CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Projet de loi 7151

Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant organisation du Service de renseignement de l'État

Date de dépôt : 19-06-2017
Date de l'avis du Conseil d'État : 03-04-2018

Liste des documents

Date	Description	Nom du document	Page
01-10-2018	Résumé du dossier	Résumé	3
19-06-2017	Déposé	7151/00	5
10-11-2017	Avis des autorités judiciaires 1) Avis du Parquet général (24.8.2017) 2) Avis des Parquets de Luxembourg et de Diekirch (15.10.2017) 3) Avis du Tribunal d'arrondissement de et à Luxembourg [...]	7151/01	54
18-12-2017	Avis de la Commission nationale pour la protection des données (23.11.2017)	7151/02	67
18-12-2017	Avis de la Cour supérieure de Justice (20.11.2017)	7151/03	75
20-12-2017	Avis de la Chambre de Commerce (13.12.2017)	7151/04	80
28-02-2018	Amendements gouvernementaux 1) Dépêche du Ministre aux Relations avec le Parlement au Président de la Chambre des Députés (27.2.2018) 2) Texte et commentaire des amendements gouvernementaux<br [...]	7151/05	91
03-04-2018	Avis du Conseil d'État (30.3.2018)	7151/06	104
27-04-2018	Amendements gouvernementaux 1) Dépêche du Ministre aux Relations avec le Parlement au Président de la Chambre des Députés (27.4.2018) 2) Texte et commentaire des amendements gouvernementaux<br [...]	7151/07	123
27-06-2018	Avis complémentaire du Conseil d'État (26.6.2018)	7151/08	158
20-07-2018	Rapport de commission(s) : Commission de la Force publique Rapporteur(s) :	7151/09	163
26-07-2018	Premier vote constitutionnel (Vote Positif) En séance publique n°59 Une demande de dispense du second vote a été introduite	7151	196
31-07-2018	Dispense du second vote constitutionnel par le Conseil d'Etat (31-07-2018) Evacué par dispense du second vote (31-07-2018)	7151/10	198
19-07-2018	Commission de la Force publique Procès verbal (11) de la reunion du 19 juillet 2018	11	201
05-07-2018	Commission de la Force publique Procès verbal (09) de la reunion du 5 juillet 2018	09	205
04-05-2018	Commission de la Force publique Procès verbal (05) de la reunion du 4 mai 2018	05	210
16-08-2018	Publié au Mémorial A n°690 en page 1	7151	226

Résumé

7151

Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État

Le projet de loi a pour objet de transposer en droit national la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (Passenger Name Records, 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.

L'enjeu de la directive est de mettre en place entre les États membres de l'UE un système harmonisé de collecte, d'utilisation et de conservation des données PNR, tout en garantissant le respect des droits fondamentaux et surtout de la protection des données à caractère personnel. Ce système repose sur la création dans chaque État membre d'une unité centrale nationale appelée « Unité d'informations passagers » (« UIP ») chargée d'analyser les données PNR transférées par les transporteurs aériens et d'assurer la coordination des procédures et le transfert des informations entre les UIP des différents États membres, certaines autorités nationales bien définies, Europol, ainsi qu'à destination de pays non-membres de l'UE dans les cas où le traitement des données PNR s'avérerait positif.

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 usage commercial. Elles comprennent des informations telles que les coordonnées du passager, la date du voyage et d'émission du billet, le mode de paiement utilisé et le poids des bagages.

Outre leur usage commercial, les données PNR présentent un intérêt avéré pour les autorités chargées de la prévention et de la répression de la criminalité et sont utilisées depuis des années par les services policiers et douaniers de certains pays. Les activités liées à la criminalité organisée et au terrorisme impliquent souvent des déplacements internationaux. Ces données permettent de contrer la menace que représentent en particulier le terrorisme et certaines autres formes graves de criminalité sous un angle différent que d'autres catégories de données à caractère personnel traitées par les services répressifs.

Les données PNR peuvent être utilisées de différentes manières et à différentes fins. En temps réel, elles aident à trouver des personnes recherchées par la confrontation à des bases de données nationales et internationales ainsi qu'à identifier des personnes pour lesquelles l' analyse de profil indique qu'elles peuvent être impliquées dans une activité criminelle. Les données peuvent également être utilisées de manière réactive pour rassembler des preuves dans le cadre d'enquêtes et, finalement, de manière proactive pour analyser et définir des critères d' évaluation qui peuvent ensuite être appliqués afin d'évaluer le risque que représentent les passagers avant leur arrivée et avant leur départ.

7151/00

Nº 7151

CHAMBRE DES DEPUTES

Session ordinaire 2016-2017

PROJET DE LOI

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

(Dépôt: le 19.6.2017)

SOMMAIRE:

		page
1)	Arrêté Grand-Ducal de dépôt (8.6.2017)	1
2)	Exposé des motifs	2
3)	Texte du projet de loi	4
4)	Commentaire des articles	13
5)	Tableau de correspondance	24
6)	Fiche financière	26
7)	Fiche d'évaluation d'impact	28
8)	Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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	31

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre de la Sécurité intérieure et après délibération du Gouvernement en Conseil;

Arrêtons:

Article unique.– Notre Ministre de la Sécurité intérieure est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Palais de Luxembourg, le 8 juin 2017

Pour le Ministre de la Sécurité intérieure,
La Secrétaire d'Etat,
Francine CLOSENER

HENRI

*

EXPOSE DES MOTIFS

Le présent projet de loi a pour objet de transposer en droit national la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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.

*

1. RETROACTES

Le Luxembourg avait inscrit la lutte contre le terrorisme et la criminalité organisée parmi les priorités de sa présidence du Conseil de l'Union européenne au 2e semestre de l'année 2015 et s'était, entre autres, fixé comme objectif de parvenir à un accord politique sur la création d'un système PNR européen.

L'idée de créer un cadre légal européen pour l'utilisation des données passagers à des fins répressives remonte à une proposition de la Commission européenne du 6 novembre 2007. La proposition de décision-cadre n'ayant toutefois pas été adoptée par le Conseil au moment de l'entrée en vigueur du traité sur le fonctionnement de l'Union européenne (TFUE) le 1er décembre 2009, elle a dû être remplacée par un nouveau texte. Le 2 février 2011, la Commission européenne a présenté une proposition de directive sur laquelle le Conseil Justice et Affaires intérieures (JAI) a dégagé une orientation générale le 26 avril 2012. Un vote de rejet de la Commission Libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen du 24 avril 2013 a toutefois bloqué la proposition de directive.

La montée en puissance du phénomène des combattants étrangers a relancé les discussions autour de la mise en place d'un système PNR européen. Après les attenants qui ont frappé Paris en janvier 2015, les chefs d'Etat et de Gouvernement de l'Union européenne ont appelé à adopter d'urgence une directive robuste et efficace relative à un système PNR européen dotée de garanties en matière de protection des données.

Au mois de février 2015, le Parlement européen s'est engagé à travailler sur la finalisation d'une directive jusqu'à la fin de l'année 2015, tout en encourageant le Conseil à faire des progrès sur le paquet protection des données afin de permettre des trilogues en parallèle sur la proposition de directive PNR et la proposition de directive relative à la protection des données à caractère personnel en matière pénale. Le 15 juillet 2015, le Parlement européen a adopté un rapport révisé sur la proposition de directive PNR et un mandat de négociation avec le Conseil.

La Présidence luxembourgeoise du Conseil a réussi à négocier un texte de compromis qui respecte à la fois les principes fondamentaux en matière de protection des données et réponde aux besoins opérationnels des services compétents. Le texte de compromis a été approuvé par le Conseil JAI le 4 décembre 2015 et par le Parlement européen le 14 avril 2016.

Les principaux éléments de discussion entre le Conseil, la Commission et le Parlement étaient l'inclusion des vols intra-communautaires, l'application de la directive aux opérateurs économiques non transporteurs et la durée de conservation des données sous une forme „active".

Pour trouver un compromis entre les Etats membres qui plaidaient pour l'inclusion obligatoire de tous les vols intra-UE et les Etats membres qui étaient opposés à l'inclusion de ces vols, l'orientation générale adoptée en avril 2012 avait laissé le choix aux Etats membres de collecter ou non les données PNR sur tous ou sur certains vols intra-UE. En raison de la menace sécuritaire constituée par les combattants étrangers et des stratégies de contournement entretemps développées, l'inclusion des vols intra-UE n'a plus été en 2015 un sujet controversé au sein du Conseil. L'expérience acquise par les services répressifs montre en effet que les combattants étrangers empruntent des trajets de plus en plus compliqués à travers l'Union européenne pour dissimuler leur point de départ initial et leur destination finale. Le même phénomène est observé à propos des membres d'organisations criminelles.

Le Parlement européen souhaitait voir limiter l'application de la directive aux vols en provenance ou à destination d'Etats non membres de l'Union européenne.

Le texte de la directive tel qu'adopté le 27 avril 2016 retient que les Etats membres sont libres de collecter les données PNR sur tous ou sur certains vols intra-UE. Dans une déclaration commune du 4 décembre 2015, les ministres JAI se sont engagés à faire pleinement usage de la faculté de recueillir des données PNR pour les vols intra-UE dès la mise en application de la directive.

Un autre sujet de négociation était la collecte obligatoire de données PNR auprès d'opérateurs économiques tels que des agences ou des organisateurs de voyages. Il a été retenu que la Commission procède, au plus tard deux ans après le délai de transposition, à un réexamen de tous les éléments de la directive, et notamment la nécessité d'inclure ces opérateurs économiques. Par ailleurs, un considérant de la directive précise que les Etats membres peuvent prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs ou auprès de transporteurs autres que les transporteurs aériens. Dans la déclaration commune précitée du 4 décembre 2015, les ministres se sont engagés, dans la mesure du possible, à élargir la collecte des données PNR auprès d'opérateurs économiques autres que les transporteurs. Cette inclusion pose cependant des difficultés pratiques dans la mesure où les opérateurs économiques utilisent des systèmes de réservation différents et qu'il n'existe pas de standards en ce qui concerne leurs systèmes informatiques. Le Luxembourg engagera dès à présent des réflexions sur la mise en pratique de l'inclusion des opérateurs économiques, mais attendra les résultats de l'évaluation au sujet de la nécessité de les inclure dans le champ d'application.

Un troisième élément de discussion était la durée de conservation des données PNR. La proposition de la Commission prévoyait une période initiale de conservation de trente jours, suivie d'une période supplémentaire de cinq ans au cours de laquelle les données seraient masquées. Les négociations entre Etats membres ont toutefois fait apparaître qu'une période initiale de trente jours était trop courte d'un point de vue opérationnel et le Conseil a retenu une période de conservation globale de cinq ans, subdivisée en deux périodes, une première période de deux ans au cours de laquelle les données seraient pleinement accessibles, et une seconde période de trois ans où les données servant à identifier le passager seraient masquées et leur divulgation complète serait subordonnée à des conditions strictes. Selon l'avis et les expériences des services répressifs, le système PNR ne permet en effet de lutter de manière efficace contre le terrorisme et la criminalité organisée que si les données restent „actives" pendant une certaine période. Comme les actes de terrorisme se préparent généralement sur une période plus longue, le système PNR doit être conçu de manière à ce qu'il permette de reconstituer l'activité d'un ou de plusieurs individus en remontant sur une période suffisamment longue. Le suivi des groupes terroristes exige d'établir des „patterns of life", procédure qui s'inscrit dans le long terme. La probabilité qu'une information intéressante se trouve dans les données PNR recueillies depuis moins de 30 jours est quasiment nulle. Par ailleurs, concernant le cas particulier des individus se rendant dans des camps d'entraînement en Syrie ou en Irak, selon les renseignements des services spécialisés, ces séjours dépassent généralement 30 jours. Un délai de 30 jours est également trop court pour lutter contre d'autres formes de criminalité telles que le trafic de drogue. Les critères d'évaluation sont en effet établis sur base de l'analyse répétée des données de voyage d'un individu en particulier ou de personnes qui apparaissent régulièrement dans le même dossier de voyage. Or, les trafiquants de drogues sont déployés tous les 4 à 6 mois. Une période de temps avant le masquage suffisamment longue est nécessaire pour découvrir de telles routes et pour comprendre comment les criminels adaptent leurs habitudes.

Le Parlement européen a soutenu la proposition initiale de la Commission. La Présidence luxembourgeoise a toutefois réussi à démontrer, sur base d'exemples concrets fournis par les services compétents des Etats membres de l'Union européenne, qu'une période „active" de 30 jours n'est pas suffisante.

Le texte de compromis retient que les éléments des données qui peuvent servir à identifier directement le passager auquel se rapportent les données doivent être masqués à l'expiration d'une période de 6 mois à compter de leur transfert par les transporteurs aériens.

*

2. OBJET DU PROJET DE LOI

Le présent projet de loi a pour objet de régler le transfert des données PNR des transporteurs aériens vers une unité centrale nationale ayant pour mission la répression et la prévention des infractions terroristes et d'autres formes graves de criminalité ainsi que le traitement ultérieur de ces données.

Les données PNR (Passenger Name Records) 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 usage commercial. Elles comprennent des informations telles

que les coordonnées du passager, la date du voyage et d'émission du billet, le mode de paiement utilisé et le poids des bagages.

Outre leur usage commercial, les données PNR présentent un intérêt avéré pour les autorités chargées de la prévention et de la répression de la criminalité et sont utilisées depuis des années par les services policiers et douaniers de certains pays. Les activités liées à la criminalité organisée et au terrorisme impliquent souvent des déplacements internationaux. Ces données permettent de contrer la menace que représentent en particulier le terrorisme et certaines autres formes graves de criminalité sous un angle différent que d'autres catégories de données à caractère personnel traitées par les services répressifs.

Les données PNR peuvent être utilisées de différentes manières et à différentes fins. En temps réel, elles aident à trouver des personnes recherchées par la confrontation à des bases de données nationales et internationales ainsi qu'à identifier des personnes pour lesquelles l'analyse de profil indique qu'elles peuvent être impliquées dans une activité criminelle. Les données peuvent également être utilisées de manière réactive pour rassembler des preuves dans le cadre d'enquêtes et, finalement, de manière proactive pour analyser et définir des critères d'évaluation qui peuvent ensuite être appliqués afin d'évaluer le risque que représentent les passagers avant leur arrivée et avant leur départ.

*

3. LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Le considérant 27 de la directive précise que le traitement des données PNR doit être soumis à une norme de protection des données à caractère personnel du droit national conforme à la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale et aux exigences spécifiques de protection des données énoncées dans la directive PNR. Il précise par ailleurs que les références faites dans la directive PNR à la décision-cadre 2008/977/JAI doivent s'entendre comme des références à la législation actuellement en vigueur et à la législation qui la remplacera.

Dans la mesure où la décision-cadre 2008/977 a été abrogée par la directive du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, qui est transposée en droit national parallèlement à la directive PNR, le présent projet de loi fait référence aux dispositions pertinentes du projet de loi de transposition de la directive du 27 avril 2016 aux endroits où la directive PNR fait référence à la décision-cadre 2008/977. Il est renvoyé à cette loi de transposition notamment en ce qui concerne les droits des personnes et l'autorité de contrôle en matière de données PNR. En dehors de ces références à la loi de transposition de la directive du 27 avril 2016, le présent projet de loi comporte toute une série de dispositions spéciales qui sont destinées à garantir la protection des données PNR en particulier.

*

TEXTE DU PROJET DE LOI

Chapitre 1er – *Dispositions générales*

Art. 1er. La présente loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Art. 2. Pour l'application de la présente loi, on entend par:

a) „transporteur aérien“: toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes;

b) „passager“: toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers;

c) „dossier passager“: le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités;

d) „système de réservation“: le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations;

e) „système de contrôle des départs“: le système utilisé pour contrôler les passagers lors de l'embarquement;

f) „données PNR“: les données contenues dans le dossier passager et énumérées à l'annexe I;

g) „méthode push“: la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'information passagers;

h) „infractions terroristes“: les infractions visées au Livre II, Titre 1ier, Chapitre III-1 du Code pénal;

i) „formes graves de criminalité“: les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans;

j) „dépersonnaliser par le masquage d'éléments des données“: rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée.

Chapitre 2 – *Unité d'information passagers*

Art. 3. Il est créé au sein de la Police grand-ducale une Unité d'informations passagers, ci-après désignée „UIP“, qui est chargée:

a) de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données;

b) du transfert de ces données et des résultats de leur traitement aux services compétents;

c) de l'échange de ces données et des résultats de leur traitement avec les unités d'information passagers des autres Etats membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4. Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel détaché de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Art. 5. Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la méthode push, les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg dont ils disposent.

Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR incombe au transporteur aérien qui assure le vol.

Art. 6. (1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes:

a) 48 heures avant l'heure de départ programmée du vol;

b) 24 heures avant l'heure de départ programmée du vol;

c) 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 qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point c), peut se limiter à une mise à jour des transferts visés à l'alinéa 1er, points a) et b).

(2) Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP peut demander, au cas par cas, le transfert de données PNR en dehors des délais prévus au paragraphe 1er.

Art. 7. (1) Les données PNR sont transférées à l'UIP par voie électronique au moyen des protocoles communs et des formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la Directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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. Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg dès leur publication au Journal officiel de l'Union européenne.

Les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisés pour leurs transferts.

(2) En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union européenne en matière de protection des données soit pleinement respecté.

Chapitre 4 – *Traitement des données PNR*

Art. 8. Le traitement de données PNR qui révèlent 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 est interdit.

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive.

Art. 9. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données supplémentaires dès réception et de façon définitive.

Art. 10. (1) L'UIP traite les données PNR en vue de réaliser une évaluation des passagers avant leur arrivée prévue sur le territoire national ou leur départ prévu du territoire national afin d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis compte tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

(2) Pour réaliser cette évaluation l'UIP peut comparer les données PNR:

a) aux banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions;

b) à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur 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.

(3) L'UIP réexamine individuellement, par des moyens non automatisés, toute concordance positive obtenue à la suite d'un traitement automatisé des données PNR effectué en vertu du présent article.

(4) L'UIP transmet aux services compétents, au cas par cas, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au présent article ou le résultat du traitement de ces données.

(5) Les conséquences de l'évaluation des passagers ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union européenne à la libre circulation sur le territoire de Luxembourg tel que prévu par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.

(6) Lorsque les évaluations sont réalisées pour des vols entre le Luxembourg et un autre Etat membre de l'Union européenne auquel s'applique le règlement No 562/2006 du Parlement européen et du

Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes, les conséquences de ces évaluations doivent respecter ledit règlement.

Art. 11. L'UIP traite les données PNR afin de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations visées à l'article 10.

Art. 12. L'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, dûment motivées et fondées sur des motifs suffisants visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques aux fins visées à l'article 1er, et visant à communiquer aux services compétents ou, le cas échéant, à Europol, le résultat de ce traitement.

Chapitre 5 – *Services compétents*

Art. 13. Sans préjudice des attributions des autorités judiciaires telles que définies par le Code de procédure pénale, sont habilités à demander et à recevoir des données PNR ou le résultat du traitement de ces données, dans le cadre de leurs attributions légales et dans la limite du besoin d'en connaître:

a) les services de la Police grand-ducale;

b) le Service de Renseignement de l'Etat;

c) les services de l'Administration des Douanes et Accises.

Art. 14. Les services compétents ne peuvent traiter les données PNR et le résultat du traitement de ces données que pour les finalités de la présente loi telles que définies à l'article 1er.

L'alinéa 1er est sans préjudice des compétences de la Police et de l'Administration des Douanes et Accises lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement.

Art. 15. Les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Art. 16. Lorsqu'une personne est identifiée conformément à l'article 10, l'UIP communique toutes les données pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP des autres Etats membres de l'Union européenne concernés.

Lorsque l'UIP est destinataire d'informations telles que visées à l'alinéa 1er de la part d'une autre UIP, elle transmet ces informations aux services compétents.

Art. 17. (1) L'UIP transmet, dès que possible, à l'UIP d'un autre Etat membre de l'Union européenne qui en fait la demande, les données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par masquage conformément à l'article 26, et, si nécessaire, le résultat de tout traitement de ces données, s'il a déjà été réalisé conformément à l'article 10.

La demande, dûment motivée, peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière.

Si les données demandées ont été dépersonnalisées par masquage conformément à l'article 26, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que le transfert est nécessaire aux fins visées à l'article 12 et si elle y est autorisée par le procureur d'Etat de Luxembourg ou son délégué.

(2) Dans des cas d'urgence, les autorités compétentes des autres Etats membres, désignées conformément à l'article 7, paragraphe 1er, de la Directive (UE) 2016/661 du Parlement européen et du Conseil du 27 avril 2016 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 et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe (1) sont applicables.

(3) A titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un Etat membre a le droit de demander à ce que l'UIP obtienne des données PNR conformément à l'article 6, paragraphe (2), et les communique à l'UIP requérante.

Art. 18. L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres Etats membres de l'Union européenne des données PNR ou les résultats du traitement de ces données. Les demandes sont introduites et traitées conformément au droit national de l'Etat membre requis.

Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre Etat membre de l'Union européenne, il transmet copie de sa demande à l'UIP.

Art. 19. L'échange de données effectué en application du présent chapitre peut avoir lieu par l'intermédiaire de tous les canaux de coopération policière existant entre les autorités compétentes des Etats membres de l'Union européenne.

La langue utilisée pour la demande et l'échange des données est celle applicable au canal utilisé.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Art. 20. (1) Dans les limites de ses compétences et pour l'accomplissement de ses missions, Europol peut présenter à l'UIP, au cas par cas, par l'intermédiaire de son unité nationale, une demande électronique dûment motivée visant à obtenir des données PNR spécifiques ou le résultat du traitement de ces données:

a) lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des Etats membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes dans la matière et;

b) dans la mesure où ladite infraction relève de la compétence d'Europol.

(2) La demande énonce les motifs sur lesquels s'appuie Europol pour estimer que la transmission de données PNR ou du résultat de traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée ou à des enquêtes en la matière.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Art. 21. Sans préjudice des dispositions de l'article 35, paragraphe (1), point (d), et des articles 36 à 38 de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, l'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si:

a) l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité;

b) le transfert est nécessaire aux fins telles que définies à l'article 1er;

c) le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er;

d) les conditions prévues à l'article 17, paragraphe (1) sont remplies.

Art. 22. (1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre Etat membre de l'Union européenne à un pays non membre de l'Union européenne que si l'Etat membre auprès duquel les données ont été collectées a donné son accord au transfert.

(2) Dans des circonstances exceptionnelles, les données PNR peuvent être transférées à un pays non membre de l'Union européenne sans l'accord du pays membre de l'Union européenne auprès duquel les données ont été collectées si les conditions suivantes sont remplies:

a) 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 Etat membre de l'Union européenne ou un pays tiers;

b) l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'Etat membre de l'Union européenne, qui n'a pas pu donner son accord en temps utile, est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

Art. 23. L'UIP ne peut transférer des données PNR et les résultats du traitement de ces données aux autorités compétentes de pays non membres de l'Union européenne que dans les conditions compatibles avec la présente loi et après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte ces conditions et garanties.

Art. 24. Le délégué à la protection des données est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Art. 25. L'UIP conserve les données PNR pendant une durée maximale de cinq ans à compter du transfert par le transporteur aérien.

A l'issue de cette période de cinq ans, elle efface les données PNR de manière définitive. Cette disposition ne s'applique pas si les données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière.

Art. 26. (1) A l'expiration d'une période de six mois à compter du transfert par le transporteur aérien, l'UIP dépersonnalise les données PNR par le masquage des éléments suivants:

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;

b) l'adresse et les coordonnées;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne;

d) les informations „grands voyageurs“;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte;

f) toute donnée API qui a été recueillie.

(2) A l'expiration de la période de six mois visée au paragraphe (1), la communication de l'intégralité des données PNR n'est autorisée que sous les conditions suivantes:

a) elle est nécessaire aux fins visées à l'article 12;

b) elle a été approuvée par le procureur d'Etat de Luxembourg ou son délégué ou, si les données sont destinées à être communiquées au Service de Renseignement de l'Etat, par la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Art. 27. L'UIP ne conserve le résultat de l'évaluation réalisée en vertu de l'article 10 que le temps nécessaire pour informer les services compétents et, s'il y a lieu, les UIP des autres Etats membres de l'Union européenne de l'existence d'une concordance positive.

Lorsque, à la suite du réexamen individuel par des moyens non automatisés conformément à l'article 10, paragraphe (3), le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées en vertu de l'article 25, de manière à éviter de futures „fausses“ concordances positives.

Chapitre 10 – *Protection des données à caractère personnel*

Art. 28. Sans préjudice de l'article 41 de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, l'autorité de contrôle instituée par l'article 1er de la loi du *jj/mm/aaaa* relative à la création de la Commission nationale pour la protection des données et au régime général sur la protection des données est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 10 de la même loi et elle dispose, à cette fin, des pouvoirs prévus à l'article 16 de la même loi.

Art. 29. (1) Le responsable de l'UIP désigne un délégué à la protection des données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

(2) Le délégué à la protection des données contrôle le traitement des données PNR et met en œuvre les garanties pertinentes au sein de l'UIP.

Il informe et conseille le responsable et le personnel de l'UIP sur les obligations qui leur incombent en matière de protection des données.

Il fait office de point de contact pour les personnes concernées pour toutes les questions relatives au traitement de leurs données PNR et pour la Commission nationale pour la protection des données.

(3) Le délégué à la protection des données effectue ses missions en toute indépendance.

Il fait directement rapport au responsable de l'UIP.

Par dérogation à l'alinéa 2, et sans préjudice du paragraphe (4), alinéa 2, en cas de problèmes relevant de la protection des données, le délégué à la protection des données rapporte directement au Directeur général de la Police ou, s'il juge nécessaire, au Ministre ayant la Police dans ses attributions.

(4) Le délégué à la protection des données a accès à toutes les données traitées par l'UIP.

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données.

Art. 30. L'UIP met à la disposition du public, par les moyens de communication appropriés, les informations suivantes:

a) ses coordonnées;

b) les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données PNR;

d) le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité;

e) l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31. (1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 14 à 18 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 45 à 48 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 32. L'UIP conserve, traite et analyse les données PNR en un ou des endroits sécurisés situés sur le territoire du Luxembourg.

Art. 33. Le responsable de l'UIP met en œuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et la nature des données PNR.

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en œuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 29, paragraphe (2) de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 34. L'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

Cette documentation comprend:

a) Le nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès;

b) Les demandes formulées par les services compétents et les UIP des autres Etats membres de l'Union européenne;

c) Toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Art. 35. L'UIP tient des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

Les registres des opérations de consultation et de communication indiquent la finalité, la date et l'heure de l'opération et l'identité de la personne qui a consulté ou communiqué les données PNR ainsi que l'identité des destinataires de ces données.

Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit.

L'UIP met les registres à la disposition de l'autorité de contrôle, à la demande de celle-ci. Les registres sont conservés pendant cinq ans.

Art. 36. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe sans retard injustifié la personne concernée et l'autorité de contrôle de cette atteinte.

Chapitre 11 – *Sanctions*

Art. 37. La violation des articles 8, 15 et 36 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent alinéa sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 49, paragraphe 1er et paragraphes 3 à 5 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38. (1) Est puni d'une amende d'un montant maximum de 50.000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements y visés, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

(2) Le manquement est constaté par un procès-verbal établi par la Police grand-ducale. Copie en est transmise au transporteur aérien.

Le transporteur aérien a accès au dossier et est mis à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction.

L'amende est prononcée par le Ministre ayant la Police dans ses attributions.

(3) La décision du ministre qui est motivée est susceptible d'un recours en réformation à introduire devant le Tribunal administratif dans un délai d'un mois à compter de la notification.

*

ANNEXE I

Liste des données PNR

a) Code repère du dossier passager;

b) Date de réservation/d'émission du billet;

c) Date(s) prévue(s) du voyage;

d) Nom(s);

e) Adresse et coordonnées (numéro de téléphone, adresse électronique);

f) Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation;

g) Itinéraire complet pour le PNR concerné;

h) Informations „grands voyageurs";

i) Agence de voyages/agent de voyages;

j) Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation;

k) Indications concernant la scission/division du PNR;

l) Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée);

m) Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix;

n) Numéro du siège et autres informations concernant le siège;

o) Informations sur le partage de code;

p) Toutes les informations relatives aux bagages;

q) Nombre et autres noms de voyageurs figurant dans le PNR;

r) Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée);

s) Historique complet des modifications des données PNR énumérées aux points 1 à 18.

