Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Directive	2011/0023(COD)	Procédure terminée
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 Voir aussi 2011/0126(NLE) Voir aussi 2011/0382(NLE) Sujet 1.20.09 Protection de la vie privée et des données 3.20.01.01 Sécurité aérienne 7.10.04 Franchissement et contrôles aux frontières extérieures, visas 7.30 Coopération policière, judiciaire et douanière en général 7.30.20 Lutte contre le terrorisme 7.30.30 Lutte contre la criminalité		

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
LIBE Libertés civiles, justice et affaires intérieures	ECR KIRKHOPE Timothy	15/07/2014

Commission au fond précédente

LIBE Libertés civiles, justice et affaires intérieures

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
AFET Affaires étrangères	epp DANJEAN Arnaud	13/01/2015
TRAN Transports et tourisme	CRAMER Michael	17/03/2015

Commission pour avis précédente

TRAN Transports et tourisme

AFET Affaires étrangères

Conseil de l'Union européenne

Formation du Conseil	Réunion	Date
Justice et affaires intérieures(JAI)	3433	04/12/2015
Justice et affaires intérieures(JAI)	3415	09/10/2015
Justice et affaires intérieures(JAI)	3354	05/12/2014
Justice et affaires intérieures(JAI)	3162	26/04/2012

Commission européenne	Justice et affaires intérieures(JAI)	3081	11/04/2011
	DG de la Commission	Commissaire	
	Migration et affaires intérieures	MALMSTRÖM Cecilia	

Evénements clés

02/02/2011	Publication de la proposition législative	COM(2011)0032	Résumé
14/02/2011	Annonce en plénière de la saisine de la commission, 1ère lecture		
11/04/2011	Débat au Conseil	3081	Résumé
26/04/2012	Débat au Conseil	3162	Résumé
29/04/2013	Dépôt du rapport de la commission, 1ère lecture	A7-0150/2013	Résumé
10/06/2013	Décision du Parlement, 1ère lecture		Résumé
20/10/2014	Annonce en plénière de la saisine de la commission, 1ère lecture		
05/12/2014	Débat au Conseil	3354	
15/07/2015	Vote en commission,1ère lecture		
15/07/2015	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d?un rapport adopté en commission		
06/09/2015	Dépôt du rapport de la commission, 1ère lecture	A8-0248/2015	
09/10/2015	Débat au Conseil	3415	Résumé
10/12/2015	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture		
13/04/2016	Débat en plénière		
14/04/2016	Résultat du vote au parlement		
14/04/2016	Décision du Parlement, 1ère lecture	T8-0127/2016	Résumé
18/04/2016	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
27/04/2016	Signature de l'acte final		
27/04/2016	Fin de la procédure au Parlement		
04/05/2016	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de procédure	2011/0023(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Directive

	Voir aussi 2011/0126(NLE) Voir aussi 2011/0382(NLE)
Base juridique	Traité sur le fonctionnement de l'UE TFEU 087-p2; Traité sur le fonctionnement de l'UE TFEU 082-p1
Etape de la procédure	Procédure terminée
Dossier de la commission parlementaire	LIBE/8/00066

Portail de documentation

Document de base législatif		COM(2011)0032	02/02/2011	EC	Résumé
Document annexé à la procédure		SEC(2011)0132	02/02/2011	EC	
Document annexé à la procédure		SEC(2011)0133	02/02/2011	EC	
Document annexé à la procédure		N7-0062/2011 JO C 181 22.06.2011, p. 0024	25/03/2011	EDPS	Résumé
Comité économique et social: avis, rapport		CES0803/2011	05/05/2011	ESC	
Rapport déposé de la commission, 1ère lecture/lecture unique		A7-0150/2013	29/04/2013	EP	Résumé
Projet de rapport de la commission		PE549.223	17/02/2015	EP	
Amendements déposés en commission		PE554.742	20/04/2015	EP	
Amendements déposés en commission		PE554.743	20/04/2015	EP	
Amendements déposés en commission		PE554.744	20/04/2015	EP	
Avis de la commission	TRAN	PE467.175	29/04/2015	EP	
Avis de la commission	AFET	PE549.344	06/05/2015	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A8-0248/2015	07/09/2015	EP	
Document annexé à la procédure		N8-0115/2015 JO C 392 25.11.2015, p. 0011	24/09/2015	EDPS	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T8-0127/2016	14/04/2016	EP	Résumé
Projet d'acte final		00071/2015/LEX	27/04/2016	CSL	
Réaction de la Commission sur le texte adopté en plénière		SP(2016)372	31/05/2016	EC	
Document de suivi		SWD(2016)0426	28/11/2016	EC	Résumé
Document de suivi		COM(2020)0305	24/07/2020	EC	
Document de suivi		SWD(2020)0128	24/07/2020	EC	
Document de suivi		SWD(2021)0304	21/10/2021	EC	

