

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) - 02/02/2011 - Document de base législatif

OBJECTIF : prévoir un cadre juridique pour 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.

ACTE PROPOSÉ : Directive du Parlement européen et du Conseil

CONTEXTE : 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 répressives. 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 ont permis de dégager un **consensus sur la plupart de ses dispositions**.

Lors de l'entrée en vigueur du traité sur le fonctionnement de l'Union européenne (TFUE) le 1^{er} décembre 2009, la proposition de 2007, non encore adoptée par le Conseil, est devenue obsolète. La présente proposition remplace dès lors 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 2008](#) et 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 données.

Sur le fond, la proposition répond à une demande de coopération accrue de la part des États membres suite à l'augmentation drastique de la grande criminalité et de la criminalité organisée depuis une dizaine d'années. Pour contrer la menace criminelle mais aussi la menace terroriste et par suite de la suppression des contrôles aux frontières intérieures, l'UE a déjà adopté des nombreuses mesures organisant la collecte de données à caractère personnel et l'échange de celles-ci entre les services répressifs et d'autres autorités (en particulier, échanges de données sur les personnes déjà suspectées ou «connues» des services de police, avec le SIS II ou le VIS).

Toutefois, la Commission a déjà, à maintes reprises, souligné la nécessité d'accroître encore 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 PNR à des fins répressives, approche également appuyée par [le programme de Stockholm](#).

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 et que les services répressifs peuvent utiliser de plusieurs manières. Une collecte, une utilisation et une conservation plus systématiques des données PNR, sous réserve de garanties strictes pour leur protection, permettraient d'intensifier la prévention et la détection des infractions terroristes ou graves, ainsi que les enquêtes et les poursuites en la matière.

Sachant que l'utilisation des données PNR n'est pas réglementée au niveau de l'UE, il convient **d'harmoniser les dispositions des États membres** afin de faire 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. La proposition n'exigera cependant 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.

Afin d'assurer le respect du principe de proportionnalité, la proposition a par conséquent une portée soigneusement limitée et contient des garanties strictes en matière de protection des données.

ANALYSE D'IMPACT : la Commission a effectué une analyse d'impact du projet de directive qui comporte **4 options** principales dont chacune inclut deux variantes :

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,
- 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,
- selon **l'option D.2**: transporteurs aériens, maritimes et ferroviaires.

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. 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.

BASE JURIDIQUE : article 82, par. 1, point d), et article 87, par. 2, point a) du traité sur le fonctionnement de l'Union européenne (TFUE).

CONTENU : le projet de directive comporte plusieurs chapitres qui peuvent se résumer comme suit :

Chapitre I : Objectifs et champ d'application: 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 proposition seraient conformes aux règles de protection des données énoncées dans la [décision-cadre 2008 /977/JAI](#).

Les données « PNR » (« *Passenger Name Record* ») concernées seront celles figurant à l'annexe de la proposition. Elles portent notamment sur les données relatives à tous les passagers telles que : code repère du dossier passager (PNR) ; date de réservation/d'émission du billet ; date(s) prévue(s) du voyage ; nom (s) ; adresse et coordonnées (numéro de téléphone, adresse électronique) ; moyens de paiement ; etc. Parmi les données on relèvera également des données spécifiques ou « remarques générales » portant sur des informations disponibles sur les mineurs non accompagnés de moins de 18 ans. Ce type de données inclura en particulier des informations sur le nom et les coordonnées du tuteur présent au départ et/ou à l'arrivée du mineur.

Chapitre II : Responsabilités :

1. incombant aux États membres : les États membres devront désigner une autorité compétente («**unité de renseignements passagers**») chargée de collecter les données auprès des transporteurs aériens, de les conserver, de les analyser et de transmettre les résultats des analyses aux autorités compétentes. Si ces données contiennent des données supplémentaires par rapport à la liste décrite ci-avant ou des données à caractère personnel susceptibles de révéler 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 devra les effacer immédiatement.

L'unité devra notamment évaluer le risque potentiel de certaines personnes au vu des données recueillies et réagir, au cas par cas, aux demandes motivées d'autorités compétentes. L'évaluation du risque devra être réalisée de façon non discriminatoire au regard des critères d'évaluation définis par l'unité de renseignements et sans faire intervenir des critères fondés sur la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, etc.