*

ANNEXE II

Liste des infractions visées à l'article 2, point (i)

a) Participation à une organisation criminelle;

b) Traite des êtres humains;

c) Exploitation sexuelle des enfants et pédopornographie;

d) Trafic de stupéfiants et de substances psychotropes;
e) Trafic d'armes, de munitions et d'explosifs;
f) Corruption;
g) Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union;
h) Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro;
i) Cybercriminalité;
j) Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées;
k) Aide à l'entrée et au séjour irréguliers;
l) Meurtre, coups et blessures graves;
m) Trafic d'organes et de tissus humains;
n) Enlèvement, séquestration et prise d'otage;
o) Vol organisé ou vol à main armée;
p) Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art;
q) Contrefaçon et piratage de produits;
r) Falsification de documents administratifs et trafic de faux;
s) Trafic de substances hormonales et d'autres facteurs de croissance;
t) Trafic de matières nucléaires et radioactives;
u) Viol;
v) Infractions graves relevant de la Cour pénale internationale;
w) Détournement d'avion/de navire;
x) Sabotage;
y) Trafic de véhicules volés;
z) Espionnage industriel.

*

COMMENTAIRE DES ARTICLES

Chapitre 1er – *Dispositions générales*

Ad article 1er

La présente loi a pour objet d'obliger les transporteurs aériens à transférer les données des dossiers passagers (données PNR) qu'ils recueillent à des fins commerciales, à une unité centrale nationale compétente en matière de prévention et de répression du terrorisme et de la criminalité grave et de fixer les conditions selon lesquelles ces données peuvent être traitées.

L'article 1er, outre de définir l'objet de la loi, précise et limite les finalités pour lesquelles les données PNR peuvent être traitées. Ces finalités sont la prévention et la répression des infractions terroristes et des formes graves de criminalité qui sont énumérées à l'annexe II.

Ad article 2

L'article 2, qui transpose l'article 3 de la directive, définit les notions qui sont essentielles pour la compréhension et l'application de la présente loi.

Le point a) précise ce qu'il y a lieu d'entendre par „transporteur aérien". Il s'agit de toute entreprise de transport aérien qui possède une licence d'exploitation lui permettant d'assurer le transport aérien de personnes. Pour la définition des notions „entreprise de transport" et „licence d'exploitation" il y a lieu de se référer aux définitions figurant dans les textes communautaires relatifs à la navigation aérienne, et en particulier le règlement 1008/2008 du Parlement européen et du Conseil du 24 septembre 2008 qui établit des règles communes pour l'exploitation de services aériens dans la Communauté. L'entreprise y est définie comme une personne physique ou morale, poursuivant ou non un but lucratif, ou tout organisme officiel doté ou non de la personnalité juridique. La licence d'exploitation est une

autorisation délivrée par l'autorité compétente pour l'octroi des licences à une entreprise l'autorisant à fournir des services aériens selon les mentions figurant dans la licence. Le service aérien est défini comme un vol ou une série de vols transportant, à titre onéreux et/ou en vertu d'une location des passagers, du fret et/ou du courrier.

Relèvent du champ d'application de la présente loi toutes les entreprises de transport aérien qui possèdent une licence d'exploitation respectivement, pour les entreprises établies dans des Etats non membres de l'Union européenne, une habilitation équivalente les autorisant à transporter des personnes à titre onéreux ou en vertu d'un contrat de location.

Est ensuite défini, au point b), le terme de „passager". Cette notion est très importante dans la mesure où elle délimite le cercle de personnes dont les données doivent être transmises.

Le point c) précise ce qu'il y a lieu d'entendre par „dossier passager". Cette définition est à voir ensemble avec la définition figurant au point f). Les informations visées dans la définition du dossier passager sont les données PNR. Il s'agit d'informations non vérifiées fournies par les passagers et recueillies par les transporteurs aux fins de la réservation et de la procédure d'enregistrement.

Les points d) et e) n'appellent pas de commentaire particulier.

Le point g) est relatif au mode de transfert des données PNR des transporteurs aériens vers l'autorité publique. Il importe de noter dans ce contexte qu'il existe deux méthodes possibles de transfert, la méthode dite „pull", par laquelle les autorités compétentes peuvent accéder au système de réservation du transporteur aérien et en extraire copie des données PNR requises, et la méthode dite „push", par laquelle les transporteurs aériens transmettent les données PNR à l'autorité requérante, ce qui leur permet de garder le contrôle sur les données. La directive impose aux Etats membres d'adopter la méthode „push" qui est réputée offrir un niveau plus élevé de protection des données.

Les points h) et i) définissent ce qu'il y a lieu d'entendre par „infractions terroristes" et „formes graves de criminalité" au sens de la présente loi. La liste des infractions énumérées à l'annexe II de la directive est reprise telle quelle dans le présent projet de loi. La directive a retenu les seules infractions pour la prévention et l'élucidation desquelles l'exploitation de données PNR a été jugée pertinente. C'est pour cette raison que la liste figurant à l'annexe II du projet de loi, bien que se couvrant largement avec la liste des infractions pour lesquelles un mandat d'arrêt européen est exécuté sans contrôle de la double incrimination, n'est pas identique à la liste du mandat d'arrêt européen qui comprend par ailleurs le racisme et la xénophobie, l'escroquerie, le racket et l'extorsion de fonds et l'incendie volontaire.

Chapitre 2 – *Unité d'information passagers*

Ad article 3

Les Etats membres sont tenus, en vertu de l'article 4 de la directive, d'instituer une „unité d'information passagers", en abrégé „UIP", qui se charge de recueillir les données transférées par les transporteurs aériens, de les traiter, les conserver, les transmettre aux services nationaux compétents et les échanger avec les unités correspondantes des autres Etats membres, avec Europol et avec les pays tiers.

La directive laisse le choix aux Etats membres de mettre en place une autorité compétente en matière de prévention et de répression d'infractions terroristes et de formes graves de criminalité ou de désigner une autorité existante ou une antenne d'une autorité existante, compétente en cette matière, pour assurer le rôle d'unité d'information passagers.

Le Gouvernement a décidé d'intégrer cette unité à la Police grand-ducale, et plus précisément, au Service des Relations internationales. Compte tenu du fait que les détails de l'organisation future de la Police grand-ducale seront, en principe, à l'avenir arrêtés par le Directeur général de la Police, la présente loi se limite à indiquer que l'UIP est mise en place au sein de la Police.

Ad article 4

L'alinéa 1er désigne le responsable de l'UIP comme responsable du traitement des données PNR.

L'alinéa 2 fixe la composition de l'UIP. L'article 4, paragraphe 3, de la directive prévoit la possibilité pour les autorités qui sont habilitées à demander et à recevoir des données PNR, à détacher du personnel à l'UIP. Le Gouvernement a décidé de faire usage de cette faculté en prévoyant le détachement de personnel de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat à l'UIP. Le présent article est ainsi à mettre en relation avec l'article 13 qui énumère les services nationaux compétents pour recevoir et demander des données PNR.

Il importe de préciser que le personnel de l'UIP, qu'il y soit affecté ou détaché, ne traite les données PNR que dans les limites des missions légales de l'Administration pour le compte de laquelle il agit au sein de l'UIP.

A défaut de dispositions particulières dans la présente loi, les détachements à l'UIP sont effectués d'après les règles prévues par la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat en matière de détachements.

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Ad article 5

Le présent article, qui transpose l'article 8, paragraphe 1er de la directive, oblige les transporteurs aériens à transférer leurs données PNR à l'UIP. Le considérant 8 de la directive explique que la directive ne doit pas imposer aux transporteurs de recueillir ou de conserver des données supplémentaires à celles qu'ils recueillent et traitent déjà pour leur propre usage commercial. Il a pour cette raison été précisé que les transporteurs aériens ne sont obligés de transférer que les données *„dont ils disposent"*.

Les transporteurs aériens sont tenus, en vertu de l'article 106 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration et du règlement grand-ducal pris en son exécution, de transmettre au Service de contrôle à l'aéroport de la Police grand-ducale, à des fins de contrôle d'immigration, les données API *(Advanced Passenger Information)* des passagers en provenance d'un pays non membre de l'Union européenne qu'ils débarquent au Luxembourg. Les données API sont les informations biographiques extraites de la partie d'un passeport lisible par machine et contiennent le nom, le lieu de naissance et la nationalité du titulaire, le numéro du passeport et sa date d'expiration. Etant donné que les données API sont énumérées dans la directive et dans le projet de loi parmi les données PNR que les transporteurs aériens sont tenus de transmettre à l'UIP, il a été jugé nécessaire de faire référence à la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration afin de préciser que l'obligation imposée aux transporteurs aériens en vertu de la présente loi ne les dispense pas de transmettre, à des fins de contrôle d'immigration, les données API au service de Contrôle à l'Aéroport de la Police grand-ducale.

L'article 5 précise par ailleurs que les données sont transférées à l'UIP par la méthode „push". Il est renvoyé à ce propos au commentaire de l'article 2, point g.

L'article 5 détermine ensuite les vols pour lesquels les données doivent être transférées à l'UIP. Il s'agit de tous les vols en provenance et à destination de l'aéroport de Luxembourg, que leur origine ou leur destination se situent ou non sur le territoire de l'Union européenne. Cette disposition est à voir ensemble avec l'article 2, point b) qui définit comme passager non seulement les personnes pour lesquelles le Luxembourg est la destination finale, mais également celles qui sont en correspondance ou en transit au Luxembourg.

L'alinéa 2 vient préciser que pour les vols en partage de code, pratique commerciale qui consiste à ce que deux ou plusieurs compagnies aériennes partagent un vol, l'obligation de transfert repose sur le transporteur aérien qui effectue le vol.

Ad article 6

Le paragraphe 1er transpose l'article 8, paragraphe 3 de la directive, et précise à quels moments les données doivent en principe être transférées à l'UIP. En principe, car il peut arriver, pour des achats de billets à la dernière minute, que le transporteur aérien ne dispose pas encore des données PNR d'un passager à l'échéance H-48. Il est évident que le transporteur aérien ne peut transférer que les données dont il dispose et à partir du moment où il en dispose. L'obligation fixée par le présent article est dès lors à mettre en relation avec l'article 5, paragraphe 1er, qui oblige le transporteur aérien à transférer les données „dont il dispose".

L'alinéa 2 précise que, si les données ont déjà été transférées une première fois 48 heures et une seconde fois 24 heures avant le départ d'un vol, le transporteur peut limiter le troisième transfert à une mise à jour des données transmises auparavant. Il ne s'agit toutefois pas d'une obligation, le transporteur étant libre de transférer une nouvelle fois l'ensemble des données.

Si le paragraphe 1er concerne le transfert de données PNR d'office aux échéances y définies, le paragraphe 2 prévoit la possibilité pour l'UIP de solliciter des données PNR en dehors de ces échéances, au cas par cas, lorsqu'il existe une menace précise et réelle d'infraction.

Ad article 7

L'article 7 est relatif au procédé technique par lequel les données doivent être transférées à l'UIP. Ce transfert a lieu de manière électronique au moyen des protocoles communs et des formats de données qui auront été arrêtés par la Commission européenne et publiés au Journal officiel de l'Union européenne.

A titre exceptionnel, en cas de défaillances techniques, les transporteurs peuvent recourir à d'autres moyens techniques qui doivent toutefois assurer la sécurité des données transférées.

Chapitre 4 – *Traitement des données PNR*

Ad article 8

Conformément à l'article 13, paragraphe 4 de la directive, cet article interdit le traitement de données sensibles et oblige l'UIP, pour le cas où de telles données venaient à être transférées par un transporteur aérien, à les effacer dès réception et de manière définitive.

Ad article 9

L'UIP ne peut traiter que les données énumérées à l'annexe I du présent projet de loi et doit effacer, dès réception et de manière définitive, toute donnée supplémentaire qu'elle se verrait transférer.

Ad article 10

Les articles 10, 11 et 12 définissent les différentes manières dont les données PNR peuvent être utilisées dans le cadre de la prévention et la lutte contre le terrorisme et les formes graves de criminalité. Ils portent transposition de l'article 6, paragraphes 1 à 6 et paragraphe 9 de la directive.

Les données PNR peuvent ainsi être utilisées (art. 10) pour réaliser des évaluations de risques des passagers avant leur départ ou leur arrivée sur le territoire luxembourgeois afin de prévenir une infraction, de surveiller ou d'arrêter des personnes avant qu'une infraction ne soit commise ou parce qu'une infraction a été commise ou est en train de l'être.

Cette évaluation des risques est réalisée, d'une part, par la mise en corrélation des données PNR avec les données figurant dans les banques de données pertinentes nationales et internationales, qui sont exploitées par les services compétents ou qui leurs sont accessibles dans le cadre de leurs attributions respectives telles que par exemple le Schengen Information System ou Interpol. Cette mise en corrélation permettra notamment de déceler des personnes à propos desquelles les services compétents disposent d'indices qu'elles se préparent à commettre des actes terroristes ou des infractions graves telles que celles-ci sont définies à l'annexe II du présent projet de loi ou qui sont recherchées dans le cadre d'une procédure judiciaire.

L'évaluation prévue à l'article 10 consiste d'autre part à comparer les données PNR par rapport à des critères préétablis, afin d'identifier des personnes auparavant „inconnues", c'est-à-dire qui jusque-là n'étaient pas soupçonnées de participation à une infraction grave ou à un acte de terrorisme, mais dont l'analyse des données indique qu'elles peuvent être impliquées dans une infraction de cette nature et qu'elles devraient être soumises à un examen approfondi par les autorités compétentes. La confrontation en temps réel des données PNR à ces critères permet de prévenir ou de détecter des infractions. Ces critères peuvent concerner par exemple le pays de destination ou de départ, combiné à certaines autres informations telles que le mode de paiement, le poids du bagage, ou l'itinéraire choisi.

La comparaison des données par rapport à des critères préétablis est subordonnée à des règles très strictes, qui sont énoncées au paragraphe 2, alinéa 2, à savoir:

1. L'évaluation ne doit pas être réalisée de manière discriminatoire;
2. Les critères doivent être établis en coopération avec les services compétents;
3. Les critères doivent être réexaminés à des intervalles réguliers;
4. Les critères doivent être ciblés, proportionnés et spécifiques par rapport au type d'infraction qu'ils sont supposés révéler;
5. Les critères ne doivent pas être fondés sur 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.

Lorsque l'UIP obtient une correspondance positive, soit après comparaison avec les banques de données ou par rapport à des critères préétablis, elle en informe le ou les services compétents afin qu'ils

prennent les mesures qu'ils jugent appropriées. Si l'UIP estime qu'un autre Etat membre a besoin d'être informé, elle transmet toutes les données qu'elle juge nécessaires et pertinentes à l'unité d'information passagers de cet Etat membre, conformément à ce qui est prévu à l'article 16 du présent projet de loi et exigé par l'article 9, paragraphe 1er de la directive.

Le paragraphe 3 oblige l'UIP à faire réexaminer individuellement, par une personne physique, toute concordance positive obtenue par des moyens automatisés. L'UIP ne peut transmettre des données PNR ou des résultats de traitements de données PNR à des services nationaux compétents et à une UIP étrangère qu'après avoir effectué cette vérification.

Le paragraphe 4 prévoit la transmission spontanée des correspondances positives par l'UIP aux services nationaux compétents. Cette transmission sera en relation avec une personne pour laquelle il existe une raison de croire qu'elle est liée à une activité criminelle rentrant dans le champ d'application de la présente loi, ou parce que son nom apparaît dans une base de données, ou parce que son *„travel pattern"* ou son comportement correspond à un des critères prédéterminés. Il en est de même pour la transmission spontanée de correspondances positives aux UIP des autres Etat membres.

Les paragraphes 5 et 6 visent à préciser que le présent projet de loi ne modifie pas, ni n'affecte les règles de l'UE actuelles définissant les modalités des contrôles aux frontières, pas plus que les règles de l'UE applicables aux entrées sur le territoire de l'Union et aux sorties de celui-ci.

Ad article 11

Outre la réalisation d'évaluations telles que décrites à l'article 10, les données PNR peuvent être traitées pour établir et pour mettre à jour, si nécessaire, les critères utilisés pour l'évaluation des risques. Ainsi par exemple, une analyse de données PNR peut donner des indications sur les itinéraires les plus empruntés, ou de nouveaux itinéraires empruntés pour la traite des êtres humains ou le trafic de drogues, autant d'éléments qui peuvent être intégrés dans les critères d'évaluation.

Ad article 12

Les données PNR peuvent par ailleurs servir comme éléments de preuve dans le cadre d'enquêtes judiciaires. A titre d'exemple, les données PNR peuvent aider à orienter les enquêteurs sur le lieu de séjour d'une personne suspecte au moment où les faits ont été commis.

Chapitre 5 – *Services compétents*

Ad article 13

Cet article dresse la liste des services nationaux qui peuvent solliciter des données PNR auprès de l'UIP et qui sont destinataires, selon leurs compétences respectives, des concordances positives trouvées lors des évaluations des risques. Il ne porte pas préjudice aux compétences des autorités judiciaires telles que celles-ci sont définies par le Code de procédure pénale.

Il échet de préciser que tous les policiers n'ont pas besoin de recourir à des données PNR dans l'exécution de leurs missions, ces informations n'étant destinées qu'à être utilisées dans le cadre de la recherche d'infractions terroristes et d'infractions graves dont la liste figure en annexe de la présente loi. Il en est de même pour les agents du Service de Renseignement de l'Etat et de l'Administration des Douanes et Accises, qui ne peuvent obtenir ou demander des données PNR ou des résultats de traitements de ces données que pour autant qu'ils agissent dans le cadre respectivement de la prévention ou de la recherche des infractions rentrant dans le champ d'application de la présente loi. Il a pour cette raison été précisé que les services compétents énumérés à l'article 13 ne peuvent demander et obtenir des données PNR que dans les limites de leurs attributions légales et du besoin d'en connaître.

Ad article 14

L'article 14 transpose l'article 7, paragraphes 4 et 5 de la directive. Il interdit aux services compétents d'utiliser les données PNR et les résultats de traitements de telles données à des fins autres que la prévention ou la répression des infractions terroristes et des infractions énumérées à l'annexe II du présent projet de loi.

L'alinéa 2 vient toutefois préciser que l'interdiction visée à l'alinéa 1er n'empêche pas la Police ou l'Administration des Douanes d'enquêter sur d'autres infractions qui seraient détectées à la suite d'un traitement de données PNR et qui ne rentreraient pas dans le champ d'application de la présente loi.

Ad article 15

Cet article, qui porte transposition de l'article 7, paragraphe 6, de la directive précise que les autorités compétentes ne peuvent prendre aucune décision ayant des conséquences juridiques pour une personne ou l'affectant gravement sur base du traitement automatisé des données PNR.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Ad article 16

Les articles 16 et 17 transposent l'article 9, paragraphes 1 à 4, de la directive.

Lors des négociations en trilogues, une très grande importance avait été accordée à l'échange d'informations entre Etats membres. Les articles 16 et 17 sont ainsi parmi les éléments-clés du système PNR européen.

L'article 16 règle la transmission d'office d'informations aux UIP d'autres Etats membres, tandis que l'article 17 règle la transmission d'informations sur demande.

L'article 16, alinéa 1er prévoit que, lorsque l'UIP luxembourgeoise a identifié une personne susceptible d'être impliquée dans une infraction terroriste ou une forme grave de criminalité, et qu'il existe un lien avec un ou plusieurs autres Etats membres, elle transmet les données qu'elle juge nécessaires et pertinentes à l'unité ou aux unités correspondantes.

Le 2e alinéa envisage le cas de figure où une UIP étrangère transmet à l'UIP luxembourgeoise des informations relatives à des personnes qu'elle a identifiées sur base de l'évaluation des risques comme pouvant être impliquées dans une infraction tombant dans le champ d'application de la directive. Les conditions de transmission de ces données ne relèvent pas de la législation luxembourgeoise, mais des législations respectives des Etats membres qui ont réalisé l'évaluation. La présente disposition vise à préciser que, lorsque l'UIP luxembourgeoise reçoit de telles informations, elle les continue aux services nationaux compétents, conformément à ce qui est prévu à l'article 9, paragraphe 1er, 2e phrase de la directive.

Ad article 17

L'article 17 définit les conditions selon lesquelles les autorités des autres Etats membres peuvent solliciter des données PNR ou des résultats du traitement de ces données auprès de l'UIP luxembourgeoise.

Excepté les circonstances exceptionnelles prévues au paragraphe 2, les demandes et les échanges de données ont toujours lieu par l'intermédiaire des UIP. Autrement dit, un service compétent d'un autre Etat membre ne peut pas, en principe, solliciter directement des données auprès de l'UIP luxembourgeoise, mais doit s'adresser à sa propre UIP.

L'UIP d'un autre Etat membre de l'Union européenne peut demander à l'UIP luxembourgeoise de recevoir des données PNR ou des résultats de traitements de données PNR que cette dernière est tenue de transmettre dès que possible. La dernière partie du paragraphe 1er, alinéa 1er vise à préciser que, dans l'hypothèse où l'évaluation des risques n'aurait pas encore été réalisée par notre UIP, l'UIP étrangère ne peut pas exiger qu'elle le soit.

Le paragraphe 1er distingue entre deux cas de figure envisagés respectivement à l'alinéa 1er (les données demandées n'ont pas encore été masquées) et à l'alinéa 2 (la demande intervient après écoulement des 6 mois au terme desquels certaines données doivent être masquées). L'UIP requérante doit en tout état de cause motiver les raisons de sa demande. Si la demande porte sur des données qui ont déjà été masquées, les données ne seront communiquées que si l'UIP luxembourgeoise estime qu'il existe des motifs raisonnables de croire que le transfert est nécessaire et obtient l'autorisation afférente du procureur d'Etat ou de son délégué.

Le paragraphe 2 prévoit que dans des cas d'urgence, et par exception au principe que les demandes et échanges de données PNR ont lieu par l'intermédiaire de l'UIP, les autorités compétentes des autres Etats membres peuvent directement demander des données PNR à l'UIP luxembourgeoise. La directive oblige les Etats membres à notifier leurs autorités compétentes à la Commission européenne, qui se charge d'en faire la publication au Journal officiel de l'Union européenne. L'UIP luxembourgeoise ne transmettra des données qu'aux autorités compétentes qui figurent sur la liste publiée au Journal officiel de l'Union européenne. A l'instar des demandes introduites par les UIP, les demandes des autorités

compétentes doivent être motivées d'après les circonstances particulières de l'espèce. Par ailleurs, les conditions spéciales prévues pour la communication des données déjà masquées aux UIP s'appliquent également aux demandes formulées directement par les services compétents.

Le paragraphe 3 prévoit la possibilité pour une UIP étrangère de demander à l'UIP luxembourgeoise de solliciter des données auprès d'un transporteur aérien en dehors des délais auxquels les transporteurs sont tenus de transférer les données. Cette faculté est toutefois limitée aux cas où il existe une menace précise et réelle qu'un acte terroriste ou une infraction grave sera commis.

Ad article 18

L'article 18 vise le cas où les autorités luxembourgeoises souhaitent obtenir des données recueillies ou traitées par l'UIP d'un autre Etat membre. Elles doivent dans ce cas s'adresser à l'UIP de l'Etat membre concerné en respectant les conditions fixées par la législation nationale de cet Etat membre.

L'alinéa 2 envisage le cas de figure où un service compétent national s'adresse directement à une UIP étrangère. En effet, si les conditions d'obtention des données sont régies par la législation de l'Etat requis, il importe toutefois de préciser dans notre législation nationale que le service national requérant doit adresser une copie de sa demande à l'UIP luxembourgeoise, conformément à ce qui est exigé par l'article 9, paragraphe 3 de la directive.

Ad article 19

Cet article est relatif aux modalités techniques d'échange des informations entre Etats membres et ne suscite pas de commentaire particulier.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Ad article 20

L'article 20 définit les conditions selon lesquelles Europol peut demander des données à l'UIP et transpose l'article 10 de la directive.

La demande d'Europol doit transiter par son unité nationale, le service de police judiciaire de la Police grand-ducale en l'occurrence, et être motivée. Europol ne peut solliciter des données PNR ou des résultats de traitements que dans les limites de ses compétences et des objectifs qui lui sont assignés. Pour les infractions relevant de la compétence d'Europol, il est renvoyé au règlement 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Ad article 21

L'article 21, transposant l'article 11, paragraphe 1er de la directive, règle les conditions du transfert de données PNR à un pays non membre de l'Union européenne.

Un tel transfert est d'abord subordonné à l'existence d'une décision d'adéquation de la Commission européenne ou, en l'absence d'une telle décision, à l'existence de garanties appropriées.

Les autres conditions, respectivement énoncées aux points a, b et c, sont que la demande émane d'une autorité ayant pour mission la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité, que les données soient sollicitées à ces fins et que l'autorité n'accepte de transférer les données reçues à un autre pays tiers qu'à ces seules fins.

Le point d) précise que les conditions régissant les transferts de données PNR aux UIP des autres Etats membres sont également applicables aux transferts de données aux Etats tiers.

Ad article 22

L'article 22, transposant l'article 11, paragraphe 2 de la directive, envisage le transfert de données recueillies auprès d'un autre Etat membre à un pays tiers. Un tel transfert ne peut avoir lieu que si les

conditions définies à l'article 21 sont remplies et si l'Etat membre auprès duquel les données ont été recueillies a donné son accord (paragraphe 1er).

Le paragraphe 2 prévoit toutefois, à titre exceptionnel, que s'il existe une menace précise et réelle et si l'accord n'a pas pu être obtenu en temps utile, les données puissent être transférées sans l'accord préalable de l'Etat membre d'où proviennent les données.

Ad article 23

L'article 23 pose une condition supplémentaire aux transferts de données vers des pays tiers qui s'applique dans les cas de figure prévus respectivement aux articles 21 et 22.

Ad article 24

Cet article n'appelle pas de commentaire particulier.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Ad article 25

L'article 25 porte transposition de l'article 12, paragraphes 1er et 4 de la Directive. Il fixe la durée maximale de conservation des données PNR.

L'UIP ne peut conserver les données que pendant une période maximale de 5 ans qui commence à courir à partir du moment où les données ont été transférées. Etant donné que la loi prévoit trois transferts consécutifs de données, le premier ayant lieu deux jours avant le départ programmé du vol, le deuxième un jour avant le départ et le dernier immédiatement après la clôture du vol, il importe de préciser que c'est le dernier transfert prévu à l'article 6, paragraphe 1er du présent projet de loi qui fait courir le délai de cinq ans.

Au terme de la période de cinq ans, l'UIP doit effacer les données de façon irrémédiable. Cette disposition ne s'applique toutefois pas aux données qui ont été transmises aux services compétents et qui sont utilisées dans le cadre d'enquêtes ou de poursuites.

Ad article 26

Conformément à l'article 12, paragraphe 2 de la directive, le présent article oblige l'UIP à masquer les informations qui peuvent servir à identifier directement la personne à laquelle se rapportent les données PNR. Le masquage est une technique qui consiste à rendre ces éléments de données invisibles, sans toutefois les altérer. Des recherches automatisées restent ainsi possibles parmi les données masquées et des hits peuvent être générés. Toutefois les informations permettant d'identifier la personne à laquelle les données se rapportent ne sont pas affichées sur l'écran. Pour pouvoir visualiser ces informations, l'UIP doit obtenir l'accord du procureur d'Etat ou de son délégué ou, si la requête émane du Service de Renseignement de l'Etat, l'accord de la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de Renseignement de l'Etat.

Le système technique devra été conçu de manière à ce que les données masquées ne puissent être consultées qu'après que l'accord de l'autorité compétente désignée en vertu du présent article aura été obtenu et qu'il soit possible de retracer les opérations de démasquage effectuées.

Des prescriptions de service interne à l'UIP devront établir une procédure à suivre par l'opérateur lorsqu'un *hit* est généré parmi des données PNR masquées.

