sont des informations non vérifiées fournies par les passagers et recueillies par les transporteurs aux fins de la réservation et de la procédure d'enregistrement. Ces informations constituent le dossier de voyage de chaque passager, conservé dans les systèmes de réservation et de contrôle des départs des transporteurs. Ce dossier contient différents types d'informations, par exemple les dates de voyage et l'itinéraire, les informations relatives aux billets, les coordonnées telles que l'adresse et les numéros de téléphone, l'agence de voyage, les informations relatives au paiement, le numéro de siège et les informations relatives aux bagages.

Les données PNR sont à distinguer des renseignements préalables concernant les passagers (API – *Advance Passenger Information*). Les données API sont les informations biographiques extraites de la partie d'un passeport lisible par machine et contenant le nom, le lieu de résidence, le lieu de naissance et la nationalité du titulaire du document. En vertu de la directive API[10], les données API sont transmises aux autorités chargées d'effectuer les contrôles aux frontières uniquement pour les vols entrant sur le territoire de l'UE aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration illégale. Bien que leur utilisation à des fins répressives soit autorisée par la directive, elle est plutôt considérée comme une exception à la règle. Ces données sont conservées par les États membres pendant 24 heures.

Les données API servent essentiellement à effectuer des contrôles d'identité dans le cadre des contrôles aux frontières et de la gestion des frontières, même si, dans certains cas, les autorités répressives les utilisent également afin d'identifier des suspects et des personnes recherchées. Les données API sont donc principalement utilisées comme un outil de gestion de l'identité. L'utilisation de ces données est de plus en plus répandue dans le monde: plus de 30 pays les utilisent systématiquement et plus de 40 mettent actuellement en place des systèmes API.

Outre la transmission des données API, certains pays exigent des transporteurs qu'ils leur transmettent également les données PNR. Ces dernières servent alors à la lutte contre le terrorisme et les formes graves de criminalité, telles que la traite des êtres humains et le trafic de drogue. Les dossiers passagers sont utilisés depuis près de 60 ans, principalement par les autorités douanières, mais aussi par les autorités répressives du monde entier. Mais jusqu'à une époque récente, il n'était techniquement pas possible d'accéder à ces données à l'avance et par la voie électronique, si bien que leur utilisation se limitait à un traitement manuel pour certains vols seulement. Grâce aux progrès technologiques, il est aujourd'hui possible de transmettre ces données à l'avance par la voie électronique.

L'utilisation qui est faite des données PNR se distingue nettement de celle dont les données API font l'objet, principalement parce que les dossiers passagers contiennent des types de données très différents. Les dossiers passagers servent surtout d'outil de renseignement sur les activités criminelles, plutôt que d'outil de vérification de l'identité. Les données PNR, quant à elles, sont principalement utilisées: i) pour évaluer les risques associés aux passagers et identifier les personnes «inconnues», c'est-à-dire les personnes n'ayant pas encore été suspectées, mais susceptibles d'intéresser les services répressifs; ii) parce qu'elles sont disponibles avant les données API, et qu'elles laissent ainsi aux autorités répressives plus de temps pour les traiter, les analyser et prendre toute mesure de suivi nécessaire; iii) pour

[10] Directive 2004/82/CE du 29.8.2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.

déterminer à quelles personnes appartiennent certaines adresses, cartes crédits, etc. associées à des infractions pénales; et iv) pour effectuer des comparaisons avec d'autres données PNR dans le but d'identifier des complices, par exemple en recherchant les personnes qui voyagent ensemble.

La nature et l'utilisation des données PNR sont uniques. Trois types d'utilisation sont possibles:

- une utilisation réactive (données historiques): 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 à cet effet une période de conservation des données par ces services qui soit proportionnée;

- une utilisation en temps réel (données actuelles): dans le cadre de la prévention de la criminalité, d'enquêtes ou de l'arrestation de 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 indicateurs de risque factuels prédéterminés afin d'identifier les suspects jusqu'alors «inconnus» et, d'autre part, avec diverses bases de données de personnes et objets recherchés;

- une utilisation proactive (schémas et modèles): dans le cadre de l'analyse de tendances et de la création de schémas de déplacement et de modèles comportementaux généraux basés sur les faits, qui peuvent ensuite être utilisés en temps réel. Afin d'établir les schémas de déplacement et les modèles comportementaux, les analystes de tendances doivent pouvoir utiliser les données pendant une période suffisamment longue. Il convient donc de prévoir à cet effet une période de conservation des données par les services répressifs qui soit proportionnée.

