

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

2011/0023(COD) - 07/09/2015 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission des libertés civiles, de la justice et des affaires intérieures a adopté le deuxième rapport de Timothy KIRKHOPE (ECR, UK) sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers (données PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

La commission parlementaire a recommandé que la position du Parlement européen, adoptée en première lecture suivant la procédure législative ordinaire, modifie la proposition de la Commission comme suit.

Objet et champ d'application : la directive devrait avoir pour objet de garantir la sécurité, de protéger la vie de la population en veillant à sa sûreté, et d'établir un cadre juridique pour la protection et l'échange de données PNR entre les États membres et les services répressifs.

La directive prévoirait le transfert, par **les transporteurs aériens et les opérateurs économiques autres que les transporteurs aériens**, tels que les agences et les organisateurs de voyages, des données des dossiers des passagers de **vols internationaux à destination et en provenance des États membres**, ainsi que le traitement de ces données, et leur échange entre lesdits États et entre les États membres et l'Union européenne. Les vols intérieurs ne seraient pas couverts.

Infractions couvertes : selon les règles modifiées, les données PNR pourraient être traitées uniquement pour la prévention et la détection **d'infractions terroristes et certains types d'infractions transnationales graves**, ainsi que la réalisation d'enquêtes et de poursuites en la matière. La liste approuvée par les députés inclut, par exemple, la traite d'êtres humains, l'exploitation sexuelle des enfants, le trafic de drogues, le trafic d'armes, de munitions et d'explosifs, le blanchiment d'argent et la cybercriminalité.

Les «**infractions terroristes**» sont définies comme les infractions en droit national visées à la [décision-cadre 2002/475/JAI du Conseil](#), y compris les personnes susceptibles de voyager dans le dessein de commettre, d'organiser ou de préparer des actes de terrorisme, ou afin d'y participer ou de dispenser ou recevoir un entraînement au terrorisme.

Unité de renseignements passagers : l'unité de renseignements passagers serait chargée :

- de la collecte des données PNR auprès des transporteurs aériens et des autres opérateurs économiques, de la conservation, du traitement et de l'analyse de ces données et de la transmission des résultats des analyses aux autorités compétentes ;
- de l'échange des données PNR et du résultat de leur traitement avec les unités de renseignements passagers d'autres États membres et avec Europol.

Les unités de renseignements sur les passagers des États membres seraient autorisées à traiter les données PNR **seulement à des fins limitées**, telles que l'identification d'un passager qui pourrait être impliqué dans une infraction terroriste ou une infraction transnationale grave et qui exige un examen complémentaire. Elles devraient **nommer un délégué à la protection des données** chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties correspondantes.

Traitement des données PNR : l'application de la directive devrait être dûment justifiée et les **garanties nécessaires** devraient être mises en place afin d'assurer la légalité de tout stockage, de toute analyse, de tout transfert et de toute utilisation des données PNR.

Lors de l'évaluation du risque présenté par un passager, l'unité de renseignements passagers pourrait **confronter les données PNR au système d'information Schengen et au système d'information sur les visas**.

Les critères d'évaluation devraient être **ciblés, spécifiques, motivés, proportionnés et fondés sur des faits**. Ils ne devraient en aucun cas être fondés sur des données qui révèlent la race ou l'origine ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'orientation sexuelle ou l'identité de genre, l'appartenance à un syndicat ou les activités syndicales de la personne, ni le traitement de données qui concernent la santé ou la vie sexuelle.

Les passagers devraient être **informés du type de données** à caractère personnel qui sont collectées à des fins répressives, ainsi que de leurs droits sur leurs données en tant que passagers.

Période de conservation des données et système de masquage: les données PNR transférées par les transporteurs aériens et les non-transporteurs seraient conservées dans l'unité de renseignements sur les passagers nationale pour une période initiale de 30 jours, après laquelle tous les éléments des données qui pourraient servir à identifier le passager devraient être «**masqués**», pour être ensuite conservées jusqu'à cinq ans.

L'accès à l'intégralité des données serait autorisé pour une période de **quatre ans** après le masquage des données dans le cas d'infractions transnationales graves, et pour une période de **cinq ans** dans le cas d'infractions terroristes.

Après ces cinq années, les données PNR devraient être **effacées de manière définitive**, à moins que les autorités compétentes ne les utilisent pour des enquêtes ou des poursuites pénales spécifiques (dans ce cas, la conservation des données serait régie par le droit national de l'État membre concerné).

Les États membres assumeraient les coûts liés à l'utilisation, à la conservation et à l'échange de données PNR. Toutes les données détenues par les transporteurs aériens et par les non transporteurs devraient être **stockées dans une base de données sécurisée** dans un système informatique de sécurité homologué.

Conditions de consultation des données PNR par Europol : Europol pourrait présenter, au cas par cas, à l'unité de renseignements passagers de tout État membre, une demande électronique dûment motivée de transfert de données PNR précises lorsque cela est strictement nécessaire afin de soutenir et renforcer l'action des États membres en vue de prévenir et de détecter une infraction terroriste spécifique ou une infraction transnationale grave, ou de mener des enquêtes en la matière.

Les échanges d'information se feraient dans ce cas par l'intermédiaire du **réseau SIENA** et conformément à la décision 2009/371/JAI.

Protection des données à caractère personnel : les unités de renseignements passagers devraient :

- i) conserver une **trace documentaire** de tous les systèmes et procédures de traitement sous leur

responsabilité ; ii) garantir un **niveau maximal de sécurité** adapté aux risques présentés par le traitement et à la nature des données PNR à protéger ; iii) informer la personne concernée au sujet de ses **droits** et des modalités d'exercice de ces droits.

L'autorité de contrôle devrait tenir des **registres** au moins pour les opérations de traitement suivantes: la collecte, l'altération, la consultation, la communication, l'interconnexion ou l'effacement. En outre, les personnes qui ont accès aux données PNR et les analysent, et tiennent les données journalisées, devraient avoir **l'habilitation de sécurité nécessaire** et être formées dans ce domaine.