Ad article 27

L'article 27, portant transposition de l'article 12, paragraphe 5 de la directive, est relatif à la durée de conservation des résultats des traitements de données PNR obtenus suite à une évaluation réalisée sur base de l'article 10. Ces résultats ne doivent être conservés par l'UIP que le temps nécessaire pour informer les services compétents et les UIP des autres Etats membres concernés de l'existence d'une correspondance positive.

L'alinéa 2 vise l'hypothèse où il s'est avéré, après vérification manuelle, que la concordance positive générée automatiquement était fausse. Pour éviter que les mêmes données ne génèrent d'autres fausses concordances positives à l'avenir, les résultats de ces traitements peuvent être conservés par l'UIP aussi longtemps que les données de base n'ont pas été effacées.

Chapitre 10 – *Protection des données à caractère personnel*

Ad article 28

L'article 15 de la Directive prévoit que dans chaque Etat membre l'autorité de contrôle nationale visée à l'article 25 de la décision-cadre 2008/977/JAI est chargée de fournir des conseils sur l'application, sur son territoire, des dispositions adoptées par les Etats membres en vertu de la présente directive et de surveiller l'application de celles-ci. Etant donné que les références faites à la décision-cadre 2008/977/JAI s'entendent comme des références faites à la législation actuellement en vigueur et à la législation qui la remplacera, que la décision-cadre 2008/977 est remplacée par la directive (UE) 2016/680 DU PARLEMENT EUROPEEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil et que la directive 2016/680 est transposée en droit luxembourgeois par le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, il échet, pour satisfaire à la directive, de désigner la même autorité de contrôle que celle prévue par le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. La Commission nationale pour la protection des données sera ainsi compétente pour contrôler le respect des dispositions de la présente loi en ce qui concerne la protection des données à caractère personnel.

La référence à l'article 41 du projet de loi de transposition de la Directive 2016/680 vise à préciser que les traitements de données PNR effectués par le ministère public sont soumis au contrôle de l'autorité de contrôle judiciaire.

Ad article 29

L'article 29 transpose l'article 5 et l'article 6, paragraphe 6 de la directive.

La directive qu'il s'agit de transposer prévoit un certain nombre de garanties destinées à assurer la protection des données PNR, parmi lesquelles la désignation obligatoire d'un délégué à la protection des données au sein de l'UIP.

Le présent article, outre de définir les missions du délégué à la protection des données, comporte un certain nombre de dispositions visant à garantir que celui-ci soit mis en mesure d'exercer ses missions de manière indépendante et effective, comme exigé par la directive. Ainsi, la personne qui est appelée à exercer cette fonction doit disposer d'une expertise en matière de protection des données (paragraphe 1er, alinéa 2) et avoir accès à toutes les données traitées par l'UIP.

Le paragraphe 3 consacre expressément l'indépendance du délégué à la protection des données. Cette disposition n'interdit pas que délégué soit issu du cadre du personnel de la Police grand-ducale, mais il appartiendra à la Police de prendre les mesures adéquates pour garantir que l'indépendance soit garantie. Ainsi, quelle que soit la carrière, policière ou civile, dont est issu le délégué et quelle que soit sa position hiérarchique par rapport au personnel de l'UIP, il importe de veiller à ce qu'il n'ait à rapporter qu'au responsable de l'UIP et qu'il ne reçoive d'instructions d'aucun membre du personnel de l'UIP. L'alinéa 3 prévoit que, dans certains cas, le délégué rapporte directement au Directeur général de la Police ou au Ministre. Il n'en reste pas moins que, si le délégué estime nécessaire, dans un cas particulier, de rapporter directement au directeur général ou au Ministre, il dénonce un éventuel traitement illicite parallèlement à l'autorité de contrôle.

Le délégué à la protection des données n'a pas seulement une mission de contrôle (paragraphe 2, alinéa 1er), mais également un rôle d'information et de conseil (alinéa 2). Le délégué fait par ailleurs office de point de contact pour les citoyens et pour la Commission nationale de protection des données (CNPD).

Ad article 30

L'article 30 oblige l'UIP à mettre à disposition du public un certain nombre d'informations dont, notamment, l'information sur les droits des personnes dont les données sont traitées en vertu de la présente loi.

Cette information peut se faire par n'importe quel moyen de communication approprié. En France, par exemple, les informations pertinentes en relation avec le traitement des données PNR et les droits des personnes sont publiée sur le site internet de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Ad article 31

Cet article transpose l'article 13, paragraphe 1er de la directive.

Les droits des personnes sont définis par référence aux articles pertinents du projet de loi portant transposition de la directive sur la protection des données pénales. Il s'agit du droit d'accès (article 14) et du droit de rectification ou d'effacement des données à caractère personnel et de la limitation du traitement prévu à l'article 16. Les limitations au droit d'accès prévues à l'article 15 et les règles relatives à l'exercice des droits fixées par l'article 17 du projet de loi auquel il est fait référence sont applicables aux données PNR.

Les personnes dont les données sont traitées en vertu de la présente loi disposent par ailleurs du droit d'introduire une réclamation auprès de la CNPD (art. 45), d'un droit de recours juridictionnel contre une décision de cette autorité (art. 46), un droit à un recours juridictionnel contre le responsable du traitement (art. 47) et le droit de se faire représenter (art. 48).

Ad article 32

Conformément à l'article 6, paragraphe 8 de la directive, cet article oblige l'UIP à traiter et à analyser les données en des endroits sécurisés situés sur le territoire du Grand-Duché de Luxembourg.

Ad article 33

Cet article, portant transposition de l'article 13, paragraphes 2 et 7 de la directive, impose à l'UIP de prendre des mesures et procédures techniques nécessaires pour assurer un niveau élevé de sécurité des données.

Le paragraphe 2 impose à l'UIP un certain nombre de mesures à prendre en ce qui concerne en particulier le traitement automatisé des données. Il s'agit de mesures destinées à:

(a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations);

(b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);

(c) empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation);

(d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);

(e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données);

(f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission);

(g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);

(h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport);

(i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration);

(j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

Ad article 34

L'article 34 porte transposition de l'article 13, paragraphe 5 de la directive. Il impose l'obligation pour l'UIP de conserver une trace documentaire relative à ses systèmes et procédures de traitement.

L'alinéa 2 énumère les éléments qui doivent figurer dans cette documentation.

Ad article 35

Le traitement des données PNR doit faire l'objet d'une journalisation, conformément à ce qui est prévu à l'article 13, paragraphe 6 de la directive. Il s'agit de permettre le traçage des traitements de données effectués afin qu'il soit possible d'identifier la personne qui a consulté des données, les données consultées, le moment et la finalité de cette consultation ainsi que l'identité des destinataires des données.

L'alinéa 3 précise les finalités de cette journalisation.

Les registres doivent être mis à la disposition de l'autorité de contrôle lorsqu'elle en fait la demande.

L'alinéa dernier oblige l'UIP à conserver les registres pendant une durée de cinq ans.

Ad article 36

L'article 36, portant transposition de l'article 13, paragraphe 8 de la directive, oblige l'UIP à informer la personne concernée et l'autorité de contrôle lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection de ces données ou d'affecter négativement la vie privée de la personne.

Chapitre 11 – *Sanctions*

Ad article 37

Les articles 37 et 38 transposent l'article 14 de la directive.

L'alinéa 1er de l'article 37 prévoit des sanctions pénales pour les infractions aux dispositions prévues aux articles 8, 15 et 36 de la présente loi. Ainsi, le présent projet de loi prévoit des sanctions pénales pour les mêmes violations que celles pour lesquelles le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale établit des sanctions pénales.

Les violations des autres dispositions applicables en matière de protection des données à caractère personnel sont punies de sanctions administratives telles que prévues par le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Ad article 38

L'article 38 prévoit des sanctions administratives à l'égard des transporteurs aériens qui ne respectent pas les obligations qui leur sont imposées par la présente loi, à savoir transférer les données à l'UIP à des échéances prédéterminées ou sur demande, selon des modalités précises et dans des formats prédéfinis.

Dans la mesure où la directive impose aux Etats membres de fixer des sanctions effectives, proportionnées et dissuasives à l'égard des transporteurs et s'inspirant des textes français, allemand et belge, le Gouvernement a retenu une amende d'un montant maximal de 50.000 euros.

Le paragraphe 2 décrit la procédure à suivre en cas de manquement par un transporteur aérien. Le manquement est constaté par un procès-verbal adressé au Ministre ayant la Police dans ses attributions. Avant de prononcer une sanction, le Ministre informe le transporteur aérien de son intention de prononcer une amende en indiquant le montant de l'amende. Le transporteur a accès à son dossier et dispose d'un délai d'un mois à compter de la notification du projet de sanction par le Ministre pour présenter des observations écrites.

La décision du Ministre doit être motivée et notifiée à l'intéressé. Ce dernier dispose d'un délai d'un mois à compter de la notification pour introduire un recours en réformation devant le tribunal administratif.

*

TABLEAU DE CORRESPONDANCE

Directive (UE) 2016/681	*Projet de loi*
Art. 1er	
Art. 1	Art. 1
Art. 2	
Art. 2	//
Art. 3	
Art. 3	Art. 2
Art. 4	
Art. 4 paragraphe 1er	Art. 3
Art. 4 paragraphe 2	
Art. 4 paragraphe 3	Art. 4, alinéa 2
Art. 4 paragraphe 4	//
Art. 4 paragraphe 5	
Art. 5	
Art. 5, paragraphe 1er	Art. 29, paragraphe 1, alinéa 1er et paragraphe 2, alinéas 1er et 2
Art. 5, paragraphe 2	Art. 29, paragraphe 1er, alinéa 2 et paragraphe 3
Art. 5, paragraphe 3	Art. 29, paragraphe 2, alinéa 3
Art. 6	
Art. 6, paragraphe 1er	Art. 9
Art. 6, paragraphe 2	Art. 10, paragraphe 1er, art. 11, art. 12
Art. 6, paragraphe 3	Art 10, paragraphe 2
Art. 6, paragraphe 4	Art. 10, paragraphe 2
Art. 6, paragraphe 5	Art. 10, paragraphe 3
Art. 6, paragraphe 6	Art. 10, paragraphes 3 et 4
Art. 6, paragraphe 7	Art. 29, paragraphe 4
Art. 6, paragraphe 8	Art. 32
Art. 6, paragraphe 9	Art. 10, paragraphes 5 et 6
Art. 7	
Art. 7 paragraphe 1er	Art. 13
Art. 7 paragraphe 2	Art. 13
Art. 7 paragraphe 3	//
Art. 7 paragraphe 4	Art. 14, alinéa 1er
Art. 7 paragraphe 5	Art. 14, alinéa 2
Art. 7 paragraphe 6	Art. 15 et art. 8
Art. 8	
Art. 8, paragaphe 1er	Art. 5
Art. 8, paragraphe 2	//
Art. 8, paragraphe 3	Art. 6, paragraphe 1er, alinéa 1er et art. 7
Art. 8, paragraphe 4	Art. 6, paragraphe 1er, alinéa 2
Art. 8, paragraphe 5	Art. 6, paragraphe 2

Directive (UE) 2016/681	*Projet de loi*
Art. 9	
Art. 9, paragraphe 1er	Art. 16
Art. 9, paragraphe 2	Art. 17, paragraphe 1er
Art. 9, paragraphe 3	Art. 17, paragraphe (2) et 18 alinéa 2
Art. 9, paragraphe 4	Art. 17, paragraphe 3
Art. 9, paragraphe 5	Art. 19
Art. 10	
Art. 10, paragraphe 1er	Art. 20, paragraphe 1er
Art. 10, paragraphe 2	Art. 20
Art. 10, paragraphe 3	//
Art. 10, paragraphe 4	//
Art. 11	
Art. 11, paragraphe 1er	Art. 21
Art. 11, paragraphe 2	Art. 22
Art. 11, paragraphe 3	Art. 23
Art. 11, paragraphe 4	Art. 24
Art. 12	
Art. 12, paragraphe 1er	Art. 25, alinéa 1er
Art. 12, paragraphe 2	Art. 26, paragraphe 1er
Art. 12, paragraphe 3	Art. 26, paragraphe 2
Art. 12, paragraphe 4	Art. 25, alinéa 2
Art. 12, paragraphe 5	Art. 27
Art. 13	
Art. 13, paragraphe 1er	Art. 30, point e) at art. 31
Art. 13, paragraphe 2	Art. 33, alinéa 2
Art. 13, paragraphe 3	//
Art. 13, paragraphe 4	Art. 8
Art. 13, paragraphe 5	Art. 34
Art. 13, paragraphe 6	Art. 35
Art. 13, paragraphe 7	Art. 33, alinéa 1er
Art. 13, paragraphe 8	Art. 36
Art. 14	
Art. 14	Art. 37 et 38
Art. 15	
Art. 15, paragraphe 1er	Art. 28
Art. 15, paragraphe 2	
Art. 15, paragraphe 3	
Art. 15, paragraphe 4	
Art. 16	
Art. 16, paragraphe 1er	Art. 7
Art. 16, paragraphe 2	
Art. 16, paragraphe 3	
Art. 16, paragraphe 4r	
Art. 16, paragraphe 5	

Directive (UE) 2016/681	*Projet de loi*
Art. 17	
Art. 17	//
Art. 18	
Art. 18	//
Art. 19	
Art. 19	//
Art. 20	
Art. 20	//
Art. 21	
Art. 21	//
Art. 22	
Art. 22	//
Annexe I	Annexe I
Annexe II	Annexe II

*

FICHE FINANCIERE

Conformément à l'article 79 de la loi modifiée du 8 juin 1999 portant sur le budget, la comptabilité et la trésorerie de l'Etat, le Ministre de la Sécurité Intérieure déclare que le présent projet de loi aura un impact sur le budget de l'Etat.

Remarque préliminaire

Par la transposition de la directive (UE) 2016/681 un nouveau système devra être crée de toutes pièces avec une unité spécifique. Les besoins exprimés ci-dessous reflètent l'état de connaissance des évaluations à l'heure actuelle et sont susceptibles d'être revues au fil du temps.

Le Luxembourg peut bénéficier du cofinancement communautaire par le Fonds pour la Sécurité intérieure 2016-2020 pour la mise en place du PNR, qui s'élève à 292.217 euros.

1. La mise en place d'une Unité d'information passagers (UIP)

a) Infrastructure: Des aménagements dans les immeubles seront nécessaires ainsi que l'équipement des locaux: Investissement: 60.000,00 € au titre de l'article 06.1.12.270 „entretien, exploitation et location d'immeubles, dépenses diverses".

b) Personnel: L'UIP devra être dotée du personnel nécessaire à la réalisation de ses missions. Ce besoin est évalué à 4 personnels de la Police grand-ducale (2 en 2017 et 2 en 2018) dans un premier temps et pour un fonctionnement en semaine sur un horaire en journée. Si une entrée en opération 24/24 heures devait s'avérer nécessaire, un triplement des personnels serait nécessaire.

2. La collecte des données

Pour la collecte des données passagers auprès des transporteurs aériens opérant à l'aéroport de Luxembourg un dispositif technique doit être mis en place et entretenu. Un raccordement avec le système informatique de la quarantaine de transporteurs aériens afin de recueillir la vingtaine de champs d'informations par passagers doit être établi.

- Investissement: 540.000,00 € au titre de l'article 06.1.74.051 „Coopération policière européenne: développement de nouveaux systèmes d'information"
- Maintenance: 215.000,00 € /an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

- Frais d'exploitation: 503.000,00 € /an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

Des synergies européennes pourraient permettre de réduire le coût net par transaction par des économies d'échelle.

3. Le traitement des données

Un logiciel pour l'analyse et l'exploitation des données passagers recueillies doit être installé. Pour l'heure le Luxembourg a repris à titre gratuit le système d'un partenaire européen. Si un développement propre devait s'avérer comme indispensable au cours des premières années d'opération les coûts suivants seraient à prévoir:

- Investissement: 500.000,00 € au titre de l'article 06.1.74. 051 „Coopération policière européenne: développement de nouveaux systèmes d'information"
- Maintenance: 100.000,00 €/an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

4. Le système de gestion des échanges entre les Etats membres de l'Union Européenne

Un projet européen devrait voir le jour pour gérer les échanges entre les Unités Informations Passagers des 28 Etats membres. Sur besoin un développement propre serait nécessaire.

- Investissement: 150.000,00 € au titre de l'article 06.1.74.051 „Coopération policière européenne: développement de nouveaux systèmes d'information"
- Maintenance: 30.000,00 €/an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

*

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet:	**Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave**
Ministère initiateur:	**Ministère de la Sécurité intérieure**
Auteur(s):	**Martine Schmit**
Tél:	**247-84687**
Courriel:	**martine.schmit@msi.etat.lu**
Objectif(s) du projet:	**transposition de la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s):	
Ministère d'Etat (Service de Renseignement de l'Etat) Ministère des Finances (Administration des Douanes et Accises) Ministère du Développement durable et des Infrastructures (Direction de l'Aviation civile) Ministère de la Justice/autorités judiciaires	
Date:	**1.6.2016**

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s): Oui ☒ Non ☐

   Si oui, laquelle/lesquelles:
   Ministère d'Etat (Service de renseignement)
   Ministère des Finances (Administration des Douanes et accises)
   Ministère du Développement durable et des Infrastructures (Direction de l'aviation civile)
   Ministère de la Justice / autorités judiciaires
   Commissaire du gouvernement à la protection des banques de données

   Remarques/Observations:

2. Destinataires du projet:
   - Entreprises/Professions libérales: Oui ☒ Non ☐
   - Citoyens: Oui ☒ Non ☐
   - Administrations: Oui ☒ Non ☐

3. Le principe „Think small first" est-il respecté? Oui ☐ Non ☐ N.a.[1] ☒

   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité?)

   Remarques/Observations:

4. Le projet est-il lisible et compréhensible pour le destinataire? Oui ☒ Non ☐

   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière? Oui ☐ Non ☒

   Remarques/Observations:

1 N.a.: non applicable.

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures? Oui ☐ Non ☒
   Remarques/Observations:

6. Le projet contient-il une charge administrative[2] pour le(s) destinataire(s)? (un coût imposé pour satisfaire à une obligation d'information émanant du projet?) Oui ☒ Non ☐
   Si oui, quel est le coût administratif[3] approximatif total? (nombre de destinataires x coût administratif par destinataire)
   Le coût des transferts des données PNR (0,04 € par „push" par passager)

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire? Oui ☐ Non ☒ N.a. ☐
   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il?
   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4]? Oui ☒ Non ☐ N.a. ☐
   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il?
   Des données à caractère personnel contenues au niveau des dossiers passagers

8. Le projet prévoit-il:
   – une autorisation tacite en cas de non-réponse de l'administration? Oui ☐ Non ☐ N.a. ☒
   – des délais de réponse à respecter par l'administration? Oui ☐ Non ☐ N.a. ☒
   – le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois? Oui ☐ Non ☒ N.a. ☐

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p. ex. prévues le cas échéant par un autre texte)? Oui ☐ Non ☐ N.a. ☒
   Si oui, laquelle:

10. En cas de transposition de directives communautaires, le principe „la directive, rien que la directive" est-il respecté? Oui☒ Non ☐ N.a. ☐
    Si non, pourquoi?

11. Le projet contribue-t-il en général à une:
    a) simplification administrative, et/ou à une Oui ☐ Non ☒
    b) amélioration de la qualité réglementaire? Oui ☐ Non ☒
    Remarques/Observations:

---

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

3 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites? Oui ☐ Non ☐ N.a. ☒

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office)? Oui ☒ Non ☐
Si oui, quel est le délai pour disposer du nouveau système?
25 mai 2018 (= délai de transposition)

14. Y a-t-il un besoin en formation du personnel de l'administration concernée? Oui ☒ Non ☐ N.a. ☐
Si oui, lequel? formation des agents de l'unité d'information passagers
Remarques/Observations:

Egalité des chances

15. Le projet est-il:
- principalement centré sur l'égalité des femmes et des hommes? Oui ☐ Non ☒
- positif en matière d'égalité des femmes et des hommes? Oui ☐ Non ☒
  Si oui, expliquez de quelle manière:
- neutre en matière d'égalité des femmes et des hommes? Oui ☒ Non ☐
  Si oui, expliquez pourquoi:
- négatif en matière d'égalité des femmes et des hommes? Oui ☐ Non ☒
  Si oui, expliquez de quelle manière:

16. Y a-t-il un impact financier différent sur les femmes et les hommes? Oui ☐ Non ☒ N.a. ☐
Si oui, expliquez de quelle manière:

Directive „services"

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5]? Oui ☐ Non ☐ N.a. ☒
Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur:
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6]? Oui ☐ Non ☐ N.a. ☒
Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur:
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

5 Article 15, paragraphe 2 de la directive „services" (cf. Note explicative, p. 10-11)

6 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive „services" (cf. Note explicative, p. 10-11)

DIRECTIVE (UE) 2016/681 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1, point d), et son article 87, paragraphe 2, point a),

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen ([1]),

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) Le 6 novembre 2007, la Commission a adopté une proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives. Cependant, n'ayant pas encore été adoptée par le Conseil lors de l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009, la proposition de la Commission est devenue obsolète.

(2) «Le programme de Stockholm — Une Europe ouverte et sûre qui sert et protège les citoyens» ([3]) invite la Commission à présenter une proposition concernant l'utilisation des données PNR 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.

(3) Dans sa communication du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, la Commission a décrit un certain nombre d'éléments essentiels d'une politique de l'Union dans ce domaine.

(4) La directive 2004/82/CE du Conseil ([4]) régit la transmission aux autorités nationales compétentes, par les transporteurs aériens, d'informations préalables relatives aux passagers (ci-après dénommées «données API»), en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration illégale.

(5) Les objectifs de la présente directive sont, 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.

(6) L'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire 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, et donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels.

(7) L'évaluation des données PNR permet d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité avant cette évaluation et qui devraient être

([1]) JO C 218 du 23.7.2011, p. 107.
([2]) Position du Parlement européen du 14 avril 2016 (non encore parue au Journal officiel) et décision du Conseil du 21 avril 2016.
([3]) JO C 115 du 4.5.2010, p. 1.
([4]) Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO L 261 du 6.8.2004, p. 24).

soumises à un examen plus approfondi par les autorités compétentes. L'utilisation des données PNR permet de contrer la menace que représentent les infractions terroristes et les formes graves de criminalité sous un angle autre que par le traitement d'autres catégories de données à caractère personnel. Cependant, pour veiller à ce que le traitement de données PNR reste limité à ce qui est nécessaire, la création et l'application de critères d'évaluation devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente. Par ailleurs, les critères d'évaluation devraient être définis d'une manière qui réduise au minimum le nombre d'identifications erronées de personnes innocentes par le système.

(8) Les transporteurs aériens recueillent et traitent déjà des données PNR de leurs passagers pour leur propre usage commercial. La présente directive ne devrait pas leur imposer l'obligation de recueillir ou de conserver des données supplémentaires des passagers et ne devrait pas non plus contraindre les passagers à communiquer des données en sus de celles qui sont déjà transmises aux transporteurs aériens.

(9) Certains transporteurs aériens conservent les données API qu'ils recueillent en les regroupant avec les données PNR, alors que d'autres ne le font pas. L'utilisation combinée des données PNR et des données API présente une valeur ajoutée en ce qu'elle aide les États membres à vérifier l'identité d'une personne, renforçant ainsi la valeur du résultat en termes de prévention, de détection et de répression des infractions et réduisant au minimum le risque de soumettre des personnes innocentes à des vérifications et à des enquêtes. C'est pourquoi il est important de veiller à ce que, lorsque les transporteurs aériens recueillent des données API, ils les transfèrent, que les données API soient conservées ou non par des moyens techniques différents de ceux utilisés pour d'autres données PNR.

(10) 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, il est essentiel que tous les États membres adoptent des dispositions obligeant les transporteurs aériens qui assurent des vols extra-UE à transférer les données PNR qu'ils recueillent, y compris les données API. Les États membres devraient également avoir la possibilité d'étendre cette obligation aux transporteurs aériens qui assurent des vols intra-UE. Ces dispositions devraient s'entendre sans préjudice de la directive 2004/82/CE.

(11) Le traitement des données à caractère personnel devrait être proportionné aux objectifs de sécurité spécifiques poursuivis par la présente directive.

(12) La définition des infractions terroristes appliquée dans le cadre de la présente directive devrait être la même que celle figurant dans la décision-cadre 2002/475/JAI du Conseil ([1]). La définition des formes graves de criminalité devrait englober les catégories d'infractions énumérées à l'annexe II de la présente directive.

(13) Il convient que les données PNR soient transmises à une seule unité d'information passagers désignée (UIP) dans l'État membre concerné, de manière à garantir la clarté et à réduire les coûts supportés par les transporteurs aériens. L'UIP peut avoir plusieurs antennes dans un même État membre et les États membres peuvent également mettre en place conjointement une seule UIP. Les États membres devraient échanger leurs informations par l'intermédiaire de réseaux d'échange d'informations appropriés afin de faciliter le partage des informations et de garantir l'interopérabilité.

(14) Les États membres devraient assumer les coûts liés à l'utilisation, à la conservation et à l'échange de données PNR.

(15) Une liste des données PNR à transmettre à une UIP devrait être établie dans le but de refléter les exigences légitimes des pouvoirs publics en matière de prévention et de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, renforçant par là la sécurité intérieure de l'Union et la protection des droits fondamentaux, notamment le respect de la vie privée et la protection des données à caractère personnel. À cette fin, il convient d'appliquer des normes élevées conformément à la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après dénommée «convention nº 108») et la convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). Une telle liste ne devrait pas être fondée sur l'origine raciale ou ethnique, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne. Les données PNR ne devraient comporter que des informations relatives aux réservations et aux itinéraires de voyage des passagers qui permettent aux autorités compétentes d'identifier les passagers aériens représentant une menace pour la sécurité intérieure.

(16) Actuellement, deux méthodes de transfert des données sont possibles: la méthode «pull», par laquelle les autorités compétentes de l'État membre qui requièrent les données PNR peuvent accéder au système de réservation du transporteur aérien et en extraire («pull») une copie des données PNR requises, et la méthode «push», par laquelle les transporteurs aériens transmettent («push») les données PNR requises à l'autorité requérante, ce qui permet aux transporteurs aériens de garder le contrôle sur les données transmises. La méthode «push» est réputée offrir un niveau plus élevé de protection des données et devrait être obligatoire pour tous les transporteurs aériens.

([1]) Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

(17) La Commission soutient les lignes directrices de l'organisation de l'aviation civile internationale (OACI) relatives aux données PNR. Ces lignes directrices devraient, par conséquent, servir de base pour l'adoption des formats de données reconnus pour les transferts des données PNR par les transporteurs aériens aux États membres. Afin d'assurer des conditions uniformes d'exécution des formats de données reconnus et des protocoles correspondants applicables au transfert des données provenant des transporteurs aériens, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil ([1]).

(18) Les États membres devraient prendre toutes les mesures nécessaires pour permettre aux transporteurs aériens de remplir leurs obligations au titre de la présente directive. Il y a lieu que les États membres prévoient des sanctions effectives, proportionnées et dissuasives, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne respectent pas leurs obligations en matière de transfert de données PNR.

(19) Chaque État membre devrait être responsable de l'évaluation des menaces potentielles liées aux infractions terroristes et aux formes graves de criminalité.

(20) En tenant pleinement compte du droit à la protection des données à caractère personnel et du droit à la non-discrimination, aucune décision qui produit des effets juridiques préjudiciables à une personne ou l'affecte de manière significative ne devrait être prise sur la seule base du traitement automatisé des données PNR. Par ailleurs, conformément aux articles 8 et 21 de la Charte, aucune décision de cette nature ne devrait introduire de discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. La Commission devrait également prendre en compte ces principes lors du réexamen de l'application de la présente directive.

(21) Le résultat du traitement des données PNR ne devrait en aucun cas être utilisé par les États membres comme motif pour se soustraire à leurs obligations internationales au titre de la convention du 28 juillet 1951 relative au statut des réfugiés, telle qu'amendée par le protocole du 31 janvier 1967, ni être invoqué pour refuser aux demandeurs d'asile des voies sûres et effectives d'entrée légales sur le territoire de l'Union afin d'y exercer leur droit à la protection internationale.