2.2. Tendances actuelles

Certains pays tiers, à savoir les États-Unis, le Canada, l'Australie, la Nouvelle-Zélande et la Corée du Sud, utilisent déjà les données PNR à des fins répressives. D'autres, tels que le Japon, l'Arabie Saoudite, l'Afrique du Sud et Singapour, ont adopté une législation en la matière et/ou utilisent les données PNR à titre expérimental. Plusieurs autres pays tiers ont commencé à envisager la possibilité d'utiliser les données PNR, mais n'ont pas encore adopté de législation à ce sujet. Dans l'UE, le Royaume-Uni dispose déjà d'un système PNR. La France, le Danemark, la Belgique, la Suède et les Pays-Bas ont adopté une législation ad hoc et/ou utilisent les données PNR à titre expérimental. Plusieurs autres États membres étudient la possibilité de mettre en place un système PNR.

Reconnaissant la nécessité de disposer des données PNR dans le cadre de la prévention du terrorisme et des formes graves de criminalité et de la lutte contre ces phénomènes, la Commission européenne avait présenté, conformément à la communication de 2003, une proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* - PNR) à des fins répressives. À la suite de l'entrée en vigueur du traité de Lisbonne, elle a l'intention de remplacer cette proposition par une proposition de directive portant le même intitulé, qui visera à obliger les transporteurs aériens à transmettre aux États membres les données PNR qui seront utilisées pour lutter contre les attaques terroristes et les formes graves de criminalité.

La nécessité de disposer des données PNR pour lutter contre le terrorisme et les formes graves de criminalité est de plus en plus reconnue à l'échelon international. Cette tendance résulte de trois paramètres. Premièrement, le terrorisme et la criminalité au niveau international font peser une lourde menace sur la société et des initiatives doivent être prises pour s'attaquer à ces phénomènes. La consultation et l'analyse des données PNR font partie des mesures jugées

nécessaires du point de vue répressif. Deuxièmement, les récents progrès technologiques ont rendu cette consultation et cette analyse possibles, ce qui était inconcevable il y a quelques années. Les diverses avancées technologiques de ces dernières années sont également largement mises à profit par les auteurs d'infractions pour planifier, préparer et exécuter leurs méfaits. Troisièmement, face à l'essor rapide des déplacements internationaux et du volume de passagers, le traitement électronique des données préalablement à l'arrivée des passagers facilite et accélère grandement les contrôles de sécurité et les contrôles aux frontières, puisque le processus d'évaluation des risques s'effectue avant l'arrivée. Il permet aux services répressifs de se concentrer exclusivement sur les passagers pour lesquels ils disposent d'éléments factuels indiquant un risque réel pour la sécurité, plutôt que de tirer des conclusions fondées sur leur intuition, des stéréotypes ou des profils prédéfinis.

2.3. Effets des tendances actuelles sur l'Union européenne

La législation de l'Union en matière de protection des données n'autorise pas les transporteurs assurant des vols au départ de l'UE à transmettre les données PNR de leurs passagers à des pays tiers n'offrant pas un niveau adéquat de protection des données à caractère personnel sans fournir des garanties appropriées. Par conséquent, lorsque les États-Unis, le Canada et l'Australie ont demandé aux transporteurs de transmettre les données PNR relatives aux vols à destination de leur territoire, lesdits transporteurs se sont retrouvés dans une situation très délicate. C'est pourquoi l'UE est intervenue et a négocié et signé des accords internationaux distincts avec chacun de ces trois pays[11] afin de rendre possible le transfert de données PNR en dehors de l'UE aux services répressifs de ces trois pays. Cette intervention avait pour but d'aider les transporteurs à sortir de cette situation, d'assurer un niveau adéquat de protection des données des passagers et de reconnaître la nécessité et l'importance de l'utilisation des données PNR dans le cadre de la lutte contre le terrorisme et les formes graves de criminalité.