Informations complémentaires

Parlements nationaux	IPEX
Commission européenne	EUR-Lex

Acte final

Directive 2016/681
JO L 119 04.05.2016, p. 0132 Résumé

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

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 1er décembre 2009, la proposition de 2007, non encore adoptée par la 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 :

- selonl'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 2ème 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 ?uvre : 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 ?uvre 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.

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

Avis du Contrôleur européen de la protection des données sur la proposition de directive relative à 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.

Le CEPD se félicite d?avoir été consulté par la Commission. Déjà avant l?adoption de la proposition, le CEPD avait eu la possibilité de présenter des observations informelles. Certaines de ces observations ont été prises en considération dans la proposition et le CEPD relève que dans l?ensemble, les garanties de protection des données ont été renforcées dans la proposition. Cependant, un certain nombre de points restent préoccupants, notamment en ce qui concerne l?ampleur et les finalités de la collecte des données à caractère personnel.

Pour rappel, le principal objectif d?un système PNR au niveau de l?Union est la mise en place d?un système obligeant les transporteurs aériens assurant des vols internationaux entre l?UE et des pays tiers à transmettre aux autorités compétentes les données PNR de tous les passagers, afin de prévenir et de détecter les infractions terroristes et les formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière. Les données seraient centralisées et analysées par des unités de renseignements passagers et le résultat de l?analyse serait transmis aux autorités nationales compétentes de chaque État membre.

Depuis 2007, le CEPD suit de près les développements liés à un possible système PNR au niveau de l?Union, parallèlement aux développements concernant les systèmes PNR de pays tiers. Le principal aspect régulièrement soulevé par le CEPD porte sur la justification de la nécessité d?un système PNR européen qui viendrait s?ajouter à un certain nombre d?autres instruments autorisant le traitement de données à caractère personnel à des fins répressives.

Le CEPD reconnaît que des améliorations visibles sur le plan de la protection des données ont été apportées à la proposition actuelle, par rapport à la version sur laquelle il a déjà rendu un avis (voir CNS/2007/0237). Ces améliorations portent notamment sur le champ d?application de la proposition, la définition du rôle des différentes parties prenantes (unités de renseignements passagers), l?exclusion du traitement de données sensibles, l?adoption d?une méthode «push» sans période de transition et la limitation de la période de conservation des données.

Cependant, alors qu?il existe une volonté claire d?expliquer la nécessité du système, le CEPD ne trouve toujours aucun motif probant pour développer le système, notamment en ce qui concerne «l?information préalable» à grande échelle de tous les passagers.

Globalement, le CEPD estime donc que la condition préalable indispensable à tout développement d?un système PNR ? à savoir le respect des principes de nécessité et de proportionnalité ? n?est pas satisfaite dans la proposition. Le CEPD rappelle que selon lui, les données PNR pourraient certainement être nécessaires à des fins répressives dans des cas bien déterminés et être utilisées de façon conforme aux exigences en matière de protection des données. C?est leur utilisation de façon systématique et sans discernement pour tous les passagers qui soulève des préoccupations particulières.

Pour le CEPD, la seule mesure conforme aux exigences en matière de protection des données serait l?utilisation des données PNR au cas par cas, quand survient une menace sérieuse accompagnée par des indicateurs concrets.