(22) En tenant pleinement compte des principes mis en évidence par la récente jurisprudence pertinente de la Cour de justice de l'Union européenne, l'application de la présente directive devrait garantir le plein respect des droits fondamentaux et du droit au respect de la vie privée ainsi que du principe de proportionnalité. Elle devrait aussi véritablement remplir les objectifs de nécessité et de proportionnalité afin de répondre aux intérêts généraux reconnus par l'Union et à la nécessité de protéger les droits et libertés d'autrui dans la lutte contre les infractions terroristes et les formes graves de criminalité. L'application de la présente 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 ou de toute utilisation des données PNR.

(23) Les États membres devraient échanger entre eux et avec Europol les données PNR qu'ils reçoivent, lorsque cela est jugé nécessaire 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. Les UIP devraient, le cas échéant, transmettre sans tarder le résultat du traitement des données PNR aux UIP des autres États membres en vue d'un complément d'enquête. Les dispositions de la présente directive devraient s'entendre sans préjudice d'autres instruments de l'Union relatifs à l'échange d'informations entre les services de police et d'autres services répressifs et les autorités judiciaires, y compris la décision 2009/371/JAI du Conseil ([2]) et la décision-cadre 2006/960/JAI du Conseil ([3]). Il convient que les échanges de données PNR soient régis par les règles relatives à la coopération policière et judiciaire et ne portent pas atteinte au niveau élevé de protection de la vie privée et des données à caractère personnel exigé par la Charte, la convention nº 108 et la CEDH.

(24) L'échange sécurisé d'informations relatives aux données PNR entre les États membres devrait être assuré par l'intermédiaire de tout canal de coopération existant entre les autorités compétentes des États membres, et en particulier avec Europol, par l'intermédiaire de son application de réseau d'échange sécurisé d'informations (SIENA).

([1]) Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

([2]) Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) (JO L 121 du 15.5.2009, p. 37).

([3]) Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne (JO L 386 du 29.12.2006, p. 89).

(25) Les données PNR ne devraient être conservées que pour la durée nécessaire et proportionnée aux objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière. En raison de leur nature et de leurs utilisations, il est indispensable que les données PNR soient conservées pendant une période suffisamment longue pour permettre leur analyse et leur utilisation dans le cadre d'enquêtes. Pour éviter toute utilisation disproportionnée, il convient que, après le délai initial de conservation, les données PNR soient dépersonnalisées par le masquage d'éléments des données. Afin de garantir le niveau le plus élevé de protection de données, l'accès à l'intégralité des données PNR, qui permettent l'identification directe de la personne concernée, ne devrait être accordé que dans des conditions très strictes et limitées après ce délai initial.

(26) Lorsque des données PNR spécifiques ont été transmises à une autorité compétente et servent dans le cadre d'enquêtes ou de poursuites pénales spécifiques, leur durée de conservation par cette autorité devrait être fixée par le droit national, indépendamment des périodes de conservation de données prévues par la présente directive.

(27) Dans chaque État membre, le traitement de données PNR effectué par l'UIP et par les autorités compétentes devrait être soumis à une norme de protection des données à caractère personnel du droit national conforme à la décision-cadre 2008/977/JAI du Conseil ([1]) et aux exigences spécifiques de protection des données énoncées dans la présente directive. Les références à la décision-cadre 2008/977/JAI devraient s'entendre comme des références faites à la législation actuellement en vigueur ainsi qu'à la législation qui la remplacera.

(28) Compte tenu du droit à la protection des données à caractère personnel, il convient que les droits des personnes concernées en ce qui concerne le traitement de leurs données PNR, tels que les droits d'accès, de rectification, d'effacement et de limitation, ainsi que le droit à réparation et le droit à un recours juridictionnel, soient conformes à la décision-cadre 2008/977/JAI et au niveau de protection élevé conféré par la Charte et la CEDH.

(29) Eu égard au droit des passagers d'être informés du traitement des données à caractère personnel les concernant, les États membres devraient veiller à ce que les passagers reçoivent des informations précises, aisément accessibles et facilement compréhensibles, sur la collecte des données PNR, le transfert de celles-ci à l'UIP et leurs droits en tant que personnes concernées.

(30) La présente directive s'applique sans préjudice du droit de l'Union et du droit national concernant le principe de l'accès du public aux documents officiels.

(31) Les États membres ne devraient être autorisés à transférer des données PNR vers des pays tiers qu'au cas par cas et dans le plein respect des dispositions adoptées par les États membres en vertu de la décision-cadre 2008/977/JAI. Pour assurer la protection des données à caractère personnel, ces transferts devraient être soumis à des exigences supplémentaires relatives à leur finalité. Ils devraient également être soumis aux principes de nécessité et de proportionnalité et au niveau de protection élevé conféré par la Charte et la CEDH.

(32) Les autorités de contrôle nationales mises en place en application de la décision-cadre 2008/977/JAI devraient également être chargées de fournir des conseils sur l'application des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci.

(33) La présente directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne, sous réserve que ce droit national respecte le droit de l'Union.

(34) La présente directive est sans préjudice des règles actuelles de l'Union sur les modalités des contrôles aux frontières ou des règles de l'Union régissant l'entrée sur le territoire de l'Union et la sortie de celui-ci.

(35) Comme les dispositions nationales relatives au traitement des données à caractère personnel, y compris des données PNR, divergent sur le plan juridique et technique, les transporteurs aériens doivent et devront faire face à des exigences différentes en ce qui concerne le type d'informations à transmettre et les conditions dans lesquelles

([1]) Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350 du 30.12.2008, p. 60).

ces informations doivent être communiquées aux autorités nationales compétentes. Ces divergences peuvent nuire à une coopération efficace entre ces autorités aux fins de la prévention et de la détection des infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. Il est dès lors nécessaire d'établir, au niveau de l'Union, un cadre juridique commun pour le transfert et le traitement des données PNR.

(36) La présente directive respecte les droits fondamentaux et les principes énoncés dans la Charte, en particulier le droit à la protection des données à caractère personnel, le droit au respect de la vie privée et le droit à la non-discrimination consacrés par ses articles 8, 7 et 21; elle devrait dès lors être mise en œuvre en conséquence. La présente directive est compatible avec les principes de la protection des données et ses dispositions sont conformes à la décision-cadre 2008/977/JAI. En outre, afin de respecter le principe de proportionnalité, la présente directive prévoit, pour des points spécifiques, des règles de protection des données plus strictes que celles prévues dans la décision-cadre 2008/977/JAI.

(37) Le champ d'application de la présente directive est aussi limité que possible dès lors que: il 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 devraient être effacées; il prévoit que les données sont dépersonnalisées par le masquage d'éléments des données après une période initiale de six mois; et il interdit la collecte et l'utilisation des données sensibles. Pour garantir l'efficacité et un niveau élevé de protection des données, les États membres sont 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. Tout traitement de données PNR devrait 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. Les États membres devraient également veiller à ce que les passagers reçoivent des informations claires et précises sur la collecte des données PNR et sur leurs droits.

(38) Étant donné que les objectifs de la présente directive — à savoir le transfert de 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 — ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(39) Conformément à l'article 3 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, ces États membres ont notifié leur souhait de participer à l'adoption et à l'application de la présente directive.

(40) Conformément aux articles 1er et 2 du protocole n° 22 sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

(41) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 du Parlement européen et du Conseil [1] et a rendu son avis le 25 mars 2011,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

Dispositions générales

Article premier

Objet et champ d'application

1. La présente directive prévoit:

a) le transfert, par les transporteurs aériens, de données des dossiers des passagers (PNR) de vols extra-UE;

b) le traitement des données visées au point a), notamment leur collecte, leur utilisation et leur conservation par les États membres et leur échange entre les États membres.

[1] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

2. Les données PNR recueillies conformément à la présente directive ne peuvent 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, comme prévu à l'article 6, paragraphe 2, points a), b) et c).

Article 2

Application de la présente directive aux vols intra-UE

1. Si un État membre décide d'appliquer la présente directive aux vols intra-UE, il le notifie à la Commission par écrit. Un État membre peut adresser ou révoquer une telle notification à tout moment. La Commission publie cette notification et la révocation éventuelle de celle-ci au *Journal officiel de l'Union européenne*.

2. Lorsqu'une notification visée au paragraphe 1 est adressée, toutes les dispositions de la présente directive s'appliquent aux vols intra-UE comme s'il s'agissait de vols extra-UE et aux données PNR des vols intra-UE comme s'il s'agissait de données PNR de vols extra-UE.

3. Un État membre peut décider d'appliquer la présente directive uniquement à certains vols intra-UE. Lorsqu'il prend une telle décision, l'État membre sélectionne les vols qu'il juge nécessaires afin de poursuivre les objectifs de la présente directive. L'État membre peut décider à tout moment de modifier la sélection des vols intra-UE.

Article 3

Définitions

Aux fins de la présente directive, on entend par:

1) «transporteur aérien», une entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de passagers;

2) «vol extra-UE», tout vol, régulier ou non, effectué par un transporteur aérien en provenance d'un pays tiers et devant atterrir sur le territoire d'un État membre ou en provenance du territoire d'un État membre et devant atterrir dans un pays tiers, y compris, dans les deux cas, les vols comportant d'éventuelles escales sur le territoire d'États membres ou de pays tiers;

3) «vol intra-UE», tout vol, régulier ou non, effectué par un transporteur aérien en provenance du territoire d'un État membre et devant atterrir sur le territoire d'un ou de plusieurs États membres, sans escale sur le territoire d'un pays tiers;

4) «passager», toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers;

5) «dossier(s) passager(s)» ou «PNR», un dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs (utilisés pour contrôler les passagers lors de l'embarquement) ou des systèmes équivalents offrant les mêmes fonctionnalités;

6) «système de réservation», le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations;

7) «méthode push», la méthode par laquelle les transporteurs aériens transfèrent les données PNR énumérées à l'annexe I vers la base de données de l'autorité requérante;

8) «infractions terroristes», les infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI;

9) «formes graves de criminalité», les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre;

10) «dépersonnaliser par le masquage d'éléments des données», rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée.

CHAPITRE II

Responsabilités des états membres

Article 4

Unité d'informations passagers

1. Chaque État membre met en place ou désigne une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, ou crée ou désigne une antenne d'une telle autorité, en tant que son UIP.

2. L'UIP est chargée:

a) 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 aux autorités compétentes visées à l'article 7;

b) 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, conformément aux articles 9 et 10.

3. Les membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes. Les États membres dotent les UIP des ressources adéquates pour l'accomplissement de leurs missions.

4. Deux États membres ou plus (ci-après dénommés «États membres participants») peuvent mettre en place ou désigner une autorité unique en tant qu'UIP. Cette UIP est établie dans l'un des États membres participants et est considérée comme l'UIP nationale de tous les États membres participants. Ces derniers conviennent conjointement des modalités de fonctionnement de l'UIP et respectent les exigences prévues dans la présente directive.

5. Chaque État membre notifie à la Commission la mise en place de son UIP dans un délai d'un mois à compter de cette mise en place et peut, à tout moment, modifier sa notification. La Commission publie cette notification et toute modification y afférente au *Journal officiel de l'Union européenne*.

Article 5

Délégué à la protection des données au sein de l'UIP

1. L'UIP nomme un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes.

2. Les États membres dotent les délégués à la protection des données des moyens pour accomplir leurs missions et obligations, conformément au présent article, de manière effective et en toute indépendance.

3. Les États membres veillent à ce que la personne concernée ait 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.

Article 6

Traitement des données PNR

1. Les données PNR transférées par les transporteurs aériens sont recueillies par l'UIP de l'État membre concerné comme prévu à l'article 8. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données immédiatement et de façon définitive dès leur réception.

2. L'UIP ne traite les données PNR qu'aux fins suivantes:

a) réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes visées à l'article 7 et, le cas échéant, par Europol conformément à l'article 10, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité;

b) répondre, au cas par cas, aux demandes dûment motivées fondées sur des motifs suffisants des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière, et visant à communiquer aux autorités compétentes ou, le cas échéant, à Europol le résultat de ce traitement; et

c) analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées au titre du paragraphe 3, point b), en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité.

3. Lorsqu'elle réalise l'évaluation visée au paragraphe 2, point a), l'UIP peut:

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, y compris les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données; ou

b) traiter les données PNR au regard de critères préétablis.

4. L'évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci effectuée au titre du paragraphe 3, point b), au regard de critères préétablis est réalisée de façon non discriminatoire. Ces critères préétablis doivent être ciblés, proportionnés et spécifiques. Les États membres veillent à ce que ces critères soient fixés et réexaminés à intervalles réguliers par les UIP en coopération avec les autorités compétentes visées à l'article 7. Lesdits critères ne sont en aucun cas fondés sur 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.

5. Les États membres s'assurent que toute concordance positive obtenue à la suite du traitement automatisé des données PNR effectué au titre du paragraphe 2, point a), est réexaminée individuellement par des moyens non automatisés, afin de vérifier si l'autorité compétente visée à l'article 7 doit prendre des mesures en vertu du droit national.

6. L'UIP d'un État membre transmet, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au paragraphe 2, point a), ou le résultat du traitement de ces données aux autorités compétentes visées à l'article 7 de ce même État membre. Ces transferts ne sont effectués qu'au cas par cas et, en cas de traitement automatisé des données PNR, après un réexamen individuel par des moyens non automatisés.

7. Les États membres veillent à ce que le délégué à la protection des données ait accès à toutes les données traitées par l'UIP. Si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, le délégué à la protection des données peut renvoyer l'affaire à l'autorité de contrôle nationale.

8. Le stockage, le traitement et l'analyse des données PNR par les UIP sont effectués exclusivement dans un ou des endroits sécurisés situés sur le territoire des États membres.

9. Les conséquences des évaluations des passagers visées au paragraphe 2, point a), du présent article ne compromettent pas 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 ([1]). En outre, lorsque des évaluations sont réalisées pour des vols intra-UE entre des États membres auxquels s'applique le règlement (CE) nº 562/2006 du Parlement européen et du Conseil ([2]), les conséquences de ces évaluations doivent respecter ledit règlement.

Article 7

Autorités compétentes

1. Chaque État membre arrête une liste des autorités compétentes habilitées à demander aux UIP ou à recevoir de celles-ci des données PNR ou le résultat du traitement de telles données en vue de procéder à un examen plus approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière.

2. Les autorités visées au paragraphe 1 sont des autorités compétentes en matière de prévention ou de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes ou de poursuites en la matière.

3. Aux fins de l'article 9, paragraphe 3, chaque État membre notifie à la Commission la liste de ses autorités compétentes au plus tard 25 mai 2017 et peut modifier sa notification à tout moment. La Commission publie cette notification et toute modification y afférente au *Journal officiel de l'Union européenne*.

4. Les données PNR et le résultat du traitement de ces données reçus par l'UIP ne peuvent faire l'objet d'un traitement ultérieur par les autorités compétentes des États membres qu'aux seules fins spécifiques de la prévention ou de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes ou des poursuites en la matière.

5. Le paragraphe 4 s'applique sans préjudice des compétences des autorités répressives ou judiciaires nationales, lorsque d'autres infractions, ou des indices d'autres infractions, sont détectés dans le cadre d'actions répressives menées à la suite de ce traitement.

6. Les autorités compétentes ne peuvent prendre aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR. Ces décisions ne peuvent pas être fondées sur 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.

Article 8

Obligations imposées aux transporteurs aériens concernant les transferts de données

1. Les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent, par la «méthode push», les données PNR énumérées à l'annexe I, pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités, vers la base de données de l'UIP de l'État membre sur le territoire duquel le vol atterrira ou du territoire duquel il décollera. Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR de tous les passagers du vol incombe au transporteur aérien qui assure le vol. Lorsqu'un vol extra-UE comporte une ou plusieurs escales dans des aéroports des États membres, les transporteurs aériens transfèrent les données PNR de tous les passagers aux UIP de tous les États membres concernés. Il en est de même lorsqu'un vol intra-UE comporte une ou plusieurs escales dans les aéroports de différents États membres, mais uniquement en ce qui concerne les États membres qui recueillent les données PNR des vols intra-UE.

([1]) Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) nº 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO L 158 du 30.4.2004, p. 77).

([2]) Règlement (CE) nº 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO L 105 du 13.4.2006, p. 1).

2. Dans l'hypothèse où les transporteurs aériens ont recueilli des informations préalables sur les passagers (ci-après dénommées «données API») énumérées à l'annexe I, point 18, mais ne les conservent pas par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent également ces données, par la «méthode push», à l'UIP des États membres visés au paragraphe 1. Dans le cas d'un tel transfert, toutes les dispositions de la présente directive s'appliquent à ces données API.

3. Les transporteurs aériens transfèrent les données PNR par voie électronique au moyen de protocoles communs et de formats de données reconnus à adopter en conformité avec la procédure d'examen visée à l'article 17, paragraphe 2, ou, en cas de défaillance technique, par tout autre moyen approprié garantissant un niveau de sécurité des données approprié:

a) 24 à 48 heures avant l'heure de départ programmée du vol; et

b) 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 qu'ils ne peuvent plus embarquer ou débarquer.

4. Les États membres autorisent les transporteurs aériens à limiter le transfert visé au paragraphe 3, point b), aux mises à jour des transferts visés au point a) dudit paragraphe.

5. Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, les transporteurs aériens transfèrent, au cas par cas, des données PNR à d'autres moments que ceux mentionnés au paragraphe 3, à la demande d'une UIP conformément au droit national.

Article 9

Échange d'informations entre États membres

1. Les États membres veillent à ce que, en ce qui concerne les personnes identifiées par une UIP conformément à l'article 6, paragraphe 2, toutes les données PNR pertinentes et nécessaires ou le résultat du traitement de ces données soient transmis par ladite UIP aux UIP correspondantes des autres États membres. Les UIP des États membres destinataires transmettent les informations reçues à leurs autorités compétentes, conformément à l'article 6, paragraphe 6.

2. L'UIP d'un État membre a le droit de demander, si nécessaire, à l'UIP de tout autre État membre de lui communiquer des données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par le masquage d'éléments des données au titre de l'article 12, paragraphe 2, ainsi que, si nécessaire, le résultat de tout traitement de ces données, si celui-ci a déjà été réalisé en vertu de l'article 6, paragraphe 2, point a). Cette demande est dûment motivée. Elle peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière. Les UIP transmettent dès que possible les informations demandées. Si les données demandées ont été dépersonnalisées par le masquage d'éléments des données conformément à l'article 12, paragraphe 2, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que cela est nécessaire aux fins visées à l'article 6, paragraphe 2, point b), et uniquement si elle y est autorisée par une autorité visée à l'article 12, paragraphe 3, point b).

3. Les autorités compétentes d'un État membre ne peuvent demander directement à l'UIP d'un autre État membre de leur communiquer des données PNR qui sont conservées dans sa base de données que lorsque cela est nécessaire dans les cas d'urgence et dans les conditions fixées au paragraphe 2. Les demandes des autorités compétentes sont motivées. Une copie de la demande est toujours envoyée à l'UIP de l'État membre requérant. Dans tous les autres cas, les autorités compétentes canalisent leurs demandes par l'intermédiaire de l'UIP de leur propre État membre.

4. À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un État membre a le droit de demander à ce que l'UIP d'un autre État membre obtienne des données PNR conformément à l'article 8, paragraphe 5, et les communique à l'UIP requérante.

5. L'échange d'informations au titre du présent article peut avoir lieu par l'intermédiaire de n'importe quel canal de coopération existant entre les autorités compétentes des États membres. La langue utilisée pour la demande et l'échange

d'informations est celle applicable au canal utilisé. Lorsqu'ils procèdent aux notifications conformément à l'article 4, paragraphe 5, les États membres communiquent également à la Commission les coordonnées des points de contact auxquels les demandes peuvent être adressées en cas d'urgence. La Commission communique lesdites coordonnées aux États membres.

Article 10

Conditions d'accès aux données PNR par Europol

1. Europol est habilité à demander aux UIP des États membres des données PNR ou le résultat du traitement de ces données dans les limites de ses compétences et pour l'accomplissement de ses missions.

2. Europol peut présenter, au cas par cas, à l'UIP de tout État membre par l'intermédiaire de l'unité nationale Europol, une demande électronique dûment motivée de transmission de données PNR spécifiques ou du résultat du traitement de ces données. Europol peut présenter cette demande lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des États membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes en la matière, dans la mesure où ladite infraction ou ladite forme de criminalité relève de la compétence d'Europol en vertu de la décision 2009/371/JAI. Cette demande énonce les motifs raisonnables sur lesquels se fonde Europol pour estimer que la transmission des données PNR ou du résultat du traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée, ou à des enquêtes en la matière.

3. Europol informe le délégué à la protection des données nommé conformément à l'article 28 de la décision 2009/371/JAI de chaque échange d'informations au titre du présent article.

4. Les échanges d'information au titre du présent article ont lieu par l'intermédiaire de SIENA et conformément à la décision 2009/371/JAI. La langue utilisée pour la demande et l'échange d'informations est celle applicable à SIENA.

Article 11

Transfert de données vers des pays tiers

1. Un État membre peut transférer à un pays tiers des données PNR et le résultat du traitement de ces données, qui sont conservés par l'UIP conformément à l'article 12, uniquement au cas par cas et si:

a) les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI sont remplies;

b) le transfert est nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2;

c) le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2, et uniquement avec l'accord exprès dudit État membre; et

d) les mêmes conditions que celles prévues à l'article 9, paragraphe 2, sont remplies.

2. Nonobstant l'article 13, paragraphe 2, de la décision-cadre 2008/977/JAI, les transferts de données PNR sans l'accord préalable de l'État membre dont les données ont été obtenues, ne sont autorisés que dans des circonstances exceptionnelles et uniquement si:

a) 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) l'accord préalable ne peut pas être obtenu en temps utile.

L'autorité chargée de donner son accord est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

3. Les États membres ne transfèrent des données PNR aux autorités compétentes de pays tiers que dans des conditions compatibles avec la présente directive et après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte ces conditions et garanties.

4. Chaque fois qu'un État membre transfère des données PNR en vertu du présent article, le délégué à la protection des données de l'UIP de cet État membre en est informé.

Article 12

Période de conservation et dépersonnalisation des données

1. Les États membres veillent à ce que les données PNR fournies par les transporteurs aériens à l'UIP y soient 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.

2. À l'expiration d'une période de six mois suivant le transfert des données PNR visé au paragraphe 1, toutes les données PNR sont dépersonnalisées par le masquage des éléments des données suivants qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR:

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;

b) l'adresse et les coordonnées;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne;

d) les informations «grands voyageurs»;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte; et

f) toute donnée API qui a été recueillie.

3. À l'expiration de la période de six mois visée au paragraphe 2, la communication de l'intégralité des données PNR n'est autorisée que:

a) lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b); et

b) lorsqu'elle a été approuvée par:

   i) une autorité judiciaire; ou

   ii) une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post.

4. Les États membres veillent à ce que les données PNR soient effacées de manière définitive à l'issue de la période visée au paragraphe 1. Cette obligation s'applique sans préjudice des cas où des données PNR spécifiques ont été transférées à une autorité compétente et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière, auquel cas la conservation de ces données par l'autorité compétente est régie par le droit national.

5. Le résultat du traitement visé à l'article 6, paragraphe 2, point a), n'est conservé par l'UIP que le temps nécessaire pour informer les autorités compétentes et, conformément à l'article 9, paragraphe 1, pour informer les UIP des autres États membres de l'existence d'une concordance positive. Lorsque, à la suite du réexamen individuel par des moyens non automatisés visé à l'article 6, paragraphe 5, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées au titre du paragraphe 4 du présent article, de manière à éviter de futures «fausses» concordances positives.

Article 13

Protection des données à caractère personnel

1. Chaque État membre veille à ce que, pour tout traitement de données à caractère personnel effectué au titre de la présente directive, chaque passager dispose du même droit à la protection de ses données à caractère personnel, des mêmes droits d'accès, de rectification, d'effacement et de limitation, et droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union et le droit national et en application des articles 17, 18, 19 et 20 de la décision-cadre 2008/977/JAI. Lesdits articles sont par conséquent applicables.

2. Chaque État membre veille à ce que les dispositions adoptées en droit national en application des articles 21 et 22 de la décision-cadre 2008/977/JAI concernant la confidentialité du traitement et la sécurité des données s'appliquent également à tous les traitements de données à caractère personnel effectués en vertu de la présente directive.

3. La présente directive est sans préjudice de l'applicabilité de la directive 95/46/CE du Parlement européen et du Conseil ([1]) au traitement des données à caractère personnel par les transporteurs aériens, en particulier en ce qui concerne leurs obligations de prendre des mesures techniques et organisationnelles appropriées pour protéger la sécurité et la confidentialité des données à caractère personnel.

4. Les États membres interdisent le traitement des données PNR qui révèlent 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 reçoit des données PNR révélant de telles informations, elle les efface immédiatement.

5. Les États membres veillent à ce que l'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous leur responsabilité. Cette documentation comprend au minimum:

a) le nom et les coordonnées de l'organisation et du personnel chargés du traitement des données PNR au sein de l'UIP et les différents niveaux d'autorisation d'accès;

b) les demandes formulées par les autorités compétentes et les UIP d'autres États membres;

c) toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

6. Les États membres veillent à ce que l'UIP tienne 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 indiquent, 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. Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit. L'UIP met les registres à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

Ces registres sont conservés pendant cinq ans.

7. Les États membres veillent à ce que leur UIP mette en œuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et à la nature des données PNR.

8. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'entraîner un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, les États membres veillent à ce que l'UIP fasse part de cette atteinte à la personne concernée et à l'autorité de contrôle nationale sans retard injustifié.

Article 14

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions.

En particulier, les États membres déterminent le régime des sanctions, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne transmettent pas de données comme le prévoit l'article 8, ou ne les transmettent pas dans le format requis.

Les sanctions prévues doivent être effectives, proportionnées et dissuasives.

([1]) Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

Article 15

Autorité de contrôle nationale

1. Chaque État membre prévoit que l'autorité de contrôle nationale visée à l'article 25 de la décision-cadre 2008/977/JAI est chargée de fournir des conseils sur l'application, sur son territoire, des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci. L'article 25 de ladite décision-cadre s'applique.

2. Ces autorités de contrôle nationales exercent les activités au titre du paragraphe 1 en ayant en vue la protection des droits fondamentaux en matière de traitement des données à caractère personnel.

3. Chaque autorité de contrôle nationale:

a) traite les réclamations introduites par toute personne concernée, enquête sur l'affaire et informe la personne concernée de l'état d'avancement du dossier et de l'issue de la réclamation dans un délai raisonnable;

b) vérifie la licéité du traitement des données, effectue des enquêtes, des inspections et des audits conformément au droit national, de sa propre initiative ou en se fondant sur une réclamation visée au point a).

4. Chaque autorité de contrôle nationale conseille, sur demande, toute personne concernée quant à l'exercice des droits que lui confèrent les dispositions adoptées en vertu de la présente directive.

CHAPITRE III

Mesures d'exécution

Article 16

Protocoles communs et formats de données reconnus

1. Tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP aux fins de la présente directive sont effectués par des moyens électroniques qui offrent des garanties suffisantes en ce qui concerne les mesures de sécurité techniques et les mesures organisationnelles régissant le traitement à effectuer. En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union en matière de protection des données soit pleinement respecté.

2. 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 conformément au paragraphe 3, tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP aux fins de la présente directive se font par voie électronique à l'aide de méthodes sécurisées respectant ces protocoles communs. Ces protocoles sont identiques pour tous les transferts afin d'assurer la sécurité des données PNR pendant le transfert. Les données PNR sont transférées sous un format de données reconnu afin d'en assurer la lisibilité par toutes les parties concernées. Tous les transporteurs aériens sont tenus de choisir et de préciser à l'UIP le protocole commun et le format de données qu'ils ont l'intention d'utiliser pour leurs transferts.

3. La Commission dresse la liste des protocoles communs et des formats de données reconnus et, si nécessaire, l'adapte au moyen d'actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 17, paragraphe 2.