Le même problème devrait se poser au fur et à mesure que d'autres pays mettront en place des systèmes PNR. En outre, si la Commission décide d'aller de l'avant avec sa proposition de directive PNR européenne, les demandes de ce type pourraient se multiplier si les pays tiers exigent de l'UE qu'elle respecte le principe de réciprocité.

Jusqu'à présent, les accords PNR internationaux avec les pays tiers ont été conclus en fonction de la «demande» et au cas par cas. Bien que tous les accords abordent des questions communes et régissent les mêmes matières, leurs dispositions ne sont pas identiques, ce qui a parfois abouti à des divergences entre les règles applicables aux transporteurs et en matière de protection des données. Vu la probabilité que la «demande» augmente dans un avenir proche, une stratégie pourrait aider l'Union à y faire face d'une manière plus structurée, ce qui permettrait de réduire les différences entre les divers accords.

3. UNE DEMARCHE GLOBALE REVISEE EN MATIERE DE DONNEES PNR POUR L'UE

3.1. Raisons motivant la révision de la démarche globale en matière de données PNR

À l'heure de la mise en œuvre des conclusions de la communication de 2003 et alors que l'Union est confrontée à de nouvelles tendances et de nouveaux défis, il importe qu'elle tienne

---

[11] Accord PNR CE-USA de 2004 (JO L 183 du 20.5.2004, p. 84) et décision de la Commission du 14 mai 2004 (JO L 235 du 6.7.2004, p. 11); accord PNR UE-USA de 2006 (JO L 298 du 27.10.2006, p. 29) et lettres d'accompagnement (JO 259 du 27.10.2006, p. 1); accord PNR UE-USA de 2007 (JO L 204 du 4.8.2007, p. 18); accord PNR UE-Canada (JO L 82 du 21.3.2006, p. 15 et JO L 91 du 29.3.2006, p. 49) et accord PNR UE-Australie (JO L 213 du 8.8.2008, p. 47).

dûment compte de ceux-ci en étoffant encore sa démarche globale relative au transfert des données PNR à des pays tiers, pour les raisons exposées ci-après.

Lutter contre le terrorisme et les formes graves de criminalité transnationale: l'Union a l'obligation, vis-à-vis d'elle-même et des pays tiers, de coopérer avec ces derniers dans le cadre de la lutte contre ces menaces. L'une des formes de cette coopération est l'échange de données avec les pays tiers. La mise à disposition de données PNR à des fins répressives est en effet une mesure nécessaire à la lutte contre le terrorisme et les formes graves de criminalité transnationale. Tant la stratégie relative à la dimension externe de l'espace de liberté, de sécurité et de justice[12] que la stratégie de l'UE visant à lutter contre le terrorisme[13] et le programme de Stockholm[14] mentionnent la nécessité d'une telle collaboration étroite avec les pays tiers.

Assurer la protection des données à caractère personnel et de la vie privée: l'UE est déterminée à garantir un niveau élevé et effectif de protection des données à caractère personnel, notamment en veillant à ce que toute transmission de données PNR à des pays tiers se fasse d'une manière sécurisée et conforme aux exigences imposées par le droit de l'Union, et à ce que les passagers soient en mesure d'exercer leurs droits en rapport avec le traitement de leurs données.

Assurer la sécurité juridique et simplifier les obligations imposées aux transporteurs aériens: il importe que l'UE fournisse un cadre juridique cohérent pour la transmission de données PNR par les transporteurs aériens aux pays tiers. Ce cadre est indispensable pour protéger les transporteurs contre les sanctions et garantir que les conditions et modalités régissant les transmissions de données dans le monde entier soient aussi uniformes et harmonisées que possibles, de sorte à réduire la charge financière supportée par cette industrie et à assurer des conditions égales dans le secteur.

