

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) - 14/04/2016 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 461 voix pour, 179 contre et 9 abstentions, une résolution législative 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 position du Parlement européen, adoptée en première lecture suivant la procédure législative ordinaire, a modifié la proposition de la Commission comme suit :

Objet et champ d'application : la directive aurait pour objet, entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes. Elle prévoirait:

- **le transfert**, par les transporteurs aériens, de données des dossiers des passagers (PNR) de **vols extra-UE**,
- **le traitement des données**, notamment leur collecte, leur utilisation et leur conservation par les États membres et leur échange entre les États membres.

Les données PNR recueillies pourraient être traitées **uniquement à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière**.

Lorsqu'un vol extra-UE comporte une ou plusieurs escales dans des aéroports des États membres, les transporteurs aériens seraient tenus de transférer les données PNR de tous les passagers aux UIP de tous les États membres concernés.

Les États membres pourraient décider **d'appliquer la directive aux vols intra-UE** (c'est-à-dire d'un État membre à l'autre sans escale dans un pays tiers) à condition d'en informer la Commission par écrit.

Unité d'informations passagers (UIP): chaque État membre devrait créer une «unité de renseignements sur les passagers» chargée :

- de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement ;
- de l'échange à la fois des données PNR et du résultat de leur traitement avec les UIP d'autres États membres et avec **Europol**.

Délégué à la protection des données au sein de l'UIP : l'UIP devrait nommer un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes. Toute personne concernée aurait le droit de s'adresser au délégué à la protection des données,

en sa qualité de point de contact unique, pour toutes les questions relatives au traitement des données PNR la concernant.

Traitement des données : l'UIP ne pourrait traiter les données PNR que pour réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci. Cette évaluation aurait pour finalité d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes et, le cas échéant, par Europol, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

Lorsqu'il réalise cette évaluation, l'UIP pourrait: a) **confronter les données PNR aux bases de données utiles** aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière et b) traiter les données PNR au regard de critères préétablis.

Le délégué à la protection des données devrait avoir accès à toutes les données traitées par l'UIP et pourrait, s'il estime que traitement de certaines données n'était pas licite, renvoyer l'affaire à l'autorité de contrôle nationale. Le stockage, le traitement et l'analyse des données PNR par les UIP devraient être effectués exclusivement dans un ou des endroits **sécurisés** situés sur le territoire des États membres.

Les conséquences des évaluations des passagers ne devraient **pas compromettre le droit d'entrée des personnes jouissant du droit de l'Union à la libre circulation** sur le territoire de l'État membre concerné prévu dans la directive 2004/38/CE du Parlement européen et du Conseil.

Conditions d'accès aux données PNR par Europol : selon le texte amendé, Europol pourrait présenter, au cas par cas, à l'UIP de tout État membre par l'intermédiaire de l'unité nationale Europol, une **demande électronique motivée** de transmission de données PNR spécifiques ou du résultat du traitement de ces données. Cette demande pourrait être présentée lorsque cela est **strictement nécessaire** au soutien et au renforcement de l'action des États membres en vue de prévenir une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes en la matière.

Transfert de données vers des pays tiers : les transferts de données PNR sans l'accord préalable de l'État membre dont les données ont été obtenues, ne devraient être autorisés que dans des circonstances exceptionnelles et uniquement : a) si ces transferts sont essentiels pour répondre à une menace précise et réelle liée à une infraction terroriste ou à une forme grave de criminalité dans un État membre ou un pays tiers, et b) si l'accord préalable ne peut pas être obtenu en temps utile.

Période de conservation et dépersonnalisation des données : les données PNR fournies par les transporteurs aériens devraient être conservées dans une base de données pendant une période de **cinq ans** suivant leur transfert à l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol.

À l'expiration d'une période de six mois suivant le transfert des données PNR, toutes les données PNR devraient être **dépersonnalisées par le masquage des éléments des données pouvant servir à identifier directement le passager** tels que le nom, l'adresse et les coordonnées, mais également les informations sur tous les modes de paiement, y compris l'adresse de facturation, ou les informations «grands voyageurs».

À l'expiration de cette période de six mois, la communication de l'intégralité des données PNR **ne serait autorisée que:** a) lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire ; b) lorsqu'elle a été approuvée par une autorité judiciaire ou une autre autorité nationale compétente en vertu du droit national, et à condition que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post.

Protection des données à caractère personnel : selon le texte amendé, l'UIP devrait conserver une **trace documentaire** relative à tous les systèmes et procédures de traitement sous leur responsabilité.

L'UIP devrait tenir des **registres** au moins pour les opérations de traitement suivantes: la collecte, la consultation, la communication et l'effacement. Les registres des opérations de consultation et de communication devraient indiquer, en particulier, la finalité, la date et l'heure de ces opérations et, dans la mesure du possible, l'identité de la personne qui a consulté ou communiqué les données PNR, ainsi que l'identité des destinataires de ces données. Ces registres devraient être conservés pendant **cinq ans**.

Il serait **explicitement interdit** de traiter des données à caractère personnel révélant l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

Réexamen : la Commission devrait réexaminer tous les éléments de la directive **quatre ans** après son entrée en vigueur. Elle devrait accorder une attention particulière au respect des normes de protection des données à caractère personnel, à la nécessité et la proportionnalité de la collecte et du traitement des données pour chacun des objectifs énoncés, à la durée de conservation des données, ainsi qu'à l'efficacité du partage des données entre les États membres.