Utilisation des données des dossiers passagers (passenger name record - PNR) à des fins répressives

2007/0237(CNS) - 06/11/2007 - Document de base législatif

OBJECTIF : harmoniser les dispositions des États membres relatives à l'obligation de transmission et d' utilisation des données relatives aux passagers (ou données « PNR » - données des dossiers passagers) afin de prévenir et de combattre le terrorisme et la criminalité organisée.

ACTE PROPOSÉ : Décision-cadre du Conseil.

CONTEXTE : le terrorisme constitue actuellement une des plus grandes menaces pour la sécurité, la paix, la stabilité, la démocratie et les droits fondamentaux dans l'Union et une menace directe pour ses citoyens. Depuis le 11 septembre 2001, les autorités répressives du monde entier ont pu se rendre compte de la valeur ajoutée apportée par la collecte et l'analyse des données PNR dans le cadre de la lutte contre le terrorisme et la criminalité organisée. Ces données concernent en particulier les déplacements, habituellement par voie aérienne, des passagers et permettent l'identification des passagers à haut risque par les autorités répressives, qui peuvent ainsi prendre les mesures appropriées.

Jusqu'à présent, seuls quelques États membres ont adopté une législation visant à instaurer des mécanismes pour contraindre les transporteurs aériens à fournir les données PNR et permettre l'analyse de ces données par les autorités compétentes (l'expérience acquise par un projet pilote de ce type au Royaume-Uni a montré l'important bénéfice des opérations menées pour identifier des réseaux de traite d' êtres humains et obtenir de précieux renseignements concernant le terrorisme). Parallèlement, des accords en matière de transmission de données PNR dans le cadre de la lutte contre le terrorisme et la criminalité transnationale ont été conclus entre l'UE et les États-Unis et le Canada, en vertu desquels les transporteurs aériens qui enregistraient déjà les données PNR pour leur propre usage commercial, étaient tenus de les transmettre aux autorités compétentes américaines et canadiennes (voir CNS/2005/0095 pour accord UE-Canada et CNS/2004/0064 pour accord UE-USA sur la transmission des données « PNR »).

Dans ce contexte, le Conseil européen de mars 2004 a estimé que l'Union devait bénéficier d'un programme européen d'échanges et de transmission des données « PNR » et a invité la Commission à soumettre une proposition allant dans le sens en vue de déterminer une approche commune de l'UE dans l' utilisation des données passagers à des fins répressives. C'est l'objet de la présente proposition de décision-cadre.

CONTENU :

Chapitre I : Objectifs et dispositions générales : l'objectif général de la proposition est d'harmoniser les dispositions des États membres relatives à l'obligation, pour les transporteurs aériens assurant des vols vers le territoire d'au moins un État membre ou à partir de celui-ci, de transmettre aux autorités compétentes les renseignements relatifs aux passagers, aux fins de prévenir et de combattre les infractions terroristes et la criminalité organisée. Tout traitement des données PNR en vertu de la proposition sera régi par la future décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (voir CNS/2005/0202).

Les données « PNR » (« *Passenger Name Record* ») concernées sont énoncées dans une liste figurant à l' annexe de la proposition et portent sur:

1. **Données relatives à tous les passagers** : code du dossier passager (PNR) ; date de réservation /d'émission du billet ; date(s) prévue(s) du voyage ; nom(s) ; adresse et contact (numéro de téléphone, adresse électronique) ; moyens de paiement, y compris adresse de facturation ; itinéraire complet pour le PNR concerné ; profil de client fidèle ; agence de voyage/agent de voyage ; statut du voyageur (confirmations, enregistrement, non-présentation ou passager de dernière minute sans réservation) ; PNR scindé/divisé ; remarques générales (à l'exclusion de toute information sensible) ; établissement des billets (numéro du billet, date d'émission, billets aller simple, champs des billets informatisés) ; numéro du siège ; partage de codes ; bagages ; nombre et autres noms de voyageurs figurant dans le PNR ; informations API éventuellement collectées (renseignements préalables concernant les passagers) ; historique complet des modifications des PNR ;
2. **Données complémentaires relatives aux mineurs de moins de 18 ans non accompagnés** : nom et sexe de l'enfant ; âge ; langue(s) parlée(s) ; nom et contact de l'accompagnateur et lien avec l'enfant (au départ et à l'arrivée) ; agent au départ et à l'arrivée.

Chapitre II : Responsabilités :

1. incombant aux États membres : les État membre devront désigner une autorité compétente («unité de renseignements passagers») chargée de collecter auprès des transporteurs aériens (ou de leurs intermédiaires) les données PNR relatives aux vols internationaux qui ont pour point d'arrivée ou de départ le territoire des États membres. Si ces données contiennent des données supplémentaires par rapport à la liste décrite ci-avant ou des données à caractère personnel susceptibles de révéler de la race, l' origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou des données relatives à la santé ou à la vie sexuelle de la personne concernée, l'unité de renseignements passagers devra les effacer immédiatement. L'unité devra en outre analyser ces données en vue d'évaluer le risque potentiel de certaines personnes au vu des données recueillies (les critères et garanties relatifs à l'évaluation des risques seront fixés au plan national).