Établir des conditions générales visant à assurer la cohérence et à développer davantage la démarche internationale: les accords PNR conclus par l'UE avec des pays tiers sont similaires dans leur finalité, mais leur contenu varie en ce qui concerne les modalités de transmission et la nature des engagements pris par les pays tiers. Ces engagements différenciés sont acceptables dans une certaine mesure, compte tenu des écarts entre les exigences et les ordres juridiques nationaux, mais certains critères généraux devraient être respectés par tous les pays (voir les sections 3.2 et 3.3 ci-dessous). Afin d'assurer un traitement des passagers aussi uniforme que possible et de réduire les coûts supportés par l'industrie, il importe que les futurs accords conclus avec des pays tiers présentent des contenus et des critères aussi proches que possible. Ce rapprochement pourrait ensuite servir de base à l'étape suivante, qui pourrait consister à harmoniser davantage l'approche multilatérale des échanges de données PNR.

Assurer plus de commodité aux passagers: pour faire face aux menaces qui pèsent sur la sécurité dans nos sociétés, le contrôle des passagers lors du franchissement d'une frontière devient sans cesse plus détaillé et plus long. Cette situation, ajoutée à l'augmentation constante du volume des déplacements internationaux, a entraîné un allongement des files et temps d'attente aux frontières. La transmission électronique de données PNR avant le franchissement d'une frontière permet de contrôler les passagers à l'avance; ces derniers peuvent ainsi franchir plus rapidement et plus facilement les frontières, tandis que les services

---

12 COM(2005) 491.

13 Document du Conseil 14469/4/05 du 30.11.2005.

14 Document du Conseil 17024/09 du 2.12.2009.

répressifs peuvent se concentrer exclusivement sur les personnes identifiées qui les intéressent véritablement.

3.2. Considérations générales

La démarche globale révisée relative aux dossiers passagers vise à fournir à l'UE un cadre de référence qui lui permettra de décider de la meilleure manière de répondre aux demandes de transmission de données PNR qui lui seront adressées à l'avenir par les pays tiers. Outre les principes d'élaboration des politiques qui ont été définis dans la présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice, il convient de prendre en compte les considérations spécifiques exposées ci-dessous.

Intérêt partagé pour la sécurité: le terrorisme et les formes graves de criminalité présentent, de par leur nature, un caractère international. Certains pays du monde sont néanmoins plus exposés que d'autres à ce type de menaces grandissantes. L'UE est déterminée à collaborer avec ces pays et à les aider à combattre ces risques pour la sécurité.

Protection des données à caractère personnel: étant donné que la transmission, l'utilisation et le traitement des données PNR ont une incidence sur le droit fondamental des personnes à la protection de leurs données à caractère personnel, il est absolument essentiel que l'Union ne collabore qu'avec les pays tiers qui sont en mesure de fournir un niveau adéquat de protection pour les données PNR en provenance de l'UE.

Relations extérieures: la globalité de la relation extérieure de l'UE avec le pays tiers devrait également être prise en considération. Le fonctionnement des services de police et du pouvoir judiciaire ainsi que la collaboration avec ceux-ci, l'État de droit et le respect général des droits fondamentaux sont autant de facteurs importants dont il convient de tenir compte.

3.3. Normes, contenu et critères

La démarche globale en matière de données PNR devrait décrire les normes générales auxquelles les accords internationaux conclus entre l'UE et les pays tiers devraient satisfaire, afin d'assurer la plus grande cohérence possible entre les garanties offertes par ces pays en matière de protection des données et entre les modalités de transmission des données par les transporteurs aériens.

Il est également essentiel que l'UE soit dotée de mécanismes de contrôle du bon déroulement de la mise en œuvre, tels que des réexamens conjoints réguliers de l'application des accords, et des mécanismes efficaces de résolution des litiges.

3.3.1. Protection des données à caractère personnel

La collecte des données PNR et leur transfert vers les pays tiers concernent un très grand nombre de personnes ainsi que leurs données à caractère personnel. Une attention particulière doit donc être accordée à la protection efficace de ce type de données.