4. Tant que les protocoles communs et les formats de données reconnus visés aux paragraphes 2 et 3 ne sont pas disponibles, le paragraphe 1 s'applique.

5. Dans un délai d'un an à compter de la date d'adoption des protocoles communs et des formats de données reconnus visés au paragraphe 2, chaque État membre veille à ce que les mesures techniques nécessaires soient adoptées pour pouvoir utiliser ces protocoles communs et formats de données.

Article 17

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

Lorsque le comité n'émet aucun avis, la Commission n'adopte pas le projet d'acte d'exécution, et l'article 5, paragraphe 4, troisième alinéa, du règlement (UE) nº 182/2011 s'applique.

CHAPITRE IV

Dispositions finales

Article 18

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 25 mai 2018. Ils en informent immédiatement la Commission.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 19

Réexamen

1. Sur la base des informations communiquées par les États membres, y compris les informations statistiques visées à l'article 20, paragraphe 2, la Commission procède, au plus tard le 25 mai 2020, au réexamen de tous les éléments de la présente directive et communique et présente un rapport au Parlement européen et au Conseil.

2. Dans le cadre de son réexamen, la Commission accorde une attention particulière:

a) au respect des normes applicables de protection des données à caractère personnel;

b) à la nécessité et à la proportionnalité de la collecte et du traitement des données PNR au regard de chacune des finalités énoncées dans la présente directive;

c) à la durée de la période de conservation des données;

d) à l'efficacité de l'échange d'informations entre les États membres; et

e) à la qualité des évaluations, y compris en ce qui concerne les informations statistiques recueillies en vertu de l'article 20.

3. Le rapport visé au paragraphe 1 examine également s'il est nécessaire, proportionné et efficace d'inclure dans le champ d'application de la présente directive la collecte et le transfert des données PNR, à titre obligatoire, pour l'ensemble des vols intra-UE ou une sélection de ceux-ci. La Commission tient compte de l'expérience acquise par les États membres, en particulier ceux qui appliquent la présente directive aux vols intra-UE conformément à l'article 2. Le rapport examine également s'il est nécessaire d'inclure des opérateurs économiques autres que les transporteurs, tels que des agences et des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, dans le champ d'application de la présente directive.

4. Le cas échéant, au vu du réexamen effectué au titre du présent article, la Commission soumet une proposition législative au Parlement européen et au Conseil en vue de modifier la présente directive.

Article 20

Données statistiques

1. Les États membres fournissent chaque année à la Commission une série de statistiques sur les données PNR communiquées aux UIP. Ces statistiques ne contiennent pas de données à caractère personnel.

2. Les statistiques concernent au moins:

a) le nombre total de passagers dont les données PNR ont été recueillies et échangées;

b) le nombre de passagers identifiés en vue d'un examen plus approfondi.

Article 21

Rapports avec d'autres instruments

1. Les États membres peuvent continuer d'appliquer les accords ou arrangements bilatéraux ou multilatéraux en matière d'échange d'informations entre les autorités compétentes qu'ils ont conclus entre eux et qui sont en vigueur au 24 mai 2016, dans la mesure où ceux-ci sont compatibles avec la présente directive.

2. La présente directive s'applique sans préjudice de l'applicabilité de la directive 95/46/CE au traitement des données à caractère personnel par les transporteurs aériens.

3. La présente directive s'applique sans préjudice des obligations et engagements d'États membres ou de l'Union qui découlent d'accords bilatéraux ou multilatéraux avec des pays tiers.

Article 22

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Les États membres sont destinataires de la présente directive conformément aux traités.

Fait à Bruxelles, le 27 avril 2016.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

ANNEXE I

Données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens

1. Code repère du dossier passager
2. Date de réservation/d'émission du billet
3. Date(s) prévue(s) du voyage
4. Nom(s)
5. Adresse et coordonnées (numéro de téléphone, adresse électronique)
6. Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation
7. Itinéraire complet pour le PNR concerné
8. Informations «grands voyageurs»
9. Agence de voyages/agent de voyages
10. Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation
11. Indications concernant la scission/division du PNR
12. Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée)
13. Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix
14. Numéro du siège et autres informations concernant le siège
15. Informations sur le partage de code
16. Toutes les informations relatives aux bagages
17. Nombre et autres noms de voyageurs figurant dans le PNR
18. Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée)
19. Historique complet des modifications des données PNR énumérées aux points 1 à 18.

ANNEXE II

Liste des infractions visées à l'article 3, point 9)

1. Participation à une organisation criminelle
2. Traite des êtres humains
3. Exploitation sexuelle des enfants et pédopornographie
4. Trafic de stupéfiants et de substances psychotropes
5. Trafic d'armes, de munitions et d'explosifs
6. Corruption
7. Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union
8. Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro
9. Cybercriminalité
10. Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées
11. Aide à l'entrée et au séjour irréguliers
12. Meurtre, coups et blessures graves
13. Trafic d'organes et de tissus humains
14. Enlèvement, séquestration et prise d'otage
15. Vol organisé ou vol à main armée
16. Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art
17. Contrefaçon et piratage de produits
18. Falsification de documents administratifs et trafic de faux
19. Trafic de substances hormonales et d'autres facteurs de croissance
20. Trafic de matières nucléaires et radioactives
21. Viol
22. Infractions graves relevant de la Cour pénale internationale
23. Détournement d'avion/de navire
24. Sabotage
25. Trafic de véhicules volés
26. Espionnage industriel.

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/01

N° 7151[1]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

SOMMAIRE:

page

Avis des autorités judiciaires

1) Avis du Parquet général (24.8.2017) 1
2) Avis des Parquets de Luxembourg et de Diekirch (15.10.2017)..... 6
3) Avis du Tribunal d'arrondissement de et à Luxembourg (18.9.2017)..... 10

*

AVIS DU PARQUET GENERAL

(24.8.2017)

Par dépêche du 29 juin 2017, Monsieur le Ministre de la Justice a transmis la demande d'avis relatif au projet de loi sur le traitement des données passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave de Monsieur le Ministre de la Sécurité intérieure à l'attention des autorités judiciaires.

Le projet de loi sous avis a pour objet de transposer en droit national la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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.

Cette directive fait suite à la directive 2004/82/CE du Conseil du 29 avril 2004 imposant l'obligation aux transporteurs aériens de communiquer les données relatives aux passagers, directive transposée en droit luxembourgeois par la loi du 21 décembre 2006. Cette directive prévoyait entre autre l'obligation pour les transporteurs aériens de fournir préalablement, et ce avant la fin de l'enregistrement toutes les informations relatives à leurs passagers. La finalité en était d'améliorer les contrôles aux frontières et de lutter contre l'immigration illégale. La transmission de ces données dites API (*Advanced Passenger Information*) provient des informations issues dans le cadre du check-in respectivement de l'embarquement. Ces données permettent surtout l'identification des criminels signalés à l'aide des systèmes d'alerte (Interpol, SIS).

Les données PNR (*Passenger Name Record*) qui font l'objet de la directive 2016/681 sont issues des données fournies lors des réservations, contiennent donc davantage d'éléments et sont plus rapidement disponibles. Le traitement des données PNR poursuivra donc une finalité différente de celle pour laquelle ces données sont collectées par les transporteurs aériens.

Ces données se révèlent cependant essentielles pour les évaluations des risques présentés par certaines personnes et l'établissement des liens entre les personnes déjà connues et des personnes inconnues.

Les enquêtes relatives aux infractions de terrorisme et de criminalité grave montrent souvent des comportements de voyage spécifique et il donc été jugé essentiel de prévoir l'obligation notamment pour les transporteurs aériens de transmettre les données de passagers se déplaçant vers ou à partir d'un État membre, susceptibles de présenter potentiellement une menace pour la sécurité européenne et nationale.

La finalité du traitement des données des passagers s'inscrit dans le cadre de la prévention et de la recherche d'infractions terroristes, des formes graves de criminalité, des atteintes à l'ordre public dans le cadre de la radicalisation violente et des activités pouvant menacer les intérêts fondamentaux des États membres de l'Union européenne.

Les attaques terroristes récentes ensemble le phénomène du retour des *„foreign fighters"* font apparaître que la sécurité des citoyens est menacée plus que jamais et ce constat appelle une anticipation des risques entre autre par l'analyse des fichiers contenant les données de voyage.

En effet les activités terroristes tout comme la criminalité grave et organisée sont des phénomènes associés à de nombreux déplacements internationaux illimités tant à l'intérieur qu'à l'extérieur des frontières de l'Europe. En outre, la suppression des contrôles aux frontières intérieures sur la base de l'Accord de Schengen facilite davantage ces déplacements.

Ce phénomène appelle une approche commune au niveau européen afin de créer une interopérabilité maximale entre les Unités d'information des passagers des États membres lesquelles seront chargées de recueillir, de traiter et de gérer les données passagers.

Cependant les organisations terroristes et criminelles ne se limitent pas à l'utilisation du transport aérien pour organiser leurs activités. L'attentat terroriste qui a eu lieu sur la ligne Thalys Paris-Bruxelles-Amsterdam le 21 août 2015 montre clairement la nécessité d'étendre l'obligation de transmission de données de passagers à d'autres modes de transport.

La directive européenne PNR prévoit en premier lieu la collecte de données des passagers pour le trafic aérien, mais laisse explicitement (considérant 33) la possibilité aux États membres d'imposer cette obligation à d'autres opérateurs économiques autres que les transporteurs, tels que les agences ou les organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR.

Les États membres ont donc la faculté d'adopter une réglementation nationale visant d'autres modes de transport comme par exemple le transport ferroviaire ainsi que les opérateurs de transport.

Il résulte de l'exposé des motifs du présent projet de loi que dans le cadre d'une déclaration commune du 4 décembre 2015 les ministres JAI se sont engagés dans la mesure du possible, à élargir la collecte des données PNR auprès d'opérateurs économiques autres que les transporteurs. On peut déplorer que le gouvernement luxembourgeois ait choisi de limiter le champ d'application aux seuls transporteurs aériens qui ne sont que peu nombreux sur le territoire luxembourgeois et que pour des raisons pratiques liées à des systèmes de réservation informatiques différents notre pays s'engage à poursuivre ses réflexions qu'à l'issue d'une évaluation opérée par la Commission d'ici un délai de deux ans après le délai de transposition de la directive.

Les législateurs français et belges, ces 2 États ayant certes d'autres sensibilités que le Luxembourg au regard des graves attaques subies ces dernières années, ont choisi d'étendre la communication des données passagers aux opérateurs de voyage et de séjour et aux transporteurs ferroviaires et maritimes.

L'objectif premier est bien de permettre un échange de données passagers en temps réel afin de prévenir toute atteinte à la sécurité des citoyens européens déstabilisés par les évènements tragiques récents et d'aboutir à une harmonisation et à une interopérabilité entre les unités d'information de passagers des États membres.

Il faut souligner que la Cour de justice de l'Union européenne a dans un récent avis No 1/15 du 26 juillet 2017 relatif à un projet d'accord entre le Canada et l'Union européenne sur le transfert de données des dossiers passagers aériens depuis l'Union européenne vers le Canada estimé que cet accord qui reprend d'ailleurs des dispositions identiques à celles de la Directive 2016/681 du 27 avril 2016 du projet de loi sous avis, était incompatible avec les articles 7, 8 et 21 ainsi qu'avec l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne. Ainsi la Cour a estimé que l'accord ne garantissait pas que la conservation et l'utilisation des données PNR après le départ des passagers aériens soient limitées au strict nécessaire en application de l'article 52. paragraphe 1 de la Charte et que par conséquent l'accord entre le Canada et l'Union européenne était incompatible avec

le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et le principe de non-discrimination. Cet avis de la Cour de Justice de l'Union européenne permet qu'on s'interroge aussi sur la compatibilité de la directive avec les susdits articles de la Charte.

L'article 1er du projet de loi dispose que la finalité du traitement des données passager est la prévention, la recherche, la constatation et la poursuite des infractions terroristes et des formes graves de criminalité. Il faut certes relever que la collecte de ces données a à l'origine une finalité purement commerciale. Il n'en reste pas moins que les trois dernières finalités mentionnées relèvent manifestement de la compétence des autorités judiciaires de poursuite. On peut donc s'interroger s'il n'est pas opportun qu'un représentant des autorités judiciaires de poursuite fasse partie de l'Unité d'information passagers (UIP) à créer au sein de la Police grand-ducale.

Dans le cadre de la transposition de la directive 2004/82/CE du Conseil du 29 avril 2004, les entreprises de transport aérien s'étant vues imposer l'obligation de transmettre à la Police grand-ducale les renseignements relatifs aux passagers qu'ils vont transporter c'est de toute évidence que l'UIP est donc créée au sein de la Police.

L'article 2 a pour objet de définir les termes utilisés dans le cadre du projet de loi et ne reprend que partiellement les définitions de l'article 3 de la directive 2016/681. Il est à noter qu'une erreur s'est glissée au niveau de la définition des données PNR en ce sens que l'annexe I jointe au projet de loi reprend au point s) des points 1 à 18 qui de par la nouvelle numérotation par référence à l'alphabet n'existent pas. On ne voit d'ailleurs pas les raisons pour lesquelles le projet de loi ne reprend pas la numérotation de l'annexe I de la directive. On notera que la Cour de Justice de l'Union européenne a dans son avis No 1/15 du 26 juillet 2017 précité relevé que certaines rubriques de l'annexe jointe à l'accord entre le Canada et l'Union européenne laquelle reprend en partie les mêmes rubriques que l'annexe de la directive à transposer n'étaient pas suffisamment claires et précises pour encadrer l'ingérence dans les droits fondamentaux garantis par la Charte.

L'article 4 du projet de loi s'il prévoit que cette UIP est composée de personnel de la Police et le cas échéant de personnel détaché de l'Administration des Douanes et Accises et du Service de renseignement de l'État ne mentionne ni le nombre ni les qualités de ces membres. Il n'est pas non plus précisé que les membres du personnel détachés de ces services seront placés sous l'autorité fonctionnelle et hiérarchique du fonctionnaire dirigeant l'UIP. Il n'est pas non plus explicitement prévu que le dirigeant responsable de l'UIP soit obligatoirement un membre du corps de la Police ou une autre personne comme par exemple le représentant de l'autorité judiciaire si le législateur envisageait de suivre les considérations ci-avant présentées. Seule la fiche financière jointe au projet de loi permet de constater qu'il est prévu d'affecter dans un premier temps 4 membres du personnel de la Police grand-ducale sinon au vu de l'évolution d'envisager un triplement du personnel nécessaire.

L'article 5 se réfère à la „méthode push" sans que l'article 2 relatif aux définitions nous donne de précision quant à cette méthode. On peut s'interroger si la méthode utilisée pour le transfert des données doit vraiment figurer dans un texte de loi alors qu'il s'agit d'une modalité pratique d'exécution. On aurait pu compléter cette disposition en prévoyant que les données des passagers transitant par notre pays soient également communiquées à l'UIP.

L'article 6 ne reprend pas à la lettre la disposition de l'article 8.3.a) de la directive en ce sens qu'il impose une communication des données passagers 48 heures et une autre 24 heures avant le départ alors que la directive semble prévoir une seule communication entre 24 à 48 heures avant l'heure programmée du vol.

L'article 7 a pour objet de transposer l'article 16 de la directive. Il faudrait préciser que le transfert des données PNR se fait par voie électronique **sécurisée** au regard des dispositions de l'article 16 (2) de la directive.

Le projet de loi impose au paragraphe (2) de cet article que les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisées pour leurs transferts. Cet article ne reprend pas la disposition des paragraphes (2) et (3) de l'article 16 de la directive en ce sens qu'il est prévu qu'il appartient à la Commission d'adopter pour la première fois des protocoles communs et des formats de données afin d'assurer la sécurité des données pendant leur transfert et d'assurer qu'en suivant un format reconnu on puisse assurer la lisibilité par toutes les parties concernées. Il appartient aussi à la Commission de dresser la liste des protocoles communs et des formats de données reconnus. En effet il s'agit de pouvoir recourir à des protocoles et formats de données similaires sinon identiques.

L'article 9 prévoit que les données PNR transmises qui comporteraient des renseignements complémentaires à ceux prévus à l'annexe I soient effacées dès réception. Étant donné qu'il est prévu que l'UIP ne fonctionne dans un premier temps que pendant la journée de la semaine en attendant une entrée en opération 24/24 heures il serait peut-être opportun de prévoir un délai fixe maximum pour l'effacement définitif des données concernées.

L'article 10 se réfère pour la première fois aux „services compétents" notion qui ne sera cependant définie qu'à l'article 15 du Chapitre 5 du projet de loi. Il aurait peut-être été préférable et plus lisible de définir d'abord quels sont les services visés.

Dans le cadre de l'évaluation des passagers identifiés sur base de critères préétablis, l'UIP peut comparer les données PNR aux données insérées dans les banques de données gérées par la Police, le Service de renseignement et l'Administration des Douanes et Accises. Ces services ayant chacun accès légal à différentes banques de données il est donc prévisible qu'il y ait une mise en commun de certaines données pour lesquelles l'accès était cependant limité. Ne faudrait-il pas préciser les bases de données avec lesquelles les données PNR seront complétées et limiter le traitement automatisé avec les banques de données exploitées en rapport avec la lutte contre le terrorisme et le crime transnationale?

L'article 12 reprend la disposition de l'article 6. 2. (b) de la directive. On peut s'interroger si une demande qui doit être dûment motivée n'est pas implicitement fondée sur des motifs suffisants, même si cette terminologie est celle utilisée par la directive elle-même.

L'article 13 reprend l'article 7 de la directive en réservant les attributions des autorités judiciaires définies par le Code de procédure pénale alors que le projet de loi sous avis n'envisage pas d'adapter ces compétences. Il semble donc que si les „services compétents" sont habilités à échanger les données PNR sans autre formalité, les autorités judiciaires devront faire application des règles de procédure de droit commun et le cas échéant donc à défaut de pouvoirs complémentaires faire procéder par voie d'instruction préparatoire. Dans ce contexte il faut certes relever que la loi belge du 25 décembre 2016 a expressément prévu une adaptation des règles de procédure pénale en insérant un nouvel article 46 septies au Code d'instruction criminelle disposant que le procureur du Roi peut par décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer des données passagers et que cette mesure peut même porter sur un ensemble de données relatives à une enquête pénale spécifique. Dans ce cas le procureur du Roi doit préciser la durée de la mesure qui ne peut excéder un mois à dater de la décision renouvelable.

L'article 7.1 de la directive prévoit bien que l'évaluation des données PNR a une finalité de prévention et de détection d'infractions terroristes ou d'autres formes graves de criminalité, mais aussi d'instruction et de poursuites relevant du pouvoir judiciaire. Il faudrait donc envisager d'adapter notre Code de procédure pénale sur ce point.

Le projet de loi dispose que les services compétents seront habilités à recevoir les données PNR dans le cadre de leurs attributions légales, mais dans la limite „du besoin d'en connaître". Cette notion de besoin est d'une part imprécise et d'autre part entièrement subjective. La directive est sur ce point plus explicite alors qu'elle prévoit que le résultat du traitement de ces données permette de procéder soit à un examen plus approfondi de ces informations soit de prendre les mesures appropriées aux fins de prévention, détection ou instruction et poursuite.

Par ailleurs, il semble opportun de se référer simplement à la Police grand-ducale et à l'Administration des Douanes et Accises au lieu de se référer à leurs services sans les spécifier.

L'article 14 a pour objet de transposer l'article 7.4. et 5. de la directive en prévoyant une règle de la spécialité en ce sens que les données ne peuvent être utilisées qu'aux fins de prévention, détection, enquêtes et poursuites d'infractions terroristes ou autres formes graves de criminalité. Contrairement au texte de la directive, l'article du projet de loi omet de mentionner les compétences des autorités judiciaires de poursuite qui continuent cependant à assurer la direction des enquêtes judiciaires et à exercer l'action publique à l'issue des instructions pénales.

L'article 16 alinéa 2 transposant l'article 9. 1 de la directive prévoit que lorsque l'UIP a reçu des informations d'une UIP étrangère et qu'une personne a pu être identifiée elle transmet ces informations aux services compétents. On peut s'interroger si toutes les informations doivent être transmises, et ce indépendamment des compétences d'attribution respectives de ces services.

L'article 17 prévoit l'échange de données sur demande motivée d'un autre État. On peut certes s'étonner du fait que les demandes ont pour objet une fois de plus la prévention et la détection d'infractions terroristes et autres formes graves de criminalité, mais aussi plus spécifiquement une enquête ou

des poursuites pénales traditionnellement soumises au système de l'entraide judiciaire pénale avec les garanties qui s'imposent en application des conventions internationales ou traités bilatéraux y relatifs.

Il est prévu qu'une fois les données dépersonnalisées, le transfert de ces données ne puisse s'effectuer que sur autorisation du procureur d'État de Luxembourg. On peut certes s'interroger sur la désignation du procureur d'État en tant qu'autorité compétente alors que d'une part le Procureur général d'État est traditionnellement l'autorité centrale pour tous les instruments relatifs à l'entraide judiciaire et que d'autre part dans le cadre de la loi du 17 mai 2017 portant approbation de l'Accord entre le gouvernement du Grand-Duché de Luxembourg et les États unis aux fins de renforcer la coopération en matière de prévention et de lutte contre le crime grave signé en date du 3 février 2012, la transmission de certaines données a précisément été soumise à l'autorisation du Procureur général d'État.

L'article 18 quant à lui prévoit qu'une demande peut être adressée par l'UIP respectivement les services compétents aux autres UIP de l'Union européenne.

Il semble évident qu'il convient de respecter les conditions de forme et de fond des UIP requis. Si donc les services de police peuvent par simple demande adressée à l'UIP étrangère accéder aux données PNR, cette compétence ne semble pas appartenir aux autorités judiciaires de poursuites.

L'article 21 alinéa 1er fait référence à certains articles d'une loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale laquelle entend sans doute transposer la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, mais dont le projet n'avait pas été déposé au jour du dépôt du présent projet de loi sous avis.

Il est prévu que l'échange direct de données avec des pays non membres de l'Union européenne se fasse même dans le domaine de la constatation et poursuite d'infractions donc dans le cadre d'une instruction pénale proprement dite. S'agit-il là de soustraire cet échange de données aux dispositions traditionnelles de l'entraide judiciaire?

L'article 25 alinéa 2 prévoit une durée de conservation de 5 ans ce qui correspond au délai de l'article 12.1 de la directive. L'alinéa 2 reprend à la lettre l'alinéa 4 de l'article 12 de la directive en ce sens qu'il définit une exception à la règle de la durée de conservation. On aurait pu certes préciser ce qu'au regard de la législation luxembourgeoise on entend par usage dans des „des cas spécifiques" terme plus qu'imprécis et surtout susceptible d'arbitraire.

Au regard des considérations reprises à l'article 17 ci-avant il faut une fois de plus relever que le Procureur général d'État est l'autorité centrale en matière d'entraide judiciaire.

Les articles 28 et suivants traitent de la protection des données à caractère personnel faisant référence à une loi respectivement un projet de loi qui n'a été déposé que postérieurement au présent projet de loi. Y avait-il lieu de reprendre dans le présent projet des dispositions légales spécifiques sinon identiques à celles figurant dans le projet de loi qui entend de façon générale régler la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale?

Les articles 37 et 38 du projet ont trait aux sanctions pénales et administratives.

L'article 37 alinéa 1er prévoit des sanctions pénales identiques à celles prévues à l'article 49 (2) du projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. Si la violation de l'article 8 relatif à l'interdiction de révéler 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 peut se concevoir en tant qu'infraction pénale à condition cependant qu'il y ait eu intention délictuelle on s'interroge cependant sur les sanctions pénales relatives aux violations des articles 15 et 36 du projet de loi sous avis.

Ces articles 15 et 36 correspondent aux articles 1 I et 30 du projet de loi relatif à la protection des données.

Ainsi l'article 15 dispose que les services compétents définis par le projet de loi ne peuvent pas prendre de décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR. Quels sont les éléments constitutifs de cette infraction qui ne rencontre pas non plus le caractère de la prévisibilité nécessaire? Doit-il y avoir une intention délibérée ou non? S'agit-il au contraire d'une infraction purement matérielle de sorte que les agents de la Police, du SRE et de l'Administration des Douanes

et Accises amenés à prendre une décision en violation de cette disposition engageraient leur responsabilité pénale? Les mêmes considérations valent pour la violation de l'article 36 qui prévoit qu'au cas où l'atteinte est susceptible d'engendrer un risque élevé pour la protection des données ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe la personne concernée et l'autorité de contrôle de cette atteinte. S'agit-il vraiment de comportements qui doivent être sanctionnés par la voie pénale?

On peut surtout s'interroger s'il y a lieu de prévoir dans une loi spéciale les mêmes infractions que celles prévues dans la loi générale de la protection de données à caractère personnel ou si on avait pu se limiter à un simple renvoi à cette législation?

L'article 38 du projet prévoit une sanction administrative d'un montant maximum de 50.000 euros par vol pour lequel le transporteur n'a pas transmis les données PNR ou ne les a pas transmis dans le délai imposé. Cet article reprend les principes de procédure de l'article 30-4 de la loi du 21 décembre 2006 sur l'entrée et le séjour des étrangers repris par les articles 108 et 148 de la loi du 29 août 2008 sur la libre circulation et l'immigration. Le montant maximum de l'amende administrative est identique à celui prévu par les législations belges et françaises sauf que l'article 45 de la loi belge du 25 décembre 2016 a prévu un seuil d'amende supérieur en cas de récidive dans les 2 ans.

On aurait pu prévoir afin de respecter le principe du contradictoire que l'entreprise de transport aérien puisse prendre position dès réception du procès-verbal dressé par la Police et non pas à l'issue de la transmission du projet de sanction. En effet ces éléments sont susceptibles d'influer l'appréciation du comportement fautif et le taux de l'amende envisagée sur base de moyens présentés à décharge.

Finalement on note l'absence de règles de procédure quant aux voies de transmission et de notification. Afin de tenir compte de l'évolution technologique depuis la loi du 21 décembre 2006 (actuellement la loi du 29 août 2008 portant libre circulation des personnes et l'immigration) ayant transposé la directive 2004/82/CE du 29 avril 2004 on aurait dû prévoir tant la transmission du procès-verbal sous la forme d'un document numérique qu'une procédure facultative par moyen de communication électronique sécurisé.

Martine SOLOVIEFF
Procureur général d'État

*

AVIS DES PARQUETS DE LUXEMBOURG ET DE DIEKIRCH

(15.10.2017)

Le projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave a pour objet de transposer en droit national la Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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.

L'article 1er définit le champ d'application de la loi et précise que celle-ci règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Les finalités de constatation et de poursuite des infractions incombant essentiellement aux autorités judiciaires, le Parquet de Diekirch entend commenter surtout les dispositions du projet de loi qui impliquent ou, devraient impliquer, l'intervention des Parquets

L'article 3 prévoit la création de l'Unité d'informations passagers (UIP) au sein de la police.

Parmi les missions de cette unité figure au point b le transfert des données et des résultats de leur traitement aux services compétents. Ces services ne sont toutefois définis qu'à l'article 13 du projet de loi, ce qui fait que l'article 3 manque, sans renvoi à l'article 13, de lisibilité.

S'y ajoute que la notion de „service" n'est précisée ni à l'article 3, ni à l'article 13 qui se borne à énumérer, en dehors du Service de Renseignement de l'Etat, les services de la Police grand-ducale ainsi que les services de l'Administration des Douanes et Accises, sans préciser quels services de la Police et des Douanes sont visés par le législateur.

L'article 4 règle la composition de l'UIP.

Or, cette composition n'est pas clairement énoncée dans le texte de loi étant donné qu'il y est fait référence d'une part, au „personnel de la Police grand-ducale" sans indication du nombre et du grade des policiers à affecter à cette unité et d'autre part, à la possibilité d'y intégrer „du personnel détaché de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat", sans en faire une obligation et sans en fixer le grade des agents à y détacher.