L'unité devra uniquement transmettre ces données aux **autorités compétentes** lesquelles prendront les mesures qui s'imposent pour prévenir ou combattre les infractions terroristes et la criminalité organisée. Le résultat du traitement des données ne pourra 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.

2. incombant aux transporteurs aériens : les transporteurs aériens auront l'obligation de transférer les données par voie électronique au moyen des protocoles communs et de formats de données reconnus aux unités désignées (méthode *push*) : i) **24 à 48 heures avant le départ programmé du vol**; et ii) **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. Dans un 2^{ème} temps, les unités de renseignements des États membres devront transmettre ces données ou le résultat du traitement de ces données aux autorités compétentes d'autres États membres, dans le cadre d'un échange d'informations, **si ces unités considèrent que ce transfert est nécessaire** pour prévenir ou détecter des infractions graves ou terroristes. Une procédure spécifique de demande de renseignement sur un PNR spécifique est également prévue, notamment en cas de menace grave et immédiate.

Transfert de données vers des pays tiers : il est clairement établi qu'un État membre ne pourra transférer à un pays tiers des données PNR et les résultats du traitement de telles données que dans des cas strictement limités prévus à proposition de directive. Ces transferts sont strictement limités et autorisés à la condition expresse que les autorités des pays tiers concernés n'utilisent ces données que pour prévenir et combattre les infractions terroristes et la criminalité organisée.

Durée de conservation des données : les données PNR transmises par les transporteurs aériens à l'unité de renseignements devront être conservées dans une base de données pendant 30 jours. À l'expiration de ce délai, les données seront conservées pendant une **période supplémentaire de 5 ans** (par l'unité de renseignement). Durant cette période, **les données seront anonymisées** de sorte à ne pas identifier le passager auquel se rapportent les données PNR. Ces données ne seraient en outre accessibles qu'à un nombre limité d'employés de l'unité de renseignements. 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. Dans ce dernier cas, la conservation des données par l'autorité compétente sera régie par le droit interne de l'État membre concerné.

Sanctions : des sanctions sont prévues contre les transporteurs aériens qui ne transmettraient pas les données ou les transmettraient de manière incomplète ou selon un mauvais format.

Protection des données à caractère personnel : [la 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 s'appliquera aux traitements de données à caractère personnel de la présente directive.

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 proposition de directive prévoit un certain nombre de dispositions pour :

- interdire tout traitement de données PNR révélant de la race ou de 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 ;
- interdire tout transfert de données PNR par les unités de renseignements et les autorités compétentes à des personnes privées établies dans un État membre ou un pays tiers ;
- assurer la traçabilité du traitement de données PNR à des fins de vérification de la licéité du traitement des données, d'autocontrôle et de garantie de l'intégrité et de la sécurité des données ;
- assurer la transparence de l'information aux passagers de la part des transporteurs aériens, agents ou autres vendeurs de billets sur la communication des données PNR à l'unité de renseignements passagers, la finalité du traitement de ces données, la durée de conservation des données, et l'éventuelle utilisation de celles-ci ainsi que le droit de déposer plainte auprès de l'autorité nationale de contrôle de la protection des données ;
- prévoir des sanctions effectives, proportionnées et dissuasives en cas de violation des dispositions adoptées en application de la directive.

Chapitre IV – Mesures de mise en œuvre : ce chapitre est consacré à la mise en commun des méthodes de cryptage des données transmises vers les unités de renseignements passagers. À l'issue d'une 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 se feraient par voie électronique à l'aide de **méthodes sécurisées utilisant des protocoles communs acceptés**, identiques pour tous les transferts. La Commission dresserait la liste des protocoles communs acceptés et des formats de données reconnus. Des modalités techniques de comitologie sont prévues à cet effet.

Chapitre V – Dispositions finales: il est prévu que la proposition de directive soit transposée en droit national dans les 2 ans qui suivent son entrée en vigueur. La proposition fera l'objet d'une **période transitoire** sous la forme d'un délai de mise en œuvre de 2 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 6 ans à compter de l'entrée en vigueur de la directive.

Une clause de **réexamen** du fonctionnement de la directive est également prévue dans les 4 ans qui suivent sa 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. Il est également prévu que les États membre effectuent des statistiques sur les données PNR communiquées aux unités de renseignements passagers.

Application territoriale : 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 TFUE.

INCIDENCE BUDGÉTAIRE : la proposition n'a pas d'incidence sur le budget de l'UE.