Au-delà de cette lacune majeure, les observations du CEPD concernent les aspects suivants:

- le champ d?application devrait être beaucoup plus limité compte tenu du type d?infractions concernées. Le CEPD émet des doutes quant à l?inclusion dans la proposition de formes graves de criminalité n?ayant aucun lien avec le terrorisme. En tout état de cause, les infractions mineures devraient être explicitement circonscrites et écartées. Le CEPD recommande donc d?exclure la possibilité pour les États membres d?élargir le champ d?application;
- la nature des différentes menaces autorisant l?échange de données entre unités de renseignements passagers ou avec les États membres n?a pas été suffisamment définie;
- les principes de protection des données applicables ne devraient pas uniquement se fonder sur la décision-cadre 2008/977/JAI du

Conseil qui comprend des lacunes, notamment au niveau des droits des personnes concernées et des transferts à des pays tiers. Un niveau plus élevé de garanties, basé sur les principes de la directive 95/46/CE, devrait être introduit dans la proposition;
- aucune donnée ne devrait être conservée au-delà de 30 jours sous une forme identifiable, sauf dans les cas nécessitant une enquête plus approfondie;
- la liste des données PNR à traiter devrait être restreinte, notamment, le champ «remarques générales» ne devrait pas être inclus;
- l?évaluation de la directive devrait être fondée sur des données exhaustives, incluant le nombre de personnes effectivement condamnées ? et pas seulement poursuivies ? sur la base du traitement de leurs données.

Le CEPD recommande également que les développements relatifs à un système PNR au niveau de l?Union soient évalués dans une perspective plus large, incluant l?évaluation générale actuelle de l?ensemble des instruments européens dans le domaine de la gestion de l?échange de l?information mise en ?uvre par la Commission en janvier 2010. En particulier, les résultats des travaux actuels sur le modèle européen d?échange d'informations, dont la publication est prévue pour 2012, devraient être pris en considération lors de l?évaluation de la nécessité d?un système PNR à l?échelle de l?Union.

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

Les ministres ont examiné une proposition de directive relative à l'utilisation des données des dossiers passagers à des fins de protection contre les infractions terroristes et les formes graves de criminalité.

Un des principaux points sur lesquels les discussions ont porté a été de déterminer si les nouvelles dispositions proposées devraient concerner uniquement la collecte des "données des dossiers passagers" (PNR) pour les vols en provenance et à destination de pays tiers ou si les vols intérieurs à l'UE devraient également être couverts. La majorité des États membres considéraient qu'il convenait d'inclure au moins une option afin que les États membres aient, individuellement, la possibilité de recueillir des données PNR y compris concernant certains vols intra-UE.

L'objectif général de la directive proposée est de mettre en place un système cohérent, à l'échelle de l'UE, concernant les données des dossiers passagers, en créant un modèle UE unique pour tous les États membres participant au nouveau système et en assurant la coopération entre les autorités concernées au sein de l'Union. En conséquence, tous les transporteurs aériens effectuant des vols couverts par les nouvelles dispositions seront tenus de fournir aux services répressifs des États membres les "données des dossiers passagers" (PNR). Ceux-ci ne seront cependant autorisés à utiliser ces données - qui sont déjà recueillies actuellement par les transporteurs aériens - que pour la prévention et la détection des infractions terroristes et des formes graves de criminalité (transnationale), ainsi que pour les enquêtes et les poursuites en la matière.

Vingt-quatre États membres de l'UE participeront certainement à l'adoption de la nouvelle directive; le Danemark, en revanche, ne sera pas lié par les nouvelles dispositions. Le Royaume-Uni et l'Irlande devront, pour leur part, indiquer s'ils souhaitent y participer ("opt in") ou non.

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

Les ministres ont approuvé une orientation générale sur le projet de directive relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité (données PNR). L'accord dégagé au sein des États membres permet à la présidence danoise d'ouvrir les négociations avec le Parlement européen dans le cadre de la procédure législative ordinaire.

Le débat au sein du Conseil a porté entre autres sur deux questions fondamentales.

1. La première question consiste à déterminer si les nouvelles dispositions proposées devraient concerner uniquement la collecte des «données des dossiers passagers» (PNR) pour les vols en provenance et à destination de pays tiers ou si les vols intérieurs à l'UE devraient également être couverts. Le compromis proposé permettrait aux États membres, sans les y contraindre, de recueillir des données PNR également en ce qui concerne certains vols intra-UE.
2. La deuxième question a été celle de la période de conservation des données. La proposition initiale de la Commission prévoit une période de conservation totale de cinq ans. Au bout de 30 jours cependant, les données PNR seraient masquées, de façon à ce que les éléments des données PNR se rapportant au passager ne soient plus visibles par l'agent des services répressifs chargé du contrôle en première ligne, mais ne pourraient être consultées qu'après obtention d'une autorisation spécifique. Certains États membres estiment que cette période initiale de conservation de 30 jours est trop courte d'un point de vue opérationnel. La position dégagée par le Conseil consiste à maintenir la période globale de conservation de cinq ans mais à étendre à deux ans la première période au cours de laquelle les données seraient totalement accessibles.