Il importe de constater qu'aucun membre des autorités judiciaires chargées de la poursuite des infractions de terrorisme et de criminalité grave n'est prévu pour faire partie de cette unité, ce qui est tout de même étonnant étant donné que la Ddirective à transposer vise les enquêtes et les poursuites du chef d'infractions terroristes et de formes graves de criminalité, et partant l'intégration des données des dossiers passagers recueillies et traitées par l'UIP dans les poursuites pénales à engager par les Parquets.

On peut d'ailleurs se demander s'il ne serait pas recommandable de faire présider cette unité à créer au sein de la Police grand-ducale par un magistrat en vue d'extérioriser à l'égard des passagers le souci du législateur de garantir non seulement le traitement des données PNR, mais également celui de veiller au mieux à la protection de ces données à caractère personnel dans le cadre de la recherche, de la constatation et de la poursuite des infractions de terrorisme et de criminalité grave qui se déroulent sous la direction des autorités judiciaires.

En tout cas, il semble indiqué de déterminer le responsable de l'UIP dans le texte de loi.

L'article 5 impose aux transporteurs aériens le transfert à l'UIP des données PNR concernant tous les passagers de vols à destination ou en provenance du Luxembourg. Comme il n'est pas question des données PNR des voyageurs en transit, il pourrait être soutenu que l'article 8 de la Directive ne serait pas intégralement transposé dans notre législation nationale.

L'article 6 va au-delà des exigences énoncées à l'article 8 de la Directive en prévoyant 2 transferts successifs des données PNR à l'UIP, à savoir 48 heures, puis 24 heures avant l'heure du départ programmée du vol.

Si ce double transfert devait être maintenu, il semble toutefois indiqué, comme déjà prévu pour le point c), que le transfert des données PNR visé au point b) peut se limiter à une mise à jour des transferts visés à l'alinéa 1er, point a).

L'article 8 interdit le traitement des données PNR qui révèlent 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. L'UIP est tenue d'effacer, dès réception et de façon définitive, des informations de ce type lorsqu'elles lui seraient transférées.

Comme la transgression de ces dispositions est punie de peines d'emprisonnement et d'amende conformément à l'article 37, il serait indiqué de prévoir un délai maximal endéans lequel ces données devraient être effacées.

L'article 9 prévoit que les données transférées à l'UIP mais non prévues à l'annexe I du texte de loi, devront être effacées. La violation de cette disposition n'est toutefois réprimée ni par une peine pénale, ni par une sanction administrative. Au vu des dispositions de l'article 8, on aurait pu s'attendre à voir réprimer le fait de préserver de telles données à l'UIP au-delà d'un certain délai qu'il conviendrait de circonscrire avec plus de précision.

L'article 12 dispose que l'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, ceux-ci étant énumérés à l'article 13. Tout en reprenant le texte de la Directive, il est prévu que les demandes des services compétents devraient être dûment motivées et fondées sur des motifs légitimes.

Bien qu'il puisse être soutenu qu'une demande n'est motivée dûment que si elle est fondée sur des motifs légitimes, il faut remarquer que cette condition n'est plus reprise à l'article 13 qui énumère les services qui sont habilités à demander des données PNR à l'UIP. Il n'est pas non plus indiqué qui est appelé à apprécier le bien-fondé de la motivation invoquée par le service compétent.

L'article 13 détermine les services compétents habilités à demander et à recevoir de la part de l'UIP des données PNR ou le résultat du traitement de ces données.

Cet article entend transposer l'article 7, points 1 et 2 de la Directive qui précise que les autorités compétentes qui sont habilitées à demander et à recevoir de la part de l'UIP des données PNR sont des

autorités compétentes en matière de prévention ou de détection des infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes ou des poursuites en la matière.

La Directive parle ainsi d'autorités et non de services et énumère parmi ces autorités celles qui ont compétence en matière de poursuites.

Les „services" énumérés par le projet de loi sont a) les services de la Police grand-ducale, b) le Service de Renseignement de l'Etat et c) les services de l'Administration des Douanes et Accises.

En mentionnant sans précision les services de la Police grand-ducale ainsi que les services de l'Administration des Douanes et Accises, le législateur semble habiliter tout policier et tout douanier à formuler une demande à l'UIP pour recevoir des données PNR ou le résultat du traitement de ces données.

Par contre, en faisant précéder cette énumération des termes „Sans préjudice des attributions des autorités judiciaires telles définies par le Code de procédure pénale", le texte du projet pourrait être interprété en ce sens qu'à défaut de disposition expresse contenue au Code de procédure pénale, les autorités judiciaires chargées d'engager les poursuites pénales, n'auraient aucun droit d'accès direct aux données PNR, mais devraient recourir aux procédures de droit commun pour se faire délivrer ces données.

Comme la Directive prévoit l'habilitation des autorités qui ont compétence en matière de poursuites, à demander et à recevoir directement des données PNR de la part de l'UIP, il est proposé, en vue d'une transposition correcte et intégrale de la Directive, de faire figurer les autorités judiciaires dans l'énumération des autorités habilitées à demander et à recevoir de la part de l'UIP des données PNR ou le résultat du traitement de ces données.

Pour couper court à toute discussion ultérieure sur les intentions du législateur en la matière, la notion de „service" devrait être précisée.

L'article 15 prévoit que les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Une violation de cette obligation est punie de peines d'emprisonnement et/ou d'amende en application de l'article 37 du projet de loi.

Le texte de l'article 15 qui reprend celui énoncé à l'article 7. point 6 de la Directive, ne semble toutefois pas assez précis pour qu'il puisse être érigé en infraction pénale au vu notamment des termes „préjudiciable" et „significative" qui donneront nécessairement lieu à des interprétations divergentes en cas de poursuites pénales devant un tribunal répressif.

A qui incomberait d'ailleurs la responsabilité pénale du „service" qui prendrait une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la base du traitement automatisé des données PNR? Est-ce que cette décision, pour être répréhensible, devrait être prise avec le dol général d'enfreindre la loi pénale ou est-ce que le simple fait de prendre une telle décision suffirait pour justifier des poursuites pénales?

L'article 18

Comme les autorités judiciaires ne sont pas mentionnées à l'article 13 parmi les services compétents habilités à demander et à recevoir de la part de l'UIP des données PNR, il semble que serait également exclue la possibilité pour les autorités judiciaires de formuler une demande directe aux UIP des autres Etats membres, et que les autorités judiciaires devraient procéder par la voie d'une commission rogatoire internationale sur base des traités réglant l'entraide judiciaire pour obtenir une transmission de données PNR recueillies à l'étranger.

Une reformulation de l'article 13 en vue d'une transposition complète de la Directive permettrait de remédier à un tel retard injustifié pour l'accomplissement d'enquêtes et de poursuites du chef d'infractions de terrorisme et de criminalité grave.

Les articles 20 à 24 déterminent les conditions du transfert des données PNR vers des pays non membres de l'Union européenne.

Si ces conditions proprement dites n'appellent aucune observation particulière, il convient par contre de relever que le texte de loi omet de déterminer qui est appelé à contrôler le respect de ces conditions et à autoriser la transmission des données à l'État non membre de l'Union européenne. A défaut de toute indication à ce sujet, ce contrôle ne peut appartenir qu'au responsable de l'UIP qui, conformément à l'article 4, a la qualité de responsable du traitement des données PNR.

Comme cette transmission des données PNR peut viser la poursuite proprement dite, dans des pays non membres de l'Union européenne, d'infractions terroristes et de formes graves de criminalité où le transfert d'informations est soumis aux formes et conditions d'entraide judiciaire applicables avec ces États, il est renvoyé aux commentaires développés à l'article 4 pour souligner l'importance de voir déterminer avec précision dans le texte de loi qui est le responsable de l'UIP et d'envisager la nomination d'un magistrat à ce poste.

L'article 36 prévoit l'obligation pour l'UIP d'informer, sans retard injustifié, la personne concernée ainsi que l'autorité compétente lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection de ces données ou d'affecter négativement la vie privée de cette personne.

La violation de cette obligation est punie de peines d'emprisonnement et/ou d'amende en application de l'article 37 du projet de loi.

Le texte de l'article 36 reprend l'article 13 point 8 de la Directive, mais semble trop imprécis, notamment en faisant référence à „un risque élevé", pour une application en droit pénal.

Est-ce que le législateur entend effectivement engager la responsabilité du directeur de l'UIP ou d'un des agents y affectés en cas de retard injustifié d'une transmission d'informations à une personne? Ce retard injustifié devra-t-il résulter d'une abstention volontaire? Ou est-ce qu'il suffira de retenir une simple négligence de l'auteur de l'infraction, voire le simple constat d'un retard injustifié pour engendrer la condamnation pénale de la personne mise en cause?

L'article 37 érige en infraction pénale l'inobservation des articles 8, 15 et 36 du projet de loi.

Ainsi, l'interdiction prévue à l'article 8 de traiter des données PNR qui révèlent 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 est punie d'un emprisonnement de huit jours à un ans et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie pourra en outre prononcer la cessation du traitement contraire „aux dispositions du présent alinéa" sous peine d'une astreinte dont le maximum est fixé par la juridiction.

Il est d'abord demandé pourquoi la juridiction saisie ne devrait pas obligatoirement prononcer la cessation du traitement prohibé et réprimé pénalement au vu de sa gravité? En énonçant que la juridiction saisie pourra prononcer la cessation du traitement illégal, le législateur laisse en effet aux juges un pouvoir d'appréciation qui pourrait aboutir à la continuation de l'acte prohibé, ce qui ne semble guère indiqué.

Le renvoi „aux dispositions du présent alinéa" ne semble d'autre part pas tout-à-fait correct puisqu'il s'agit plutôt d'un traitement contraire aux articles 8, 15 et 36 du texte de loi.

Jean-Paul FRISING
Procureur d'Etat à Luxembourg

Aloyse WEIRICH
Procureur d'Etat à Diekirch

*

AVIS DU TRIBUNAL D'ARRONDISSEMENT DE ET A LUXEMBOURG

(18.9.2017)

Note sur le projet de loi relative au traitement des dossiers passagers dans le cadre de la prévention de la répression du terrorisme et de la criminalité grave

Il est entendu que le but de la législation projetée n'est pas discutable, la connaissance des données en relation avec les déplacements effectuées par les personnes constitue, à l'évidence, un élément très important dans la lutte, tant contre le terrorisme, que la criminalité grave, tel que cela est d'ailleurs exposé dans le paragraphe „Objet du projet de loi".

A noter qu'il est indubitable que la frontière entre le terrorisme et le grand banditisme est très perméable et que les uns et les autres ont besoin de ressources financières, de logistique, d'un „savoir-faire" et de contacts qui se contactent et se recrutent parfois de la même façon, dans les mêmes régions/pays et dans un même milieu, quoique avec une idéologie et un but légèrement différents.

Ainsi, la surveillance et la connaissance des „patterns of movement" sera un outil important, tant au niveau de la prévention que de la répression de toutes les personnes impliquées dans ces activités, en quelque qualité que ce soit (auteur, coauteur, complice ou autre „intermédiaire ou sympathisant").

Ceci étant, il faudra néanmoins veiller à entourer la collecte de ces données essentiellement liées notamment à la liberté d'aller et de venir, d'une protection adéquate, tel que cela est repris au paragraphe intitulé „La protection des données à caractère personnel".

A cette fin, il faudra établir un juste équilibre entre les nécessités de la politique sécuritaire telle qu'elle est exigé au regard de la situation actuelle, tant au niveau de la répression du grand banditisme que, sien évidemment, du terrorisme.

Dans un souci de lisibilité seuls les chapitres et articles qui ont semblé appeler un bref commentaire ont été repris ci-après.

Article 8

L'exclusion des critères repris à l'article 8 est conforme à la finalité de la loi qui tend à concilier impératifs sécuritaires et protection de données personnelles. L'indication de la nationalité devrait suffire dans le cadre de la présente loi.

En cas de suspicion légitime, le SRE p. ex. devrait disposer de ressources permettant de creuser un peu plus profond, en cas de besoin (cf.: article 10). Cette compétence d'autres services et les impératifs d'une enquête éventuellement à mener ne font cependant pas directement l'objet du présent projet de loi.

Chapitre 5

Le chapitre 5 du projet de loi met en exergue la séparation des compétences entre les différents services, sans préjudice des attributions des autorités judiciaires telles qu'elles résultent du code de procédure pénale, ce qui semble une évidence.

Les données PNR devraient ainsi pouvoir être saisies, soit sur décision du Parquet ou d'un juge d'instruction, selon la situation procédurale qui se présente. Cette base de données pourrait ainsi se révéler un outil important, tant dans la prévention que dans la répression des infractions visées par le présent projet de loi. Il devrait également être permis au parquet d'avoir accès à ces données dans le cadre d'une enquête préliminaire dans les matières visées à l'annexe II.

Il est également important de souligner que les personnes chargées du traitement des données PNR, ne sont habilitées à ce faire que dans le cadre de leurs attributions et ne suppléent en aucun cas à des enquêteurs de quelque service que ce soit.

Chapitre 7

Le chapitre 7 du projet de loi met une limite à la diffusion automatique des informations PNR à Europol et rejoint en quelque sorte la limitation déjà prévue au chapitre 5. Il s'agit d'éviter une diffusion automatique à Europol, hors le cadre très limité défini à ce chapitre, ce qui correspond également à l'esprit du projet de loi, en évitant une sorte de „fishing/charing" automatique.

Chapitre 8

Le chapitre 8 oeuvre dans le même sens.

Chapitre 9

Le chapitre 9 limite la durée de conservations des données PNR à 5 ans, sauf l'exception y prévue, ce qui permet d'éviter un stockage „illimité" de ces données, garantie d'une certaine protection de ces données, non utilisées.

Chapitre 10

Le chapitre 10 concerne la protection des données et le rôle du délégué à la protection des données au sein de l'UIP.

Ce responsable est désigné par l'UIP et il fait directement rapport au responsable de l'UIP.

Dans un souci de transparence et d'impartialité la question se pose si le délégué à la protection des données ne devrait pas être désigné par une instance extérieure à l'UIP, certes avec les mêmes exigences professionnelles.

En prenant en considération le but poursuivi par cette législation dans le cadre de la situation géo-politique actuelle, il n'y a pas d'objections particulières à ce projet de loi qui concilie à suffisance les exigences sécuritaires évidentes et la protection des données personnelles.

Il s'agit en définitive d'éviter les abus de la collecte, de la conservation et de la diffusion de ces données, l'utilité de cette pratique, dans le cadre du présent projet de loi n'étant cependant pas à remettre en cause en tant que telle.

Chapitre 11

Quitte à mélanger les sanctions pénales et civiles, ne devrait-on pas indiquer une limite (en durée/ montant) concernant l'astreinte que la juridiction répressive serait éventuellement amenée à prononcer?

Ceci d'autant plus que si la pratique répréhensible de l'UIP continuerait, on se trouverait de nouveau face à une nouvelle infraction pour laquelle une nouvelle sanction pénale serait envisageable. La raison de l'astreinte en la présente matière semble discutable et résulter d'un souci quelque peu exagéré en matière de protection des données personnelles.

Dans l'ensemble le projet de loi reflète dès lors à suffisance un juste équilibre entre l'utilité et la nécessité indiscutable de la collecte des données PNR et le souci de protection des données personnelles qui ne devraient en aucun cas être accessibles et utilisables en dehors du champ légal dans le cadre duquel elles ont été collectées.

ANNEXE II

Listing des infractions:

Quelques considérations: (Sous réserve des impératifs liés au texte même de la directive UE 2016/681 du Parlement européen)

Point a):

Il se pose la question pourquoi l'association de malfaiteurs ne figure pas dans ce listing alors que surtout en matière de criminalité grave, on n'est pas forcément toujours en présence d'une organisation criminelle. Il serait éventuellement utile d'inclure l'association de malfaiteurs (au sens des dispositions de l'article 322 code pénal) afin d'éviter éventuellement des problèmes procéduraux subséquents.

Point e)

Il se pose la question s'il ne serait pas opportun d'inclure plus généralement TOUTE infraction à la législation sur les armes, les munitions et les explosifs et de ne pas se limiter textuellement, ab initio, au seul terme de „Trafic". Compte tenu des infractions concernées par ce projet de loi, ceci semble quelque-peu restrictif.

A titre d'exemple: une personne (physique ou morale) peut légalement détenir des armes/explosifs qu'elle mettra à disposition d'une autre qui s'en servira pour commettre des infractions, le fournisseur

n'aura pas participé, au sens strict, à un trafic d'armes. Ceci ne fera qu'alimenter des discussions procédurales.

Point h)

Il se pose la question du blanchiment du produit du CRIME. Ce terme semble superflu. Il serait utile de ne pas se limiter textuellement au blanchiment du produit du CRIME, même entendu en son sens générique. Ceci permettrait d'éviter des discussions procédurales.

Point I

L'assassinat ne figure pas dans ce listing; certes il s'agit d'un meurtre avec la circonstance aggravante de la préméditation, mais afin d'être complet et toujours dans un souci d'éviter les discussions procédurales, ne faudrait-il pas l'inclure?

Point O

Il se pose la question s'il ne faudrait pas viser textuellement le vol commis en association également, la criminalité grave ne nécessitant pas forcément toujours l'existence d'une organisation criminelle et fait aussi partie des infractions à forte propension migratoire.

Point X

A noter que les infractions de terrorisme au sens des dispositions du chapitre III-1 du code pénal, articles 135-1 à 136, ne sont pas reprises textuellement sur ce listing?

Le terme sabotage semble quelque peu vague, notamment au vu du champ d'application du présent projet de loi. Ne serait-il pas utile d'inclure textuellement les infractions reprises ci-avant.

Paul VOUEL

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/02

N° 7151²

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(23.11.2017)

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après : « la CNPD ») a notamment pour mission d'aviser *« tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Sécurité intérieure en date du 15 juin 2017, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n° 7151 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave (ci-après : « le projet de loi »).

Ledit projet de loi a pour objet de transposer en droit national la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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 (ci-après : « la directive PNR »).

Deux autres instruments européens qui constituent le « paquet sur la protection des données » s'ajoutent à la directive PNR, réformant en profondeur le droit de la protection des données au niveau de l'Union européenne. Ainsi, le Parlement européen et le Conseil ont adopté parallèlement en date du 27 avril 2016:

– le règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après : « le RGPD ») ;
– la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après « la directive 2016/680 »).

Suivant l'exposé des motifs, le projet de loi vise à « *régler le transfert des données PNR des transporteurs aériens vers une unité centrale nationale ayant pour mission la répression et la prévention des infractions terroristes et d'autres formes graves de criminalité ainsi que le traitement ultérieur de ces données*. »

La Commission nationale est bien consciente que le législateur a l'obligation de transposer la directive PNR en droit national au plus tard pour le 25 mai 2018, faute de risquer un recours en manquement de la part de la Commission européenne sur base des articles 258 et 260 du traité sur le fonctionnement de l'Union européenne.

De manière générale, l'intention de la CNPD n'est ainsi pas de remettre en cause en lui-même le système PNR, dont la mise en place a été décidée par le législateur européen « *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. »[1] Par ailleurs, à part une restructuration des articles, le projet de loi est quasiment une copie fidèle de la directive PNR. La Commission nationale limite ainsi ses observations aux dispositions où les auteurs du projet de loi ont usé la marge de manoeuvre laissée aux Etats-membres lors de la transposition en droit national d'une directive européenne. En effet, une telle directive n'instaure qu'une obligation de résultat, tout en laissant les Etats-membres de l'Union européenne libres quant aux formes et moyens à prendre pour y parvenir.[2]

Néanmoins, la Commission nationale tient à relever à titre préliminaire que la Cour de Justice de l'Union européenne (ci-après : « la CJUE ») a critiqué dans son arrêt «Digital Rights Ireland » que la directive 2006/24 sur la conservation de données par les services de communications électroniques, directive annulée suite audit arrêt, n'avait établi aucune relation entre d'un côté les données collectées et conservées et de l'autre côté une menace à l'ordre public en n'étant pas « *limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves*. »[3]

S'agissant du contexte spécifique des données PNR, la CJUE a par ailleurs pris position dans son avis 1/15 du 26 juillet 2017 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers. Elle a souligné que pour les passagers aériens où aucun risque en matière de terrorisme ou de criminalité transnationale grave n'a pu être identifié à leur arrivée au Canada et jusqu'à leur départ de ce pays tiers, il n'y existe pas, une fois qu'ils sont repartis, de rapport (directe ou indirecte) entre leurs données PNR et l'objectif poursuivi par l'accord envisagé qui justifierait la conservation de ces données. La CJUE a rejeté les considérations avancées par le Conseil et la Commission se basant sur la durée de vie moyenne des réseaux internationaux de criminalité grave, ainsi que sur la durée et la complexité des enquêtes portant sur ces réseaux, afin de « *justifier un stockage continu des données PNR de l'ensemble des passagers aériens après leur départ du Canada aux fins d'un accès éventuel auxdites données, indépendamment d'un lien quelconque avec la lutte contre le terrorisme et la criminalité transnationale grave*. »[4]

La CJUE a néanmoins aussi relevé que, dans des cas particuliers, l'identification d'éléments objectifs permettant de considérer que certains passagers aériens pourraient, même après leur départ du Canada, présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave, la conservation de leurs données PNR paraissait admissible au-delà de leur séjour au Canada.[5]

Sur base des considérations ci-dessus, la CNPD doute que le système tel que prévu par la directive PNR, fixant une durée de conservation des toutes les données PNR pendant une durée de 5 ans (même si les données sont dépersonnalisées après six mois), indépendamment du fait si le passager est soupçonné d'avoir participé à un acte du terrorisme et de la criminalité grave ou non, garantit que la conservation et l'utilisation des données PNR soient limitées au strict nécessaire. Des inquiétudes quant à la proportionnalité entre le respect des droits des personnes concernées et les intérêts de poursuite des autorités compétentes subsistent. Il est fort probable que la CJUE sera saisi de recours en annulation de la directive PNR à l'instar de la directive 2006/24 sur la conservation de données par les services de communications électroniques.

---

1 Considérant 6 de la directive PNR.

2 L'article 288 du traité sur le fonctionnement de l'Union européenne dispose que la « *directive lie tout État membre destinataire quant au résultat à atteindre tout en laissant aux instances nationales la compétence quant à la forme et aux moyens*. »

3 CJUE, arrêt C-293/12 – Digital Rights Ireland et Seitlinger e.a. du 8 avril 2014, paragraphe 59, voir aussi arrêt C-203/15 – Tele2 Sverige du 21 décembre 2016, paragraphe 110.

4 Avis 1/15 de la CJUE du 26 juillet 2017 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, paragraphe 205.

5 Avis 1/15 de la CJUE, précité, paragraphe 207.

– Quant au champ d'application

Tout d'abord, la CNPD tient à féliciter les auteurs du projet de loi d'avoir anticipé le dépôt à la Chambre des députés du projet de loi portant transposition de la directive 2016/680 et d'y faire référence aux endroits où la directive PNR renvoie encore à la décision-cadre 2008/977, décision qui sera abrogée à partir du 6 mai 2018 par ladite directive.

Dans son article 2, la directive PNR laisse le choix aux Etats-membres de collecter les données PNR, en sus des vols en provenance ou à destination d'un pays tiers, aussi pour l'ensemble ou seulement une partie des vols intra-UE. Dans l'exposé des motifs, les auteurs du projet de loi se réfèrent à une déclaration commune du 4 décembre 2015, par laquelle les ministres européens de la Justice et des Affaires intérieures se sont engagés à faire usage de cette faculté pour justifier la collecte des données PNR pour tous les vols à partir ou en provenance d'un Etat-membre vers le territoire luxembourgeois.

Ainsi, la Commission nationale prend note que les auteurs du projet de loi ont opté, à l'instar de leurs homologues belges, français ou allemands, d'inclure les vols intra-UE dans le champ d'application du projet de loi afin de maximiser l'efficacité du système PNR.

Par ailleurs, la CNPD approuve la décision des auteurs du projet de loi de ne pas avoir étendu le système PNR aux agences ou organisateurs de voyages, ainsi qu'aux d'opérateurs économiques autres que les transporteurs ou auprès de transporteurs autres que les transporteurs aériens.

Comme un tel élargissement du champ d'application du système PNR menacerait de manière encore plus importante les droits fondamentaux des personnes concernées, il paraît raisonnable d'attendre l'évaluation de la Commission européenne de tous les éléments de la directive PNR. Cette évaluation aura lieu au plus tard le 25 mai 2020, c'est-à-dire deux ans après le délai de transposition de la directive PNR, et elle portera notamment sur la nécessité, la proportionnalité, et l'efficacité d'inclure lesdits opérateurs économiques dans le champ d'application de la directive PNR.

Finalement, la CNPD se demande si l'obligation de transmettre à l'Unité d'informations passagers (ci-après : « l'UIP ») les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg s'impose aussi aux taxis aériens privés. A priori, il paraît qu'une compagnie aérienne privée offrant des vols du et vers le Grand-duché correspond à la définition d'un « transporteur aérien »[6], si elle possède une licence d'exploitation en cours de validité octroyée par la Direction de l'Aviation Civile et si elle assure un transport aérien de personnes.

– Quant aux bases de données et critères d'évaluation

Sur base de l'article 10 du projet de loi, transposant l'article 6, paragraphe (3) de la directive PNR, deux méthodes s'offrent à l'UIP pour évaluer des passagers avant leur arrivée ou leur départ prévu du Grand-duché afin d'identifier des personnes « suspectes » pour lesquelles un examen plus approfondi apparaît nécessaire:

– une comparaison des données PNR aux banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;
– une comparaison des données PNR à des critères préétablis.

Le Contrôleur européen de la protection des données (ci-après : « le CEPD ») avait noté dans ce contexte qu'une évaluation sur base de critères inconnus en constante évolution suscite d'importantes inquiétudes en matière de transparence et de proportionnalité.[7] De même, il a soulevé le caractère controverse, excessif et disproportionné d'un système permettant une confrontation systématique des données PNR à un nombre illimité de bases de données non définies.[8]

---

6 Article 2, lettre a) du projet de loi : *«transporteur aérien» toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes ».*

7 Avis 2011/C 181/02 du 22 juin 2011 du Contrôleur européen de la protection des données 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, paragraphe 16.

8 Deuxième avis n°5/2015 du CEPD 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, paragraphe 37.

Dans le même contexte, l'avocat général Mengozzi avait relevé dans ses conclusions présentées le 8 septembre 2016 sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers le manque de précisions dans l'accord en cause concernant les bases de données et les critères d'évaluation dont la détermination restait de ce fait à l'entière discrétion des autorités canadiennes. Il avait souligné qu'un encadrement précis des critères d'évaluation devrait « *permettre, dans une large mesure, d'aboutir à des résultats ciblant des individus à l'égard desquels pourraient peser un « soupçon raisonnable » de participation à des infractions terroristes ou de criminalité transnationale grave*. »[9] La CJUE a repris la position de l'avocat général dans son avis 1/15 tout en précisant que les bases de données avec lesquelles les données PNR seraient recoupées devraient être fiables, actuelles et limitées à des bases de données exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave.[10]

En prenant en compte les commentaires ci-dessus, la Commission nationale est d'avis que le projet de loi en son état actuel ne définit pas avec exactitude les banques de données en cause. Le commentaire des articles quant à lui mentionne uniquement à titre d'exemple le « *Schengen Information System ou Interpol* ». Or, la Commission nationale se demande si toutes les bases de données prévues à l'article 54 du projet de loi n°7045 portant réforme de la Police grand-ducale et abrogeant la loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police sont visées ? Qu'en est-il de l'accès aux bases de données par le personnel détaché de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat qui peuvent être membre de l'UIP ?

Par ailleurs, la CNPD constate que l'article 10 du projet de loi ne contient pas de liste exhaustive énumérant les critères d'évaluation, mais prévoit uniquement que les critères doivent « *être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur 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*. » Le commentaire des articles quant à lui énumère seulement des exemples de critères tel le mode de paiement, le poids du bagage ou l'itinéraire choisi.