En Europe, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel son consacrés par l'article 8 de la convention européenne des droits de l'homme (CEDH) et par les articles 7 et 8 de la charte des droits fondamentaux de l'UE[15]. Ces

---

[15] Il importe de noter que des principes similaires en matière de protection des données ont été définis dans des instruments internationaux relatifs à la protection de la vie privée et des données à caractère personnel, tels que: l'article 17 du pacte international relatif aux droits civils et politiques du 16 décembre 1966, les lignes directrices des Nations unies pour la réglementation des dossiers informatisés de données à caractère personnel (résolution n° 45/95 de l'Assemblée générale de l'ONU du 14 décembre 1990), la recommandation du Conseil de l'Organisation de coopération et de développement économiques concernant les lignes directrices régissant la protection de la vie privée et

droits fondamentaux s'appliquent à toute personne, quelle que soit sa nationalité ou son lieu de résidence. D'autres normes de protection des données ont été établies dans la convention n° 108 du Conseil de l'Europe de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et dans son protocole additionnel n° 181 de 2001.

Toute limitation de l'exercice des droits et libertés reconnus par la charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

Compte tenu du fait que les régimes de protection des données dans les pays tiers peuvent différer de ceux qui sont en vigueur dans l'UE, il est important que pour tout transfert de données PNR en provenance d'États membres de l'UE vers des pays tiers, ces derniers assurent un niveau adéquat de protection des données reposant sur une base juridique solide. Un tel niveau adéquat de protection des données peut être soit inscrit dans la législation du pays tiers concerné soit prévu sous la forme d'engagements juridiquement contraignants dans l'accord international régissant le traitement des données à caractère personnel.

Le caractère adéquat du niveau de protection offert par un pays tiers doit être apprécié à la lumière de l'ensemble des circonstances dans lesquelles se déroule l'opération de transfert des données. Dans ce contexte, l'UE évaluera également le respect par le pays tiers des normes internationales, en vérifiant si ce dernier a ratifié les instruments internationaux relatifs à la protection des données et aux droits fondamentaux en général. Il conviendrait de s'inspirer, afin de déterminer ce qui peut être considéré comme un niveau de protection adéquat, des décisions déjà adoptées par la Commission européenne pour constater le caractère adéquat de la protection des données.

Les principes de base que le pays tiers demandeur devrait respecter en matière de protection des données à caractère personnel sont les suivants:

- **limitation des finalités – utilisation des données:** la portée de l'utilisation des données par un pays tiers devrait être clairement et précisément définie dans l'accord et ne devrait pas dépasser ce qui est nécessaire compte tenu des objectifs à atteindre. L'expérience acquise dans le cadre des accords PNR actuels indique que les données PNR devraient être utilisées exclusivement à des fins de répression et de sécurité pour lutter contre le terrorisme et les formes graves de criminalité transnationale. Les notions clés telles que le terrorisme et les formes graves de criminalité transnationales devraient être définies sur la base de l'approche adoptée quant aux définitions dans les instruments pertinents de l'UE;
- **limitation des finalités – portée des données:** l'échange de données devrait se limiter au minimum et être proportionné. Chaque accord devrait contenir une liste exhaustive des catégories de données PNR à transférer;
- **catégories spéciales de données à caractère personnel (données sensibles):** les données PNR révélant les origines raciales ou ethniques, les opinions politiques ou les convictions religieuses ou philosophiques, l'appartenance à un syndicat, l'état de santé ou la vie sexuelle d'une personne ne seront pas utilisées, sauf dans des circonstances

---

les flux transfrontières de données à caractère personnel, et la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et le protocole additionnel à cette convention (STE n° 181), qui sont aussi ouverts à l'adhésion de pays non européens.

exceptionnelles, lorsqu'il existe un risque de mort imminent et à condition que le pays tiers fournisse les garanties requises, par exemple en veillant à ce que ces données ne puissent être utilisées qu'au cas par cas, sur autorisation d'un haut fonctionnaire et uniquement aux fins prévues pour le transfert initial;