Le Conseil a également adopté une décision relative à la conclusion d'un nouvel accord entre les États-Unis et l'UE sur les données PNR appelé à remplacer l'accord actuel, qui était appliqué à titre provisoire depuis 2007. Le Parlement européen avait donné son approbation le 19 avril 2012. Cet accord devrait entrer en vigueur le 1er juin 2012.

L'accord en question vise à mettre en place un cadre juridique régissant le transfert des données des dossiers passagers (données PNR) par les transporteurs assurant des services de transport de passagers entre l'Union européenne et les États-Unis au ministère américain de la sécurité intérieure (Department of Homeland Security, ou DHS) et l'utilisation qui en sera faite par celui-ci. Il s'agit de prévenir et de détecter les infractions terroristes ainsi que les infractions pénales qui y sont liées ainsi que d'autres formes graves de criminalité transnationale, et de mener des enquêtes et des poursuites en la matière.

Les éléments principaux du nouvel accord PNR avec les États-Unis sont les suivants:

- une limitation stricte des finalités, l'utilisation des données PNR étant limitée à la prévention et à la détection d'infractions terroristes ou de la criminalité transnationale, ainsi qu'aux enquêtes et poursuites en la matière;
- l'obligation juridiquement contraignante, pour le ministère américain de la sécurité intérieure, d'informer les États membres et les autorités de l'UE des pistes susceptibles d'intéresser l'UE qui découleraient de l'analyse de ces données PNR;
- un régime fort de protection des données, prévoyant des exigences élevées en matière de sécurité et d'intégrité des données;
- des droits d'accès, de rectification et d'effacement, ainsi que la possibilité d'introduire un recours administratif ou judiciaire;
- une durée limitée d'utilisation des données PNR, de 10 ans pour la criminalité transnationale et de 15 ans pour le terrorisme. Après six mois, les informations permettant une identification personnelle contenues dans les données PNR seront masquées et, après 5 ans, les données PNR seront transférées vers une base de données dormante faisant l'objet de contrôles supplémentaires.

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

La commission des libertés civiles, de la justice et des affaires intérieures a adopté à une courte majorité (30 voix pour, 25 voix contre et aucune abstention) le 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 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 recommande que le Parlement européen rejette la proposition et appelle la Commission à la remplacer par un autre texte.

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

Le rapporteur a demandé le renvoi en commission du rapport, conformément à l'article 175 du règlement. Par vote électronique (143 pour, 83 contre, 9 abstentions), le Parlement a approuvé la demande.

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

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 Europol. 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 dêtres humains, lexploitation sexuelle des enfants, le trafic de drogues, le trafic darmes, de munitions et dexplosifs, le blanchiment dargent 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 lidentification dun 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 uvre 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 lévaluation 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 jusquà 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 lÉtat 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.

Lautorité 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.

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

Second avis du Contrôleur européen de la protection des données (CEPD) sur la proposition de directive du Parlement européen et du Conseil relative à lutilisation 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 (directive PNR).

Pour rappel, la procédure législative est en suspens depuis que la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen a rejeté la proposition le 24 avril 2013, remettant en cause la nécessité et la proportionnalité de celle-ci. Récemment, les débats ont été relancés suite aux attentats terroristes survenus à Paris en janvier 2015.

Dans sa résolution du 11 février 2015 sur les mesures de lutte contre le terrorisme, le Parlement européen sest engagé à mettre tout en uvre pour finaliser la directive PNR de lUnion dici la fin de lannée. Il a notamment :

- prié la Commission de tirer les conséquences de larrêt de la Cour de justice de lUnion européenne relatif à la directive sur la conservation des données et ses effets possibles sur la directive PNR de lUnion ;
- demandé aux États membres doptimiser lutilisation des structures, bases de données et systèmes dalerte existants en Europe, tels que le système dinformation Schengen (SIS) et le système dinformations anticipées sur les passagers (APIS) et
- appelé à une amélioration des échanges dinformations entre les autorités policières et judiciaires des États membres et les agences de lUnion.