La Commission nationale tient à souligner dans ce contexte l'importance fondamentale du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52, paragraphes (1) et (2) de la Charte des droits fondamentaux de l'Union européenne. En substance, ces deux articles, ensemble avec la jurisprudence constante de la Cour européenne des droits de l'homme, retiennent qu'un traitement de données effectué par une autorité publique peut constituer une ingérence dans le droit au respect de la vie privée ou limiter l'exercice du droit à la protection des données. Cette ingérence ou limitation peut être justifiée à condition qu'elle :

- soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;
- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;
- respecte le contenu essentiel du droit à la protection des données ;
- réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

L'article 6, paragraphe (3) du RGPD, qui sera applicable à partir du 25 mai 2018 dans tous les Etats membres de l'Union européenne, prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être prévus soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

Suivant ledit article, ces bases légales devraient contenir des dispositions spécifiques concernant, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données

---

9 Conclusions de l'avocat général M. Paolo Mengozzi présentées le 8 septembre 2016 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, paragraphes 253 et 256.

10 Avis 1/15 de la CJUE, précité, paragraphe 172

peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

Au niveau national, la Commission nationale tient à rappeler à cet égard l'exigence de la Cour constitutionnelle selon laquelle « *dans les matières réservées par la Constitution à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc*. »[11]

Le Conseil d'Etat rappelle lui aussi régulièrement dans ses avis que « *(...) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication (...). »[12]

Dans l'optique de la CNPD, le projet de loi devrait identifier et énumérer expressément dans le corps du texte les différentes banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions. Un règlement grand-ducal pourra alors prévoir une liste exhaustive des critères d'évaluation prédéterminés qui pourrait au besoin être complétée ou modifiée si nécessaire. Le groupe de travail européen « article 29 » a rappelé dans ce contexte l'importance fondamentale de l'existence de critères spécifiques, nécessaires, justifiés et qui sont révisés régulièrement.[13]

La CNPD estime ainsi qu'en l'état actuel, le texte du projet de loi ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal et ne peut pas être considéré comme étant conforme à l'article 4 de la loi modifiée du 2 août 2002, ni à l'article 8 de la Convention européenne des droits de l'homme, à l'article 52 de la Charte des droits fondamentaux de l'Union européenne, ainsi qu'à l'article 6, paragraphe (3) du RGPD.

– Quant aux différentes catégories de données PNR

L'annexe 1 du projet de loi reprend mot par mot la liste des données PNR prévue à l'annexe 1 de la directive PNR. De même, la liste des données PNR que les transporteurs aériens seraient appelés à transférer en application de l'accord prévu entre le Canada et l'Union Européenne contient pour l'essentiel les mêmes dix-neuf catégories de données. A ce titre, dans les conclusions précitées, l'avocat général Mengozzi avait éprouvé des doutes sérieux quant au libellé suffisamment clair et précis de certaines catégories de données PNR contenues dans ledit accord. Il avait notamment critiqué que parmi les différentes catégories, il y en avait qui étaient « *formulées de manière très, voire excessivement, ouverte, sans qu'une personne raisonnablement informée puisse déterminer soit la nature, soit la portée des données à caractère personnel que ces catégories sont susceptibles de contenir*. »[14] L'avocat général s'était surtout référé à la rubrique relative aux informations disponibles sur les « grands voyageurs ». La même critique avait été soulevée par le CEPD dans son avis de 2011 concernant le champ « remarques générales ».[15]

Dans l'avis 1/15 précité concernant le projet d'accord PNR entre le Canada et l'Union européenne, la Grande Chambre de la CJUE a repris les observations de l'avocat général quant au manque de clarté et de précision de certaines données PNR à transférer. Entre-autres, la CJUE avait estimé que les rubriques « grands-voyageurs » et « remarques générales » « *n'encadrent pas de manière suffisamment claire et précise la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte*. »[16]

---

11 Arrêt 117 de la Cour constitutionnelle du 20 mars 2015

12 Voir par exemple : Conseil d'Etat, Avis n° 6975/5 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

13 Opinion 10/2011 du groupe de travail "article 29" sur la Proposition de la directive PNR, p. 5.

14 Conclusions de l'avocat général M Paolo Mengozzi, précitées, paragraphe 217.

15 Avis 2011/C 181/02 du 22 juin 2011 du Contrôleur européen de la protection des données, précité, paragraphe 39.

16 Avis 1/15 de la CJUE précité, paragraphe 163.

Dans le souci de respecter le principe de légalité, la Commission nationale se rallie aux avis de la CJUE et du CEPD et recommande aux auteurs du projet de loi de décrire de manière plus précise et concise les deux catégories de données PNR susmentionnées.

– Quant à la conservation des données

D'après le considérant 26 de la directive PNR, le droit national des Etats-membres de l'Union européenne devrait prévoir des durées de conservation spécifiques, si des données PNR ont été transmises à une autorité compétente dans le cadre d'enquêtes ou de poursuites pénales spécifiques. Or, l'article 25, alinéa 2 du projet de loi, prévoyant une obligation d'effacement des données PNR à l'issue de cinq ans, ne s'impose pas si des « *données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière* ». Ainsi, ledit article ne contient pas en lui-même de durée de conservation spécifique à respecter par les services compétents en cas de transfert de données par l'UIP. Dès lors, la Commission nationale recommande aux auteurs du projet de loi d'inclure dans le corps du texte une telle durée de conservation.

– Quant au droit à l'information des personnes concernées

S'agissant du droit des passagers aériens d'être informés du traitement des données à caractère personnel les concernant, la directive PNR ne prévoit qu'en son considérant (29) que les États membres devraient veiller à ce que les passagers reçoivent des informations précises, aisément accessibles et facilement compréhensibles sur la collecte des données PNR, le transfert de celles-ci à l'UIP, ainsi que sur leurs droits en tant que personnes concernées.

En vertu de l'article 30 du projet de loi, l'UIP a l'obligation de mettre à la disposition du public, par les moyens de communication appropriés, un certain nombre d'informations, comme par exemple ses coordonnées, celles du délégué à la protection des données, ou encore les finalités du traitement envisagé. Le corollaire de cette disposition figure à l'article 13 du projet de loi transposant la directive 2016/680. Or, ledit article contient en son paragraphe (2), en sus des informations prévues à l'article 30 du projet de loi, d'autres indications à communiquer à la personne concernée. Il s'agit notamment de la durée de conservation des données à caractère personnel et le cas échéant, des catégories de destinataires des données à caractère personnel, y compris dans les pays tiers ou au sein d'organisations internationales.

Dès lors, dans un souci de concordance entre les deux textes, la Commission nationale suggère aux auteurs du projet de loi d'inclure les deux indications susmentionnées dans les informations que l'UIP doit transmettre au public.

Par ailleurs, la CJUE a mentionné dans son avis 1/15 précité que l'accord PNR prévu entre le Canada et l'Union européenne devrait préciser que l'autorité canadienne compétente a l'obligation d'informer individuellement les passagers aériens, dont les données PNR ont été utilisées et conservées, ainsi que ceux dont les données ont été communiquées à d'autres autorités publiques, d'une telle utilisation et d'une telle communication, et ceci à partir du moment où cette information n'est plus susceptible de compromettre les enquêtes conduites par les autorités publiques visées par l'accord envisagé.[17]

La Commission nationale partage la position de la CJUE et recommande dès lors aux auteurs du projet de loi de prévoir dans le texte sous examen une disposition selon laquelle l'UIP est obligée d'informer les personnes concernées dont les données PNR ont été utilisées ou transférées, tout en y incluant la possibilité d'un retard ou d'une limitation du droit à l'information des personnes concernées conformément à l'article 13, paragraphe (3) du projet de loi transposant la directive 2016/680.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 23 novembre 2017.

La Commission nationale pour la protection des données

Tine A. LARSEN	Thierry LALLEMANG	Christophe BUSCHMANN
Présidente	*Membre effectif*	*Membre effectif*

17 Avis 1/15 de la CJUE précité, paragraphes 223 à 225.

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/03

N° 7151[3]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

AVIS DE LA COUR SUPERIEURE DE JUSTICE

(20.11.2017)

En date du 29 juin 2017, Monsieur le Ministre de la Justice a sollicité de la de la Cour Supérieure de Justice (la Cour) pour Monsieur le Ministre de la Sécurité Intérieure un avis sur le projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave constituant la transposition de la directive 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.

Parallèlement, un avis sur le projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale a été sollicité par Monsieur Ministre de la Justice (transposition de la directive (UE) 2016/680) et un avis sur le projet de loi portant création de la Commission nationale pour la protection des données et la mise en oeuvre du règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données a été sollicité par Monsieur le Ministre des Communications et des Médias.

Les projets de loi sous avis constituent la mise en oeuvre et la transposition en droit national du règlement UE 2016/679, précité et de deux directives européennes (UE 2016/680 et UE 2016/681) visant à l'harmonisation des dispositions nationales des Etats membres en matière de protection de données personnelles et ils forment un paquet de dispositions sur cette protection de données qui devront de ce fait être considérées ensemble.

Ils instaurent une réforme du cadre existant, visant à renforcer la protection des données à caractère personnel et à adapter les règles aux nouveaux défis réglementaires, dans un souci de pérennité et de neutralité technologique, en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

Le projet de loi sous avis a pour objet de transposer en droit national la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) (*Passenger Name Record*) 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. Cette directive fait suite à la directive 2004/82/CE du Conseil du 29 avril 2004 imposant l'obligation aux transporteurs aériens de communiquer les données relatives aux passagers, directive transposée en droit luxembourgeois par la loi du 21 décembre 2006 et qui prévoyait entre autre l'obligation pour les transporteurs aériens de fournir préalablement, et ce avant la fin de l' enregistrement toutes les informations relatives à leurs passagers.

L'objectif de la directive (UE) 2016/681 est de permettre un échange de données passagers en temps réel afin de prévenir toute atteinte à la sécurité des citoyens européens marqués par les évènements tragiques récents et d'aboutir à une harmonisation et à une interopérabilité entre les unités d'information de passagers des Etats membres.

Les données PNR qui font l'objet de la directive sont issues des données fournies lors des réservations auprès des entreprises de transport aérien, contiennent davantage d'éléments et sont plus rapidement disponibles.

La finalité du traitement des données des passagers s'inscrit dans le cadre de la prévention et de la recherche d'infractions terroristes, des formes graves de criminalité, des atteintes à l'ordre public dans le cadre de la radicalisation violente et des activités pouvant menacer les intérêts fondamentaux des Etats membres de l'Union européenne. Ces menaces terroristes, tout comme la criminalité grave et organisée, appellent une approche commune des Etats membres et la directive permet de prévoir la possibilité d'étendre l'obligation de collecte des données des passagers à d'autres transporteurs, tels les transporteurs ferroviaires ou maritimes. Contrairement aux législateurs français et belges, le législateur luxembourgeois n'a pas choisi d'appliquer les dispositions découlant de la directive à d'autres opérateurs de transport que les transporteurs aériens.

Il convient d'observer que dans un récent avis n° 1/15 du 27 juillet 2017 relatif à l'accord PNR UE-Canada et après plusieurs arrêts historiques mettant au premier plan le droit fondamental à la protection des données personnelles (arrêts *Digital Rights Ireland Ltd*, C-293/12 et C-592/12, 8 avril 2014, *Schrems*, C-362/14, 6 octobre 2015 et *Tele2 Sverige* (C-203/15, 21 juillet 2016) qui pouvaient laisser entrevoir une invalidation du système PNR en raison de la condamnation par la Cour de justice de l'Union européenne (CJUE) de tout stockage de données de masse, et ce de façon indifférenciée, la CJUE a conclu la très longue polémique suscitée par les accords PNR et la directive (UE) 2016/681 et elle a validé le système PNR dans son principe tout en émettant des réserves auxquelles la Cour se rallie.

Ainsi, le juge européen a indiqué un certain nombre de dispositions de l'accord PNR UE-Canada, qui nécessitent une révision afin d'assurer leur conformité avec la Charte des droits fondamentaux. Parmi les points listés, la CJUE estime tout d'abord que les 19 catégories de données qui figurent dans l'accord (les mêmes dans tous les accords PNR ainsi que dans la directive européenne) devraient être définies de manière claire et précise et des termes comme «*toutes les coordonnées disponibles* » ou «*remarques générales*» sont à exclure dès lors qu'ils ne fixent aucune limitation quant à l'étendue et à la nature des informations susceptibles d'y figurer. La CJUE exclut par ailleurs le transfert de données sensibles (celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou concernant l'état de santé ou la vie sexuelle d'une personne), comme étant contraire à la Charte des droits fondamentaux.

La CJUE relève encore que les autorités devront produire des « *modèles et critères préétablis (...) spécifiques et fiables* » de sorte à aboutir à des «*résultats ciblant les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou de criminalité transnationale grave*» Les avancées technologiques devront être un outil au service de la société et non un prétexte à instituer des politiques ultra-sécuritaires violant les droits fondamentaux.

S'agissant de la conservation des données, la CJUE relève que la conservation dans le pays destinataire doit être limité au strict nécessaire après le départ du passager, mais la durée de cinq ans prévue par la directive (UE) 2016/681 et reprise par le projet de loi sous avis ne semble pas « *excéder les limites de ce qui est strictement nécessaire à des fins de lutte contre le terrorisme et la criminalité transnationale grave* ».

Quant au possible transfert de données PNR vers un pays tiers, la CJUE ne l'admet que si la Commission a constaté l'existence d'un « *niveau adéquat* » de protection dans le pays destinataire (art. 25, paragraphe 6 de la directive 95/46), ou « *substantiellement équivalent* » à celui assuré au sein de l'UE.

Quant au contrôle du respect des exigences de la protection des données par le biais d'une autorité indépendante, exigence figurant tant dans la Charte (art. 8, paragraphe 3) que dans le Traité (Article 16, paragraphe 2 TFUE), seule une « *autorité publique indépendante* » présente les qualités requises et la CJUE n'admet pas d'autres termes pour définir l'autorité visée.

Quant au projet de loi sous avis, le chapitre 1er relatif aux dispositions générales définit la finalité de la collecte des données des passagers limitée au transport aérien, finalité consistant dans la prévention, la recherche, la constatation et la poursuite des infractions terroristes et des formes graves de criminalité. Or, si la finalité première de la collecte des données personnelles de passagers aériens est de nature commerciale, le projet de loi sous avis concerne les autorités chargées de la prévention et de la répression du terrorisme et de la criminalité grave.

S'agissant des données (au nombre de 19) à recueillir, elles sont définies à l'annexe I du projet de loi et constituent la reprise textuelle de l'annexe I de la directive (UE) 2016/681, sauf que la numérotation du projet de loi sous avis est constituée par les lettres de l'alphabet dans le projet de loi sous avis et par des chiffres dans la directive.

S'agissant des formes de criminalité grave, il s'agit de 26 infractions faisant l'objet de l'annexe II du projet de loi reprises textuellement de l'annexe II de la directive, infractions qui doivent en outre être sanctionnées d'une peine privative de liberté d'un maximum d'au moins trois ans. La première infraction libellée est la « *participation à une organisation criminelle* » et l'on peut se poser la question si cette infraction inclut l'association de malfaiteurs du titre VI chapitre Ier de notre Code pénal.

Le chapitre 2 du projet de loi sous avis traite de l'Unité d'information passagers (UIP) que chaque Etat membre est obligé d'instituer. Or, selon le projet de loi c'est la Police grand-ducale qui composera cette UIP avec comme personnel détaché possible des membres de l'Administration des Douanes et Accises ou du Service de renseignement de l'Etat. Etant donné que les autorités de poursuite judiciaires sont également compétentes en la matière, il serait opportun de prévoir la possibilité d'un détachement d'un membre des Parquets ou du Parquet général afin d'assurer une meilleure liaison à ce niveau.

Le chapitre 3 du projet de loi traite de la transmission des données PNR par les entreprises de transport aérien à l'UIP prévoyant la méthode de transmission, les délais et le procédé technique. Quant à la méthode à employer dite «push», l'exposé de motifs explique qu'il s'agit de la méthode la plus protectrice des données personnelles alors qu'il s'agit de la transmission par les entreprises de transport de leurs données aux Etats membres ce qui leur permet de garder le contrôle de ces données, la méthode alternative étant la méthode dite «pull» consistant dans l'accès aux données des entreprises de transport par les Etats membres. Il serait opportun de préciser la méthode visée afin de ne pas laisser de doute à ce sujet (article 5 du projet). Quant aux délais dans lesquels les données doivent être transmises, le projet de loi est plus strict que la directive en ce qu'il prévoit deux transmissions, la première transmission devant se faire 48 heures avant le départ et la seconde 24 avant le départ, tandis que la directive ne prévoit qu'une communication de 24 à 48 heures avant l'heure du départ programmé (article 6 du projet).

Le chapitre 4 concerne le traitement des données à caractère personnel en interdisant tout traitement des données personnelles révélant l'origine raciale ou ethnique de la personne, ses opinions politiques, sa religion, ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie ou son orientation sexuelles et en imposant l'effacement de toutes informations complémentaires à celles prévues à l'annexe I du projet de loi. Les articles 10,11 et 12 prévoient les différentes manières dont les données PNR peuvent être utilisées, ainsi que leur évaluation et il faut observer d'abord que la notion de « services compétents » apparaît pour la première fois dans ce chapitre, la notion de services étant traitée plus amplement au chapitre 5 dudit projet. Or, dans les autres projets de loi, précités et dans les directives, il est toujours question des *autorités compétentes* et il y aurait lieu de préciser la notion de service compétent à l'article 2 du projet sous avis relatif aux définitions. En outre, le texte de l'article 13 n'est pas très clair en ce qu'il semble limiter la transmission des données PNR aux autorités judiciaires seulement selon les règles du code de procédure pénale et non en vertu du projet de loi sous avis. Enfin, si le fait de limiter la demande et la réception des données au seul cadre de prévention et de détection des infractions visées par la loi s'inscrit dans les principes prévalant en matière de protection des données à caractère personnel, il y a lieu d'observer que les termes de « *dans la limite du besoin d'en connaître* » sont imprécis et risquent de donner lieu à des interprétations diverses.

Le chapitre 6 vise l'échange d'informations entre Etats membres de l'Union européenne et entre les UIP des Etats membres et les articles 16 et 17 sont parmi les éléments-clé du système PNR européen dès lors qu'ils règlent les transmissions d'office et sur demande des informations PNR au sein de l'Union européenne.

La question se pose cependant s'il n'est pas opportun d'ajouter une référence à l'application des dispositions nationales et internationales en matière d'entraide et de coopération judiciaire qui risquent de se voir en concours avec les dispositions du projet de loi sous avis. La même remarque vaut pour le chapitre 8 relatif au transfert des données PNR à des pays tiers.

Le chapitre 7 relatif aux conditions d'accès aux données PNR par Europol n'appelle pas d'observation de la part de la Cour.

Le chapitre 9 relatif à la durée de conservation et à la dépersonnalisation des données constitue la transposition de l'article 12, paragraphes 1 et 4 de la directive (UE) 2016/681 et la durée de cinq ans a été approuvée par la CJUE.

Quant au chapitre 10, il faut observer ici que c'est l'autorité de contrôle judiciaire qui reçoit compétence pour toiser les réclamations tombant sous l'application des articles 1er et 2 de la loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, tandis que la Commission Nationale de Protection des données (CNDP) reste compétente pour toiser les réclamations tombant sous le champ d'application du règlement (UE) 2016/679. Or, cette dualité de compétences peut comporter un risque de conflits.

Quant aux recours juridictionnels applicables en vertu de la loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale auxquels l'article 31 (2) du projet sous avis se réfère, ils constituent une garantie adéquate et suffisante.

S'agissant du chapitre 11 relatif aux sanctions, les notions «*effets juridiques préjudiciables*» ou d'«*affectation significative*» de l'article 15 et de «*risque élevé*» de l'article 36 du projet de loi sous avis sont des notions d'un contour plutôt flou.

La cessation du traitement contraire aux dispositions en cause pourrait être obligatoire.

S'agissant du recours juridictionnel contre la décision du Ministre prononçant une amende administrative contre l'entreprise de transport dans le cadre de l'article 38, il y a lieu de préciser que le recours en question a lieu devant les juridictions administratives (y compris, en cas d'appel, la Cour administrative) selon les règles de procédure et de délais applicables devant elles.

Luxembourg, le 20 novembre 2017

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/04

N° 7151[4]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

AVIS DE LA CHAMBRE DE COMMERCE

(13.12.2017)

Le projet de loi sous avis a pour objet de transposer en droit luxembourgeois la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (Passenger Name Records, ci-après « 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 (ci-après « Directive 2016/681 »).

Les données visées sont les informations – non vérifiées – transmises par les passagers aux transporteurs aériens qui les conservent pour leur usage commercial dans leur système de réservation et de contrôle des départs. Au titre du projet de loi sous avis, 18 catégories de données PNR ont vocation à être collectées et traitées.[1] Elles sont de 2 types :

– les données collectées par les compagnies de transport aérien à des fins commerciales et dont l'analyse peut permettre de mettre en évidence des profils en lien avec diverses formes de criminalité grave[2] qui n'auraient pas nécessairement été connus des autorités en amont. Ces données regroupent principalement les informations relatives au voyage entrepris par le passager, la date de réservation ou d'émission du billet, le mode de paiement utilisé, les dates de voyage, les adresses postale et/ou électronique du passager, son nom, son itinéraire complet, ou encore le poids et le nombre de bagages ;
– les informations préalables recueillies sur les passagers (Advanced Passenger Information, ci-après « API »), qui correspondent principalement aux informations contenues dans le document d'identité fourni par le passager.

L'enjeu de la Directive 2016/681 est de mettre en place entre Etats membres de l'Union européenne (ci-après « UE ») un système harmonisé de collecte, d'utilisation et de conservation les données PNR tout en garantissant le respect des droits fondamentaux, au nombre desquels la protection des données à caractère personnel.

Ce système repose sur la création dans chaque Etat membre d'une unité centrale nationale appelée « *Unité d'Information Passagers* » (ci-après « UIP ») chargée d'analyser les données PNR transférées par les transporteurs aériens et d'assurer la coordination des procédures et le transfert des informations entre les UIP des différents Etats membres, les autorités nationales – en particulier répressives – Europol, ainsi qu'à destination de pays non-membres de l'UE, dans les cas où le traitement des données

1 Les données PNR visées sont référencées à l'annexe 1 du projet de loi sous avis qui transpose à l'identique l'annexe I de la Directive 2016/681.

2 Une liste de 26 infractions est dressée à l'annexe II de la Directive 2016/681, transposée à l'identique dans le projet de loi sous avis. Elle vise, entre autres, le trafic de stupéfiants, la traite des êtres humains, le terrorisme, la corruption, les enlèvements, etc.

PNR s'avérerait positif.[3] Le projet de loi sous avis prévoit que l'UIP luxembourgeoise sera constituée au sein de la Police grand-ducale.

Dans un contexte de multiplication des attentats sur le sol européen, les Etats membres se sont engagés collectivement, par l'intermédiaire d'une déclaration du Conseil de l'UE, à appliquer ce système de collecte et de traitement des données PNR non seulement aux vols en provenance ou à destination d'Etats tiers (hors UE) mais aussi à tous les vols intra-UE.[4] Ce choix est entériné dans le projet de loi sous avis.

Enjeu majeur des négociations entre la Commission européenne, le Conseil et le Parlement européen, l'adoption de la réglementation nécessaire à la mise en place du système de traitement des données PNR a été subordonnée à l'insertion dans le dispositif de garanties de protection strictes des données à caractère personnel traitées.[5]

Ces garanties consistent notamment à imposer des conditions limitatives d'accès et/ou de transfert des données PNR aux différentes autorités nationales, européennes ou extra-européennes visées par le projet de loi, à limiter la conservation des données PNR à une durée maximale de 5 ans à compter du transfert par le transporteur aérien, à imposer une obligation de dépersonnalisation de ces données à l'expiration d'une période de 6 mois à compter dudit transfert, ou encore à désigner un délégué à la protection des données chargé de contrôler le traitement des données PNR.

*

RESUME SYNTHETIQUE

Incertitudes quant au contenu et aux modalités de l'obligation de transfert des données PNR par les transporteurs aériens

Le transfert des données PNR par les transporteurs aériens est à la base du système de traitement des données PNR mis en place par le projet de loi sous avis. Soucieuse que cette obligation n'engendre pas d'incertitude juridique pour les transporteurs aériens, la Chambre de Commerce souhaite mettre en évidence plusieurs points sur lesquels il lui semble particulièrement important de faire évoluer le projet de loi sous avis.

Tout d'abord, la Chambre de Commerce regrette que l'article 5 du projet de loi sous avis ne reflète pas de manière suffisamment explicite le principe fondamental du système mis en place en vertu duquel les données PNR visées par l'obligation de transfert sont exclusivement les données recueillies par les transporteurs dans le cours normal de leurs activités de transport aérien au jour du transfert.

Elle constate ensuite que l'obligation systématique de transfert des données d'un vol par le transporteur aérien devrait être destiné aux UIP de chaque Etat membre sur le territoire duquel le vol décollera ou atterrira, et non pas uniquement à l'UIP luxembourgeoise, comme le prévoit le projet de

---

3 L'évaluation des risques liés aux passagers est réalisée par l'UIP qui reçoit des données PNR de la part d'un transporteur aérien concernant un vol décollant ou atterrissant sur le territoire de son Etat. Cette évaluation d'effectue de deux façons : (i) par la mise en corrélation des données PNR avec les données figurant dans les banques de données pertinentes nationales et internationales afin de déceler des personnes déjà connues des services compétents, ainsi que (ii) par la comparaison des données PNR par rapport à des critères préétablis afin d'identifier des personnes auparavant inconnues dont l'analyse des données indique qu'elles devraient être soumises à un examen plus approfondi par les autorités compétentes. Toute correspondance positive obtenue par des moyens automatisés fait l'objet d'un réexamen individuel par une personne physique avant d'être transférée par l'UIP vers tout autre service ou autorité compétent.

Outre le transfert d'informations entre Etats membres de l'Union européenne, le projet de loi contient des dispositions spécifiques relatives à l'accès aux données PNR par Europol (article 20), et au transfert de données vers des pays non membres de l'UE (articles 21 à 24).

4 La Directive 2016/681 impose aux Etats membres l'application du système de collecte et de traitement des données PNR aux vols en provenance et à destination des Etats tiers. L'extension de ce système aux vols intra-UE est une simple possibilité laissée aux Etats membres qui se sont cependant engagés à la transposer de manière collective. Cet engagement découle de la Déclaration du Conseil n°7829/16 ADD 1, dossier 2011/0023 (COD) du 18 avril 2016.

5 Communiqué de presse du Parlement européen du 10 décembre 2015, disponible en ligne : http://www.europarl.europa.eu/news/fr/press-room/201512071PRO6435/pnr-la-commission-des-libertes-civiles-soutient-l-accord-parlement-conseil.

L'intégralité de la procédure législative est disponible en ligne : http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lano=fr&reference=2011/0023(COD). Les blocages survenus au cours de la procédure ont été largement relayés dans les médias. Cf notamment les articles : « *Speicherung von Fluggastdaten gebremst* » (Tageblatt, 24 avril 2013), et « *Le Parlement européen bloque toujours sur le PNR* » (www euractiv.fr, 9 mars 2016).

loi sous avis. De manière plus générale, la Chambre de Commerce s'interroge quant aux limites du système envisagé au sein duquel le traitement des données PNR sera, selon sa compréhension, limité à un contrôle national, transmis aux autres autorités compétentes uniquement en cas de correspondance positive.

La Chambre de Commerce suggère également de limiter les transferts de données PNR à deux par vol, conformément aux obligations imposées par la Directive 2016/681.

La Chambre de Commerce s'interroge ensuite sur la signification exacte de deux dispositions spécifiques du projet de loi, à savoir la notion de transfert des données PNR « *par tout autre moyen approprié* » en cas de défaillance technique (article 7, paragraphe 2), ainsi que la notion de données correspondant aux « informations grands voyageurs » (annexe 1, point h).

Quant à la communication de données entre UIP en cas d'identification

La Chambre de Commerce suggère que l'article 16 du projet de loi sous avis soit modifié afin que, en cas d'identification d'une personne sur base du traitement de ses données PNR, la communication de données soit adressée aux UIP de tous les Etats membres de l'UE, et non pas seulement aux UIP des Etats membres concernés.