- **sécurité des données:** les données PNR doivent être protégées contre tout abus ou accès illégal au moyen de toutes les procédures et mesures techniques appropriées permettant de prévenir les risques pour la sécurité, la confidentialité ou l'intégrité des données;
- **surveillance et responsabilité:** un dispositif de supervision par un organisme public indépendant responsable de la protection des données et jouissant de véritables pouvoirs d'intervention et de répression doit être mis en place afin d'assurer la surveillance des autorités publiques utilisant les données PNR. Ces dernières seront responsables du respect des règles établies en matière de protection des données à caractère personnel et devraient être habilitées à recevoir les plaintes des particuliers relatives au traitement de leurs données PNR;
- **transparence et information:** chaque intéressé sera informé, au minimum, de la finalité du traitement des données à caractère personnel, de l'entité qui traitera ces données, conformément à quelles règles ou dispositions législatives, des types de tiers auxquels les données seront divulguées et des voies de recours disponibles;
- **accès, rectification et suppression:** chaque intéressé aura accès à ses données PNR et jouira, le cas échéant, du droit de demander la rectification ou la suppression de ces données;
- **recours:** chaque intéressé jouira d'un droit de recours administratif ou judiciaire effectif en cas de violation de sa vie privée ou des règles de protection des données, sans discrimination fondée sur la nationalité ou le lieu de résidence. Toute infraction ou violation de ce type fera l'objet de sanctions et/ou de mesures correctrices appropriées et effectives;
- **décisions individuelles automatisées:** les décisions ayant des conséquences ou des effets négatifs sur une personne ne peuvent être fondées uniquement sur le traitement automatisé de données à caractère personnel sans intervention humaine;
- **conservation des données:** la période de conservation des données PNR ne devrait pas dépasser ce qui est nécessaire à la réalisation des tâches définies. Elle devrait tenir compte des différentes utilisations des données PNR (voir section 1.2.1 ci-dessus) et des possibilités de limiter les droits d'accès pendant sa durée, par exemple par une anonymisation progressive des données;
- **restriction des transferts ultérieurs à d'autres autorités publiques:** les données PNR ne devraient être divulguées à d'autres autorités publiques que si ces dernières disposent de pouvoirs dans le domaine de la lutte contre le terrorisme et les formes graves de criminalité transnationale et si elles offrent les mêmes protections que celles garanties par l'agence destinataire en vertu de l'accord, conformément à un engagement pris à l'égard de cette dernière. Les données PNR ne devraient jamais être divulguées en vrac, mais uniquement au cas par cas;
- **restriction des transferts ultérieurs à des pays tiers:** cette restriction concerne essentiellement l'utilisation et la diffusion ultérieure des données et vise à éviter le contournement de l'accord lorsque les données PNR sont transmises à un autre pays tiers. Ces transferts ultérieurs seront soumis à des garanties appropriées. En particulier, le pays tiers destinataire ne devrait transférer les informations en question à une autorité

compétente d'un autre pays tiers que si cette dernière s'engage à garantir le même niveau de protection des données que celui prévu dans l'accord et si le transfert est strictement limité aux finalités du transfert initial des données. Les données PNR ne devraient jamais être divulguées en vrac, mais uniquement au cas par cas.

3.3.2. Modalités de transmission

Pour garantir la sécurité juridique et réduire au minimum la charge financière imposée aux transporteurs aériens, il importe de simplifier les règles régissant la transmission des données par les transporteurs aux pays tiers. Une uniformisation des obligations permettrait de réduire fortement la charge financière pesant sur les transporteurs en diminuant les investissements que ces derniers auraient à réaliser pour remplir leurs obligations. À cette fin, il serait souhaitable que les modalités de transmission suivantes, au minimum, soient normalisées:

- **la méthode de transmission**: pour protéger les données contenues dans les bases de données des transporteurs et pour en conserver le contrôle, les données devraient être transmises exclusivement à l'aide du système «push»;
- **la fréquence de transmission**: une limite raisonnable devrait être fixée au nombre de fois qu'un pays tiers peut demander que les données lui soient transmises, afin d'assurer un degré de sécurité adéquat tout en minimisant les coûts pour les transporteurs;
- **absence d'obligation pour les transporteurs de collecter des données supplémentaires**: les transporteurs ne devraient pas être tenus de collecter davantage de données que ce qu'ils recueillent déjà, ou de collecter certains types de données, mais uniquement de transmettre les données qu'ils collectent déjà dans le cadre de leurs activités.