Le Parlement européen a également encouragé le Conseil à progresser sur le paquet législatif relatif à la protection des données, afin que les négociations en «trilogue» sur la directive PNR de lUnion et le paquet législatif relatif à la protection des données puissent avoir lieu parallèlement.

Dans ce contexte, un rapport actualisé a été présenté par le rapporteur de la commission LIBE le 17 février 2015. Plusieurs modifications de la proposition de la Commission ont été suggérées dans ce document, telles que léventuelle inclusion des vols intra-UE. La commission LIBE a adopté son vote dorientation le 15 juillet 2015 et accepté dentamer les négociations avec le Conseil.

Le présent avis du CEPD se penche sur les modifications de la proposition telles que suggérées par la commission LIBE et le Conseil en vue des négociations en trilogue qui doivent débuter en novembre 2015.

Le CEPD salue les améliorations apportées à la proposition par le Conseil et la commission LIBE, par exemple concernant les dispositions spécifiques relatives à la protection des données, la présence dun délégué à la protection des données ou une référence spécifique à la compétence des autorités de contrôle.

Toutefois, le CEPD estime que les conditions préalables essentielles au système PNR - à savoir le respect des principes de nécessité et de proportionnalité - ne sont toujours pas remplies dans la proposition. Parmi les lacunes majeures, le CEPD signale :

- labsence dévaluation exhaustive de la capacité des instruments existants actuels à atteindre la finalité du système PNR de lUnion européenne ;
- labsence danalyse détaillée de la mesure dans laquelle des mesures plus respectueuses de la vie privée pourraient atteindre la finalité du système PNR de lUnion européenne ;
- le fait que la collecte non ciblée et massive de données ainsi que le traitement de celles-ci dans le cadre du système PNR sapparentent à une mesure de surveillance générale.

Le CEPD estime que la seule finalité qui serait conforme aux exigences de transparence et de proportionnalité serait lutilisation de données PNR au cas par cas mais, uniquement en cas de menace réelle et sérieuse appuyée par des indicateurs plus spécifiques. Cest pourquoi il encourage les législateurs à approfondir la réflexion sur la faisabilité, compte tenu des menaces actuelles, de mesures de surveillance plus sélectives et plus respectueuses de la vie privée sur la base dinitiatives plus spécifiques se concentrant, le cas échéant, sur des catégories ciblées de vols, de passagers ou de pays.

De lavis du CEPD, la proposition devrait :

- limiter la durée de conservation des données à la période justifiée par des critères objectifs expliquant la durée retenue ;
- prévoir de manière plus explicite que les données PNR ne peuvent pas être utilisées à dautres fins que la prévention et la détection des infractions terroristes et des infractions transnationales graves ;
- prévoir, en principe, lobtention de laccord préalable dune juridiction ou dun organe administratif indépendant en cas de demande daccès aux données émanant dune autorité compétente;
- faire référence à des garanties appropriées garantissant la sécurité des données traitées par lunité de renseignements «passagers»;
- prévoir un champ dapplication du système PNR bien plus limité en termes de type dinfraction ;
- mieux définir les critères à remplir pour que les autorités compétentes puissent accéder aux données PNR.

Le CEPD invite les législateurs à attendre ladoption du nouveau paquet législatif relatif à la protection des données, afin de veiller à ce que les obligations de la proposition soient en parfaite concordance avec les nouvelles dispositions adoptées. De plus, lévaluation de la directive devrait être fondée sur des données exhaustives, y compris le nombre de personnes effectivement condamnées, plutôt que seulement poursuivies, sur la base du traitement de leurs données.

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

La présidence a informé le Conseil de l'état d'avancement des travaux sur la proposition de directive relative à 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.

Pour rappel, en avril 2012, le Conseil «Justice et affaires intérieures» a arrêté une orientation générale concernant ce projet de directive.

Le Conseil et le Conseil européen ont régulièrement souligné qu'il était urgent de faire aboutir cette directive en raison de la menace croissante que représentent les combattants étrangers.

Le 15 juillet 2015, la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen chargée de la proposition a adopté un rapport révisé sur la directive et un mandat pour débuter les négociations avec le Conseil.

Les négociations entre les institutions sur le projet de directive sont en cours.

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

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 ?uvre 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.