Aucune action coercitive ne pourra être engagée directement par l'unité de renseignements sur la seule base du traitement automatisé des données PNR (ou en raison de la race, l'origine ethnique,… de la personne analysée). L'unité devra uniquement transmettre ces données aux autorités compétentes (dont une liste devra être dressée dans chaque État membre) lesquelles prendront les mesures qui s'imposent pour prévenir ou combattre les infractions terroristes et la criminalité organisée.

Ces **unités de renseignements nationales** seront en particulier chargées de :

- identifier les personnes qui sont ou pourraient être impliquées dans une infraction terroriste ou dans un crime organisé,
- créer des indicateurs de risque en vue d'évaluer le risque potentiel de ces personnes,
- fournir des renseignements sur les schémas de déplacement et autres tendances des personnes analysées en lien avec des infractions terroristes et la criminalité organisée,
- utiliser les données collectées dans le cadre des enquêtes et des poursuites criminelles relatives à des infractions terroristes et à la criminalité organisée.

2. incombant aux transporteurs aériens : les transporteurs aériens auront l'obligation mettre à la disposition les données PNR collectées auprès des unités désignées, 24 heures avant le départ programmé du vol ou immédiatement après la clôture du vol (et dans certains cas, plus de 24 heures avant le départ du vol lorsqu'il existe des indices qu'un accès précoce à ces données serait susceptible de répondre à une menace). Des dispositions spécifiques sont prévues pour les transporteurs aériens dont les bases de données PNR ne sont pas établies dans un État membre de l'Union européenne.

Intermédiaires : la proposition de décision-cadre prévoit que les transporteurs aériens qui le souhaitent puissent désigner un « intermédiaire » chargé de mettre les données PNR des passagers à la disposition des unités nationales, à leur place. Ces intermédiaires ne pourraient en aucun cas traiter les données

collectées à d'autres fins que celles de la transmission à l'unité responsable, et une fois l'information transmise, celle-ci devrait immédiatement être effacée des bases de données des intermédiaires.

Des **sanctions** sont prévues contre les transporteurs aériens et les intermédiaires qui ne transmettraient pas les données ou les transmettraient de manière incomplète ou erronée (pouvant aller, dans les cas répétés, jusqu'à la suspension temporaire de la licence d'exploitation aérienne ou son retrait).

La décision-cadre fixe en outre le cadre général pour :

- les échange d'informations entre unités nationales de renseignements : les informations collectées par une unité de renseignements pourront être transmises aux autres unités nationales habilitées, à la seule fin de prévenir et de combattre les infractions terroristes et la criminalité organisée ;
- la communication de données à des pays tiers : les données PNR pourront également être communiquées par un État membre aux autorités répressives de pays tiers **uniquement** à condition que cet État membre ait l'assurance que les autorités du pays tiers n'utilisent les données que pour prévenir et combattre les infractions terroristes et la criminalité organisée, et à la condition expresse que ce pays tiers ne transmette pas ces mêmes données à un autre pays tiers.

Période de rétention des données : les données PNR transmises par les transporteurs aériens ou leurs intermédiaires à l'unité de renseignements devront être conservées dans une base de données pendant **5 ans** (par l'unité de renseignement). Après ce laps de temps, les données seront conservées pour une **période supplémentaire de 8 années** (période pendant laquelle l'accès, le traitement et l'utilisation des données PNR ne pourra se faire qu'avec le consentement de l'autorité compétente et uniquement dans des circonstances exceptionnelles en réponse à une menace ou un risque réel). Les données seraient ensuite définitivement effacées (sauf si les données sont justement utilisées dans le cadre d'une enquête criminelle en cours pour une infraction terroriste ou relevant de la criminalité organisée).

Chapitre III – protection des données à caractère personnel : le projet de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (en cours d'adoption – voir CNS/2005/0202) s'appliquera aux traitements de données à caractère personnel de la présente décision-cadre.

Outre la réaffirmation que les données ne peuvent être utilisées que pour prévenir, détecter, investiguer et poursuivre les infractions terroristes ou liées à la criminalité organisée, la décision-cadre prévoit un certain nombre de dispositions pour **sécuriser** la transmission des données PNR (en prévoyant notamment une série de mesures techniques destinées à limiter l'accès aux données aux seules personnes habilitées et à en crypter la lecture aux fins de protection).

Chapitre IV - Protocoles communs de cryptage : ce chapitre est consacré à la mise en commun des méthodes de cryptage des données transmises.au terme d'un période test pendant laquelle les États membres seraient invités à trouver des solutions de sécurisation commune des données durant leur transmission. Des modalités spécifiques de comitologie sont prévues à cet effet.

Chapitre V – Dispositions finales: il est prévu que le projet de décision-cadre soit transposé en droit national pour le 31 décembre 2010. Une clause de réexamen est prévue 3 ans après son entrée en vigueur. Il est également prévu que les États membre effectuent des statistiques sur les données PNR communiquées aux unités de renseignements passagers.