3.3.3. Concepts généraux

- **Durée et réexamen:** les conditions de la coopération avec les pays tiers devraient être valables pour une durée déterminée et devraient prévoir la possibilité pour chacune des parties de dénoncer l'accord. Il devrait être possible de réexaminer les conditions de la coopération si cela est jugé opportun.
- **Surveillance:** il est essentiel que l'UE soit dotée de mécanismes lui permettant de surveiller le bon déroulement de la mise en œuvre, tels que des réexamens conjoints réguliers de l'application des accords qui porteraient notamment sur la limitation des finalités, les droits des passagers et les transferts ultérieurs de données PNR, et comprenant une évaluation du caractère proportionné des données conservées au regard des finalités pour lesquelles elles ont été transférées. Les conclusions de ces réexamens conjoints devraient être présentées au Conseil et au Parlement européen.
- **Résolution des litiges**: des mécanismes efficaces de résolution des litiges relatifs à l'interprétation, à l'application et la mise en œuvre des accords devraient être prévus.
- **Réciprocité:** la réciprocité devrait être assurée, notamment par le transfert des informations analytiques tirées des données PNR par les autorités compétentes du pays tiers destinataire aux autorités policières et judiciaires des États membres, ainsi qu'à Europol et à Eurojust.

4. PERSPECTIVE A LONG TERME

Vu le nombre croissant de pays dans le monde qui utilisent les données PNR, les questions que soulève cette utilisation concernent désormais la communauté internationale. Même si l'approche bilatérale adoptée jusqu'à présent par l'UE était la plus appropriée, compte tenu des circonstances, et semble rester la plus adaptée pour les années à venir, elle risque de devenir

caduque si le nombre de pays utilisant les données PNR augmente encore de façon sensible. L'UE devrait donc envisager la possibilité d'établir des normes pour la transmission et l'utilisation de données PNR au niveau international. Les lignes directrices relatives à l'accès aux données PNR qui ont été élaborées par l'OACI en 2004 fournissent une base solide pour l'harmonisation des modalités de transmission des données PNR. Toutefois, ces lignes directrices ne sont pas contraignantes et n'abordent pas de manière exhaustive les questions de protection des données. Elles ne sauraient donc suffire en soi, mais devraient plutôt servir à indiquer la marche à suivre, notamment pour les questions qui concernent les transporteurs.

Dès lors, l'UE devrait envisager d'entamer des discussions avec ses partenaires internationaux qui utilisent les données PNR et avec ceux qui y songent, afin de déterminer si un terrain d'entente peut être trouvé à un niveau multilatéral en ce qui concerne le traitement des transferts PNR. Si ces discussions aboutissent, l'UE devrait officiellement entrer en négociation avec les partenaires internationaux intéressés en vue d'aboutir à une solution multilatérale.

5. CONCLUSION

La présente communication présente une vue d'ensemble des tendances actuelles en matière d'utilisation des données PNR dans l'UE et dans le monde. En réponse à ces tendances, ainsi qu'aux menaces qui continuent de peser sur l'UE et le reste du monde, la Commission a estimé nécessaire que l'UE revoie sa démarche globale en matière de données PNR. Ce faisant, la Commission a tenu compte des points de vue des principaux intervenants concernant les questions générales relatives aux données PNR, ainsi que des principes d'élaboration des politiques énoncés dans la présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice.

La présente communication présente pour la première fois une série de considérations générales qui devraient guider l'UE lors de la négociation d'accords PNR avec les pays tiers. Le respect de ces principes devrait assurer davantage de cohérence entre les divers accords PNR, tout en garantissant le respect des droits fondamentaux au respect de la vie privé et à la protection des données à caractère personnel. Dans le même temps, la présente communication reste suffisamment ouverte pour pouvoir être adaptée en fonction des préoccupations en matière de sécurité et de l'ordre juridique national de chaque pays tiers.

Enfin, en envisageant le développement des politiques PNR dans le monde à plus long terme, la communication conclut que l'UE devrait étudier la possibilité de remplacer, à moyen terme, les accords bilatéraux par un accord multilatéral entre tous les pays qui utilisent les données PNR.