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

OBJECTIF : permettre le transfert des données PNR par les transporteurs aériens et leur traitement aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

ACTE LÉGISLATIF : Directive (UE) 2016/681 du Parlement européen et du Conseil relative à l'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.

CONTENU : la directive vise à réglementer le transfert vers les États membres, par les compagnies aériennes, des données PNR des passagers des vols internationaux (vols extra-UE), ainsi que le traitement de ces données par les autorités compétentes.

Si un État membre décide d'appliquer la directive aux vols intra-UE, il devra le notifier à la Commission par écrit. Un État membre pourra également décider d'appliquer la directive uniquement à certains vols intra-UE. Dans ce cas, il devra sélectionner les vols qu'il juge nécessaires afin de poursuivre les objectifs de la directive.

Unité d'informations passagers (UIP) : pour garantir l'efficacité et un niveau élevé de protection des données, les États membres seront tenus de veiller à ce qu'une autorité de contrôle nationale indépendante et, notamment, un délégué à la protection des données soient chargés de fournir des conseils et de surveiller la manière dont les données PNR sont traitées.

- Toute personne concernée aura 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.
- Le délégué à la protection des données aura accès à toutes les données traitées par l'UIP et pourra, sil estime que traitement de certaines données n'était pas licite, renvoyer l'affaire à l'autorité de contrôle nationale.
- Europol pourra également 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.

Traitement des données : les données PNR recueillies ne pourront être traitées qu'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.

Ainsi, l'UIP ne pourra 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 aura 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 pourra : a) confronter les données PNR aux bases de données utiles et b) traiter les données PNR au regard de critères préétablis.

L'évaluation des passagers au regard de critères préétablis devra être réalisée de façon non discriminatoire. Ces critères devront être ciblés, proportionnés et spécifiques, et être réexaminés à intervalles réguliers.

Transfert de données vers des pays tiers : les États membres ne seront autorisés à transférer des données PNR vers des pays tiers qu'au cas par cas et dans le respect des dispositions adoptées par les États membres en vertu de la décision-cadre 2008/977/JAI. Les transferts de données PNR sans laccord préalable de l'État membre dont les données ont été obtenues, ne seront autorisés que dans des circonstances exceptionnelles.

Conservation et dépersonnalisation des données : la directive prévoit que la conservation des données PNR dans les UIP est autorisée pendant une période n'excédant pas cinq ans au terme de laquelle les données devront être effacées.

Après une période de six mois suivant le transfert initial des données PNR, les données devront être dépersonnalisées par le masquage des éléments 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 sera autorisée que dans des conditions strictement définies.

Protection des données à caractère personnel : tout traitement de données PNR devra être consigné ou faire l'objet d'une trace documentaire à des fins de vérification de sa licéité et d'autocontrôle et pour garantir de manière adéquate l'intégrité des données et la sécurité du traitement.

LUIP devra tenir des registres au moins pour les opérations de traitement suivantes: la collecte, la consultation, la communication et l'effacement. Ces registres devront être conservés pendant cinq ans.

La directive interdit explicitement le traitement des données PNR sensibles 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. Dans l'hypothèse où l'UIP recevrait des données PNR révélant de telles informations, elle devrait les effacer immédiatement.

Protocoles communs et formats de données reconnus : à partir de l'année qui suit la date à laquelle la Commission adopte pour la première fois des protocoles communs et des formats de données reconnus, tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP devront se faire par voie électronique à l'aide de méthodes sécurisées respectant ces protocoles communs.

ENTRÉE EN VIGUEUR : 24.5.2016.

TRANSPOSITION : 25.5.2018.

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

Le présent document de travail de la Commission présente le plan de mise en uvre pour la directive (UE) 2016/681 du Parlement européen et du Conseil, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention, la détection, les enquêtes et la poursuite des infractions terroristes et des formes graves de criminalité. Les États membres sont tenus de transposer la directive dans leur législation nationale au plus tard le 25 mai 2018.

L'expérience des États membres et des pays tiers dotés d'un système PNR fonctionnel en place ou en voie de finalisation illustre les difficultés, en termes de ressources, de temps et de complexité technique, pour établir des systèmes PNR conformes à la directive. Ce processus requiert i) l'établissement des Unités nationales d'information sur les passagers (UIP), ii) l'essai du fonctionnement de leurs systèmes informatiques et iii) les ajustements nécessaires pour assurer le bon fonctionnement du système.

Mesures nationales nécessaires à la mise en uvre de la directive (UE) 2016/681: la Commission identifie les mesures les plus importantes que les États membres doivent adopter pour:

- fournir une base juridique pour la collecte et le traitement des données PNR qui inclue toutes les garanties de protection des données prévues dans la directive et dans les dispositions horizontales applicables, en particulier celles de la directive (UE) 2016/680 qui devra être transposée, sauf circonstances exceptionnelles, avant le 6 mai 2018, c'est-à-dire avant la date limite de transposition de la directive PNR de l'UE. En particulier, les États membres devraient envisager de fournir une indication claire des bases de données dans lesquelles les données PNR peuvent être comparées, et les principaux principes régissant la création, la mise à jour et le fonctionnement des critères préétablis selon lesquels les données PNR sont traitées;
- identifier et désigner l'autorité ou les autorités nationales qui abriteront lUIP et comment ces dernières seront incorporées dans leur structure administrative;
- doter l'UIP de l'infrastructure technique requise permettant le stockage, le traitement et l'analyse des données PNR;
- former le personnel de lUIP afin quil puisse sacquitter de ses fonctions d'analyse des données PNR;
- identifier et désigner les autorités compétentes habilitées à demander et à recevoir des données PNR ou le résultat du traitement de ces données auprès de lUIP;
- informer les transporteurs aériens des spécifications techniques concernant le transfert des données PNR et des essais nécessaires pour assurer leur connectivité avec l'infrastructure technique de lUIP;
- concevoir des solutions appropriées pour garantir que les UIP puissent échanger les données PNR efficacement et en temps opportun.

Progrès accomplis par les États membres dans la mise en uvre: l'état d'avancement de la directive varie considérablement d'un État membre à l'autre. Un certain nombre d'entre eux possèdent déjà un système PNR fonctionnel en place ou en sont à un stade avancé de sa finalisation :

- actuellement, quatre États membres disposent à la fois de systèmes PNR fonctionnels ou quasi fonctionnels et d'une base juridique spécifique prévoyant la collecte ou le traitement de données PNR; des modifications sont néanmoins nécessaires pour adapter complètement le cadre législatif aux exigences de la directive; l'expérience de ces quatre États membres fournit des exemples de bonnes pratiques qui devraient être utilisés par d'autres États membres ;
- douze États membres se trouvent à différents stades de l'achèvement de l'infrastructure technique et de l'adoption d'une législation spécifique sur les PNR;
- onze États membres en sont encore à un stade relativement précoce du processus de mise en uvre ; toutefois, certains de ces États membres ont déjà élaboré des plans de mise en uvre détaillés assortis de délais concrets.

Actions de soutien: pour soutenir et suivre les progrès accomplis par les États membres dans la mise en uvre de la directive PNR, la Commission prend les mesures suivantes:

- réunions régulières avec les États membres et Europol pour discuter des questions juridiques liées à l'interprétation et à la mise en uvre de la directive et pour partager les questions, les enseignements tirés et les meilleures pratiques;
- assistance financière aux États membres: la Commission a proposé à l'autorité budgétaire de fournir un montant supplémentaire de 70 millions EUR pour aider les États membres à mettre en place leurs UIP. Ce financement serait alloué principalement par le biais des programmes nationaux du Fonds de sécurité intérieure et, éventuellement, par des actions de l'Union. La Commission est prête à fournir un soutien financier supplémentaire si nécessaire;
- décision d'exécution de la Commission sur les formats de données et les protocoles de transmission: cette décision fournira une liste de protocoles communs et de formats de données acceptés par les transporteurs aériens lors du transfert des données PNR vers les PIU.

Mesures possibles pour les États membres: la Commission a identifié un certain nombre de jalons indicatifs auxquels les États membres devraient satisfaire afin que leurs PIU soient opérationnels d'ici mai 2018. Ceux-ci couvrent des aspects tels que:

- ladoption dune législation conforme à la directive ;
- la mise en place des UIP ;
- létablissement de solutions techniques pour le traitement des données PNR ;
- la dotation en personnel des UIP ;
- la participation des autorités compétentes (par ex : lidentification des autorités compétentes habilitées à demander ou à recevoir des données PNR) ;
- la connectivité du transporteur.