Quant au régime de sanctions

Au vu de la vocation générale du projet de loi n°7168 relative à la protection des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale,[6] la Chambre de Commerce regrette que la formulation de l'article 37 du projet sous avis concernant les sanctions des violations de certaines dispositions visant la protection des données personnelles dans le domaine précis de la sécurité nationale laisse planer un doute quant à la volonté ou non des auteurs d'instaurer d'ores et déjà des exceptions à la loi générale. La Chambre de Commerce s'interroge sur l'opportunité d'adopter un texte de nature à porter atteinte à un régime de protection unifié et cohérent tel qu'il a vocation à être régi par le projet de loi n°7168. La Chambre de Commerce s'interroge également quant à la légalité de certaines peines visées par le projet d'article 37 *in fine*.

La Chambre de Commerce dénonce enfin le caractère manifestement disproportionné de l'amende pouvant aller jusqu'à 50.000 € par vol pour lequel un transporteur aérien ne remplirait pas son obligation de transfert de données PNR.

Des propositions de modifications sont par conséquent intégrées dans le corps du présent avis.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi sous rubrique sous réserve de la prise en compte des commentaires formulés dans le présent avis.

Appréciation du projet de loi :

Compétitivité de l'économie luxembourgeoise	n.a.
Impact financier sur les entreprises	-
Transposition de la directive	+
Simplification administrative	-
Impact sur les finances publiques	-[7]
Développement durable	+

6 Le projet de loi n°7168 a été déposé à la Chambre des députés le 10 août 2017. Il est avisé en parallèle par la Chambre de Commerce.

7 La Chambre de Commerce constate que l'imprécision des postes référencés dans la fiche financière ne lui permet pas de se prononcer sur les coûts réels de mise en place et de fonctionnement du système de traitement des données PNR pour l'Etat.

Légende :	++	:	très favorable
	+	:	favorable
	0	:	neutre
	-	:	défavorable
	--	:	très défavorable
	n.a.	:	non applicable

*

CONSIDERATIONS GENERALES

La Chambre de Commerce note que plusieurs dispositions du projet de loi sous avis[8] mentionnent « *la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale* »[9] (ci-après « projet de loi n°7168 »).

L'article 37, paragraphe 2 du projet de loi sous avis, qui porte sur les sanctions pénales en matière de traitement des données personnelles, se réfère expressément aux sanctions prévues à l'article 49 du projet de loi n°7168, dont le paragraphe 3 fait lui-même référence à la « *loi du jj/mm/aaaa portant création de la Commission nationale pour la protection des données et au régime général sur la protection des données*. » (ci-après « projet de loi n°7184 »).[10]

Aucun de ces deux projets de loi n'ayant encore été adopté, la Chambre de Commerce – qui les avise en parallèle au présent avis – attire l'attention du législateur sur la nécessité de coordonner l'entrée en vigueur du projet de loi sous avis avec les deux autres projets de loi auxquels il fait référence.

La Chambre de Commerce note ensuite une incertitude au niveau de la dénomination de l' « *UIP* » dans le texte du projet de loi sous avis. Elle est qualifiée d' « *Unité d'information passagers* » aux articles 2, point g), dans l'intitulé du chapitre 2, et à l'article 3, point c), alors que l'article 3 mentionne une « *Unité d'informations passagers* ».

A cet égard, la Chambre de Commerce note que la version française de la Directive 2016/681 utilise les deux formes, mais que les versions espagnole et italienne utilisent la dénomination au singulier.[11] La Chambre de Commerce suggère que ces occurrences soient uniformisées dans le projet de loi sous avis.

Quant aux implications financières de l'adoption du projet de loi sous avis, la Chambre de Commerce regrette que la mise en place du système de transfert des données PNR entraîne des coûts supplémentaires à charges des opérateurs du secteur.

En ce qui concerne l'impact du projet de loi sous avis sur les finances de l'Etat, la Chambre de Commerce regrette que la fiche financière ne contienne aucune donnée précise concernant la mise en place effective du système de traitement des données PNR. Elle constate tout particulièrement que l'imprécision des postes référencés dans la fiche financière ne lui permet pas de se prononcer sur les

8 Il s'agit notamment des articles 21, 28, 31 et 33 du projet de loi sous avis.

9 Projet de loi n°7168 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, qui transpose en droit national la directive (UE) n°2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

10 Projet de loi n°7184 portant création de la Commission nationale pour la protection des données et la mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

11 Les versions espagnole « *Unidad de Información sobre los Pasajeros* » et italienne « *Unitá d'informazione sui passeggeri* » utilisent la formule au singulier.

coûts réels de mise en place et de fonctionnement du système de traitement des données PNR pour l'Etat.

*

COMMENTAIRE DES ARTICLES

Concernant l'article 5

L'article 5 du projet de loi sous avis impose aux transporteurs aériens une obligation de transfert des données PNR de tous les vols à destination et en provenance du Luxembourg.

Avant tout, la Chambre de Commerce salue le choix des rédacteurs du projet de loi sous avis de s'en tenir dans un premier temps à imposer le système de collecte de données PNR aux seuls transporteurs aériens et elle prend bonne note de leur intention d'initier une réflexion sur l'extension de ce système à d'autres opérateurs économiques tels que les agents de voyages ou encore les opérateurs de voyages.

La Chambre de Commerce note également que, comme l'indiquent les rédacteurs du projet de loi sous avis dans leur commentaire, l'article 5 n'a pas pour objectif d'imposer aux transporteurs aériens de recueillir des données supplémentaires auprès des passagers, mais bien uniquement de se limiter aux données qu'ils recueillent et traitent déjà pour leur propre usage commercial.

A cet égard, la Directive 2016/681 prévoit que : *« les transporteurs aériens transfèrent […] les données PNR […] pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités, vers la base de données de l'UIP […]. »*[12]

Cependant, l'article sous avis fait simplement référence aux données « *dont ils disposent* », terme générique susceptible d'être source d'interprétations divergentes et, par conséquent, d'insécurité juridique.

Fidèle à l'application du principe selon lequel il appartient au législateur de transposer *« toute la directive, rien que la directive »*, la Chambre de Commerce invite les auteurs à compléter comme suit l'article 5 du projet de loi sous avis afin de ne pas simplifier à outrance le texte de base et d'assurer la sécurité juridique du système mis en place :

*« **Art. 5.** […] les transporteurs aériens transfèrent […], les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg* ***pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien*** ~~***dont ils disposent***~~ *».*

La Chambre de Commerce s'interroge également sur la conformité du système mis en place par le projet de loi sous avis concernant sur la détermination des UIP réceptrices des données PNR pour chaque vol.

En effet, alors que la Directive 2016/681 prévoit l'information des UIP de chaque Etat membre sur le territoire duquel le vol décollera ou atterrira,[13] le projet de loi sous avis prévoit le transfert des données à la seule UIP luxembourgeoise.

Dans ces conditions, la Chambre de Commerce s'interroge sur l'étendue exacte des obligations pesant sur les transporteurs aériens et suggère de compléter l'article 5 du projet de loi sous avis en conséquence :

*« **Art. 5.** Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent* ~~***à l'***~~ ***aux*** *UIP* ***des Etat membres sur le territoire desquels le vol décollera ou atterrira****, par la méthode push, les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg* ***pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien*** ~~***dont ils disposent***~~ *».*

---

12 Article 8, paragraphe 1 de la Directive 2016/681.

13 L'article 8, paragraphe 1er de la Directive 2016/681 prévoit que « […] *Lorsqu'un vol extra-UE comporte une ou plusieurs escales dans des aéroports des Etats membres, les transporteurs aériens transfèrent les données PNR de tous les passagers aux UIP de tous les Etats membres concernés. Il en est de même lorsqu'un vol intra-UE comporte une ou plusieurs escales dans les aéroports de différents Etats membres […]* ».

Concernant l'article 6

L'article 6 du projet de loi sous avis détermine les échéances auxquelles les transporteurs aériens ont l'obligation de transférer les données PNR.

Alors que l'article 8, paragraphe 3 de la Directive 2016/681 prévoit que « *Les transporteurs aériens transfèrent les données PNR […] a) 24 à 48 heures avant l'heure de départ programmée du vol ; et b) immédiatement après la clôture du vol […].* », le projet de loi sous avis prévoit d'imposer aux transporteurs non pas 2 mais 3 transferts de données par vol, à savoir : 48 heures avant le départ, 24 heures avant le départ, et immédiatement après la clôture du vol.

Afin de s'en tenir aux obligations fixées par la Directive 2016/681, la Chambre de Commerce suggère que le projet de loi sous avis soit modifié comme suit :

« (1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes :

a) 24 à** 48 heures avant l'heure de départ programmée du vol**, et

~~***b) 24 heures avant l'heure de départ programmée du vol***~~

~~***c)***~~ ***b)** immédiatement après la clôture du vol »*

Concernant l'article 7, paragraphe 2

L'article 7 du projet de loi sous avis définit techniquement la méthode de transfert des données PNR entre transporteurs aériens et UIP. En vertu de cet article, les données sont transférées par voie électronique au moyen de protocoles communs et de formats de données reconnus.[14] En cas de défaillance technique, le paragraphe 2 de l'article 7 sous avis prévoit que le transfert des données peut être effectué « *par tout autre moyen approprié* ».

En l'absence d'explication de la part des rédacteurs du projet de loi sous avis, la Chambre de Commerce s'interroge sur le contenu de la notion de transfert « *par tout autre moyen approprié* » et invite le législateur à compléter l'article sous analyse afin d'assurer une meilleure sécurité juridique aux opérateurs concernés.

Concernant l'article 16

L'article 16 du projet de loi sous avis prévoit la procédure à suivre par l'UIP luxembourgeoise dans le cas où, suite à la communication de données PNR par une compagnie aérienne, le traitement des données se serait révélé positif concernant un passager.[15] Ce projet d'article impose la communication par l'UIP luxembourgeoise des données pertinentes d'une personne identifiée aux UIP d'autres Etats membres de l'UE.[16]

La Chambre de Commerce constate que le projet de loi sous avis prévoit une information « *aux UIP des autres Etats membres de l'Union européenne concernés*. », alors que la Directive 2016/681 prévoit une information plus générale « *aux UIP correspondantes des autres Etats membres*. »[17]

Une telle restriction ne semble correspondre ni à la lettre, ni à l'esprit de la Directive 2016/681 en vertu de laquelle « *Les Etats membres devraient échanger entre eux et avec Europol les données PNR qu'ils reçoivent, lorsque cela est jugé nécessaire […]. Les UIP devraient, le cas échéant, transmettre sans tarder le résultat du traitement des données PNR aux UIP des autres Etats membres en vue d'un complément d'enquête*. »[18]

La Chambre de Commerce suggère que l'article 16 du projet de loi sous avis soit modifié comme suit : « *[…] l'UIP communique toutes les données pertinentes et nécessaires* […] *aux UIP des autres Etats membres de l'Union européenne* ~~***concernés***~~. »

---

14 Les protocoles communs et formats de données reconnus font notamment l'objet d'une Décision d'exécution (UE) 2017/759 de la Commission du 28 avril 2017 sur les protocoles communs et formats de données devant être utilisés par les transporteurs aériens lors d'un transfert de données PNR aux unités d'information passagers.

15 Cf supra, note 3.

16 La communication des données PNR aux autorités d'Etats tiers est quant à elle soumise à des conditions particulières régies par le chapitre 8 intitulé « *Transfert de données Vers des pays non membres de l'Union européenne* » (articles 21 et suivants du projet de loi).

17 Article 9, paragraphe 1 de la Directive 2016/681.

18 Directive 2016/681, considérant 23.

Concernant l'article 37

L'article 37 du projet de loi sous avis prévoit les sanctions pénales applicables en cas de violation des dispositions relatives à la protection des données personnelles :

« **Art. 37.** *La violation des articles 8, 15 et 36 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. […]*

Pour le surplus, les dispositions de l'article 49, paragraphe 1er et paragraphes 3 à 5 du projet de loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère ».[19]

La Chambre de Commerce souhaite tout d'abord apporter une précision quant à l'utilisation, dans le commentaire de l'article sous analyse, de références au projet de loi n°7168 et à son contenu. De telles références sont effectuées dans le seul but d'articuler les dispositions de ces deux projets de loi, sous toute réserve de modification du projet n°7168.[20]

Quant à la forme tout d'abord, la Chambre de Commerce suggère que le terme « *projet de loi* » utilisé à l'article 37, paragraphe 2 soit remplacé par « *loi* ».

Quant à l'articulation entre le projet d'article 37 et le projet de loi n°7168

Quant au fond, la Chambre de Commerce constate que le traitement des données personnelles en matière pénale ainsi qu'en matière de sécurité nationale constitue l'objet même du projet de loi n°7168 visé à l'article sous analyse.[21]

Selon les rédacteurs du projet de loi sous avis, les comportements visés au paragraphe 1er de l'article sous analyse sont identiques à ceux visés par le projet de loi n°7168.[22] En effet, la Chambre de Commerce constate que les comportements visés aux article 8, 15 et 36 du projet de loi sous avis (paragraphe 1er) constituent une reformulation pour ainsi dire « simplifiée » des comportements visés par les articles 10, 11 et 30, tous trois visés à l'article 49, paragraphe 2 du projet de loi n°7168.

La Chambre de Commerce s'interroge dès lors quant à l'articulation des différentes dispositions et précise que le présent commentaire est formulé à la condition expresse que le projet de loi n°7168 entre en vigueur au plus tard le même jour que le projet de loi sous avis. En effet, l'intention de la Chambre de Commerce n'est aucunement de s'opposer à la pénalisation des comportements visés au projet d'article 37 sous analyse, mais bien de s'assurer de leur applicabilité.

Quant à la légalité des peines prévues au projet d'article 37, in fine

La Chambre de Commerce s'interroge également quant au respect du principe de légalité des peines de la disposition sous analyse en ce qu'elle vise à sanctionner non seulement « *les violations des règles relatives à la protection des données établies par la présente loi* », mais également « *par les lois auxquelles elle se réfère* ».

En effet, le principe de la spécification, qui est le corollaire du principe de légalité, exige que les infractions soient définies en termes suffisamment clairs et que le degré de répression soit précisé pour en exclure l'arbitraire.[23] Or, la violation de règles édictées par d'autres textes de loi, sans même que ceux-ci soient nommément cités est contraire au principe de légalité des peines.

Dès lors, dans un souci de mise en place d'un système juridique cohérent et en l'absence de dispositions spéciales relatives au mécanisme de traitement des données PNR instauré par le projet sous avis par rapport aux sanctions prévues de manière générale en matière pénale et de sécurité nationale dans le projet de loi n°7168, la Chambre de Commerce suggère que l'article 37 soit modifié comme suit :

---

19 Projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. Cf. supra, note 9.

20 La Chambre de Commerce ayant également été saisie pour avis du projet de loi n°7168, celui-ci fera l'objet d'un avis séparé.

21 Cf. commentaire de l'article 1er du projet de loi n°7168 qui qualifie ce projet de loi spéciale en matière de traitement des données personnelles en matière pénale ainsi qu'en matière de sécurité nationale.

22 Cf. commentaire des articles, p. 35.

23 Marc Besch, Traité de légistique formelle, 2005, p.69.

« ***Art. 37.*** *~~Les violations des articles 8, 15 et 36 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. Le juridiction saisie […]~~*

*~~Pour le surplus, l~~**Les** dispositions de l'article 49, ~~paragraphe 1er et paragraphes 3 à 5~~* ***paragraphes 1 à 5*** *~~du projet~~ de* ***la*** *loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi ~~et par les lois auxquelles elle se réfère~~* ».

Quant à l'insécurité juridique engendrée par la pénalisation des violations au projet d'article 8

Par ailleurs, dans l'hypothèse où la formulation actuelle de l'article sous avis serait maintenue, la Chambre de Commerce relève une difficulté d'application de l'article 37, paragraphe 1er du projet de loi sous avis concernant la violation de l'article 8.

En effet, l'article 8 du projet de loi sous avis est rédigé comme suit :

« *Le traitement de données PNR qui révèlent 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 est interdit.*

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive. »

La Chambre de Commerce constate que la formulation de l'article précité ne permet pas de déterminer avec précision quel comportement est sanctionné d'une peine pouvant aller de 8 jours à 1 an d'emprisonnement et une amende pouvant aller de 251 à 125.000 €. Il y aurait lieu de clarifier le projet de loi sur ce point.

Concernant l'article 38

L'article 38 du projet de loi sous avis fixe une amende d'un montant maximum de 50.000 € à raison de chaque vol pour lequel un transporteur aérien ne remplirait pas son obligation de communication des données PNR.

Quant au fond, les rédacteurs du projet de loi sous avis justifient la proportionnalité de la sanction en se référant au contenu des textes français, allemand et belge. Or, contrairement au projet de loi sous avis, les textes français et belge couvrant la matière de la Directive 2016/681 assortissent tous deux cette sanction d'un délai de prescription réduit à un an afin d'assurer une certaine sécurité juridique aux transporteurs aériens en contrepartie de la sévérité de la sanction imposée.[24]

De plus, la Chambre de Commerce note l'existence d'une disposition visant un comportement similaire dans la loi du 29 août 2008 portant sur la libre circulation des personnes et l'immigration. En vertu de cette loi, sont punissables d'une amende pouvant aller jusqu'à 5.000 € les transporteurs aériens qui ne respectent pas l'obligation de transmettre à la Police grand-ducale les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire du Grand-Duché de Luxembourg en provenance d'un pays non-membre de l'Union européenne.[25]

---

24 En Belgique, l'article 47 de la loi du 25 décembre 2016 relative au traitement des données des passagers est rédigé comme suit : « *Aucune sanction ne peut être infligée à raison de faits remontant à plus d'un an à dater de l'établissement du procès-verbal visé à l'article 46, § 1er* ». La loi luxembourgeoise prévoyant également l'établissement d'un tel procès-verbal par la Police grand-ducale (cf. article 38, paragraphe 2 du projet de loi sous avis), une procédure de ce type serait envisageable. En France, l'article L-232-5, dernier paragraphe du Code de la sécurité intérieure prévoit que « *l'autorité administrative ne peut infliger d'amende à raison de faits remontant à plus d'un an* ». Il y a lieu de préciser que cet article du Code de la sécurité intérieure est antérieur à l'adoption de la Directive 2016/681. Il a été adopté par ordonnance n°2012-351 du 12 mars 2012 dans le cadre de la mise en place, sur base de la proposition de Directive de la Commission européenne, d'un dispositif expérimental national visant au traitement des données API et PNR afin d'améliorer le contrôle aux frontières.

25 L'article 148 de la loi du 29 août 2008 prévoit que : « *Est punie d'une amende d'un montant maximum de 5.000 euros, l'entreprise de transport aérien […], à raison de chaque voyage pour lequel l'entreprise, par faute, n'a pas transmis les renseignements y visés, ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis des renseignements incomplets ou erronés. L'amende est prononcée par le ministre. Le montant est versé au Trésor*. »

La Chambre de Commerce dénonce par conséquent le caractère disproportionné de la sanction de 50.000 € prévue à l'article 38 du projet de loi sous avis et suggère que ce montant soit mis en rapport avec celui de 5.000 € au titre de sanction prévue par la loi du 29 août 2008 actuellement en vigueur.

Quant à la forme, la Chambre de Commerce note que la disposition sous analyse telle que formulée ne permet pas de déterminer avec précision quel comportement est susceptible de faire l'objet d'une amende. Il y aurait lieu de modifier l'article sous analyse comme suit :

« *Est puni d'une amende […] le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements* ~~*y*~~ *visés* ***à l'article 3****, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7* ».

Concernant l'annexe 1

L'annexe 1 intitulée « *Liste des données PNR* » consiste en une liste de 18 catégories de données destinées à être transmises et analysées en application du projet de loi sous avis. Elle reprend la liste annexée à la Directive 2016/681.

Quant à la forme, la Chambre de Commerce relève qu'il y a lieu de modifier le point s) de l'annexe 1 comme suit : « *s) historique complet des modifications des données PNR énumérées aux points* ~~***1 à 18***~~ ***a) à r)***. »

Quant au fond, la Chambre de Commerce s'interroge sur le contenu des informations devant faire l'objet d'un transfert par les transporteurs aériens en relation avec le point *h) Informations « grands voyageurs »*, qui plus est au regard des sanctions projetées.

Etant donné que ni le commentaire des articles du projet de loi sous avis, ni les textes européens ne permettent de comprendre avec précision quelles sont les données visées par cet alinéa, il y aurait lieu de le préciser, si nécessaire par le biais d'exemples ajoutés à la liste des données PNR.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi sous rubrique sous réserve de la prise en compte des commentaires formulés dans le présent avis.

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/05

N° 7151[5]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

SOMMAIRE:

page

Amendements gouvernementaux

1) Dépêche du Ministre aux Relations avec le Parlement au Président de la Chambre des Députés (27.2.2018) 1
2) Texte et commentaire des amendements gouvernementaux 2
3) Texte coordonné 5

*

DEPECHE DU MINISTRE AUX RELATIONS AVEC LE PARLEMENT AU PRESIDENT DE LA CHAMBRE DES DEPUTES

(27.2.2018)

Monsieur le Président,

À la demande du Ministre de la Sécurité intérieure, j'ai l'honneur de vous saisir d'amendements gouvernementaux relatifs au projet de loi sous rubrique.

À cet effet, je joins en annexe le texte des amendements avec un commentaire ainsi qu'une version coordonnée du projet de loi tenant compte desdits amendements.

Veuillez agréer, Monsieur le Président, l'assurance de ma haute considération.

Le Ministre aux Relations avec le Parlement,

Fernand ETGEN

*

TEXTE ET COMMENTAIRE DES AMENDEMENTS GOUVERNEMENTAUX

Le détail et la motivation des amendements adoptés par le Gouvernement se présentent comme suit :

Amendement n° 1

Il est inséré dans le projet de loi un nouveau chapitre 12 libellé comme suit :

« **Chapitre 12 – *Dispositions modificatives*** ».

Commentaire

En raison des deux amendements ayant pour objet d'opérer des modifications à la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, le Gouvernement propose l'insertion d'un nouveau chapitre au projet de loi regroupant l'ensemble des dispositions modificatives.

Amendement n° 2

Il est ajouté un article 39 nouveau au projet de loi libellé comme suit:

« **Art. 39.** Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

« (4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes ou de cyber-menace dans la mesure où elle est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12 de la loi du jj.mm.aaaa relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Le directeur du SRE rapporte tous les six mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en oeuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Commentaire

Contrairement à l'article 10, paragraphe 2, du projet de loi qui vise le traitement des données PNR dans le cadre de l'évaluation préalable des passagers, l'article 10, paragraphe 4, et l'article 12 du projet de loi prévoient le traitement des données PNR de personnes préalablement identifiées ou identifiables dans le cadre de recherches ponctuelles.

Pour l'article 10, paragraphe 4, du projet de loi il s'agit de personnes dont l'analyse des données en vertu de l'article 10, paragraphe 2, permet de conclure à la réalité d'une menace potentielle relevant du champ d'application des missions du SRE de sorte à ce que ce dernier décide de faire des recherches plus approfondies concernant cette personne identifiée sur hase de la loi précitée du 5 juillet 2016.

Pour l'article 12 du projet de loi, il s'agit de personnes cibles du SRE dans le cadre d'opérations existantes et dont l'intérêt du SRE est basé sur des moyens et mesures de recherches différents que l'analyse des données en vertu de l'article 10, paragraphe 2, du projet de loi. Il peut s'agir par exemple d'une personne signalée par un service de renseignement partenaire ou bien d'une personne qui a attiré l'attention du SRE par le biais d'une mesure de surveillance sur base des articles 5 et 7 de la loi précitée du 5 juillet 2016.

Aux termes de l'article 10, paragraphe 4, « *l'UIP transmet aux services compétents, au cas par cas, (...) les données PNR des personnes identifiées* » et l'article 12 autorise les services compétents d'obtenir la communication des données PNR suivant une demande motivée et limitée aux finalités de « *prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité*[1] ».

1 Article 1er du projet de loi.

Etant donné que l'article 13 du projet de loi attribue au SRE la qualité de « *service compétent* », il peut demander la communication des données PNR conformément aux conditions et critères inscrits au projet de loi.

Le deuxième amendement prévoit ainsi les modalités pratiques selon lesquelles le SRE peut demander la communication de données PNR.

Le texte proposé s'inspire de l'article 51 de la loi belge du 25 décembre 2016 relative au traitement des données des passagers, qui insère un nouvel article 16/3 dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité belges.

L'amendement précise plus concrètement les éléments suivants :

– La finalité du traitement

La demande de communication des données PNR en vertu de l'article 10, paragraphe 4, et de l'article 12 du projet de loi est limitée au traitement des données à des fins de prévention en matière de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes ou de cyber-menace dans la mesure où elle est liée aux activités précitées. Il s'agit des quatre missions du SRE inscrites à l'article 3 de la loi précitée du 5 juillet 2016 qui concordent avec les finalités inscrites à l'article 1er du projet de loi.

– La procédure d'autorisation

La procédure d'autorisation inscrite à l'article 5, paragraphe 1er, de la loi précitée du 5 juillet 2016 s'applique à cette mesure de recherche opérationnelle. Par conséquent, la demande de communication se base sur une autorisation écrite préalable du directeur du SRE, suite à une demande motivée de l'agent du SRE chargé des recherches et sous réserve des conditions et critères prévus à l'article 4 de la loi précitée du 5 juillet 2016.

De la même manière que les demandes d'observations, l'autorisation du directeur peut avoir un caractère verbal en cas d'urgence avérée et devra être confirmée par écrit dans un délai de quarante-huit heures.

– Le contrôle

A l'image de la procédure prévue à l'article 5, paragraphe 3, de la loi précitée du 5 juillet 2016 concernant les observations, le directeur du SRE rapporte par écrit au Comité les motifs des consultations effectuées les six derniers mois.

La période de six mois a été fixée par analogie à l'article 24, paragraphe 6, de la loi précitée du 5 juillet 2016 qui prévoit le contrôle des mesures de surveillance et de contrôle des communications par la commission de contrôle parlementaire tous les six mois.

Amendement n° 3

Il est ajouté un article 40 nouveau au projet de loi libellé comme suit:

« **Art. 40.** A l'article 8, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, le point a) est supprimé. »

Commentaire

L'article 8, paragraphe 1er, point a), de la loi précitée du 5 juillet 2016 permet à ce dernier de solliciter les données des dossiers passagers relatives à une ou à plusieurs personnes identifiées ou identifiables afin de pouvoir déterminer, notamment, les déplacements de personnes d'intérêt vers ou en provenance d'une zone de combat ou de crise en matière de lutte contre le terrorisme.

Cette disposition a été créée par la loi précitée du 5 juillet 2016 en attendant l'entrée en vigueur du projet de loi sous examen. En effet, le commentaire de l'article 10, paragraphe 4, point a), du projet de loi n°6675/00 (du 2 avril 2014) référait déjà aux discussions de la directive visant la mise en place d'un système européen de collecte et d'échange de données passagers au sein du Conseil Justice et Affaires Intérieures de l'union européenne.

Sur base de l'article 8, paragraphe 1er point a), de la loi précitée du 5 juillet 2016, le SRE adresse donc actuellement les demandes directement aux transporteurs aériens en vue de se faire confirmer la présence ou non d'une personne identifiée sur un vol déterminé à une date déterminée.

Or, avec l'entrée en vigueur du nouveau projet de loi et notamment ses articles 10 et 12, l'article 8, paragraphe 1er, point a), de la loi précitée du 5 juillet 2016 ne sera plus compatible avec ces nouvelles dispositions et créera non seulement une incohérence textuelle, mais surtout, une insécurité juridique pour le SRE.

Par conséquent, le Gouvernement propose de supprimer le point a) de l'article 8, paragraphe 1er, de la loi précitée du 5 juillet 2016 afin que les articles 10, paragraphe 4, et 12 ainsi que son nouvel article 39 pré-mentionné puissent s'appliquer sans contradictions textuelles avec la loi précitée du 5 juillet 2016.

Les mesures introduites par le projet de loi, en transposant la directive 2016/681, permettent en effet au SRE de combattre plus efficacement les menaces en matière de terrorisme, d'espionnage, de prolifération et de cybercriminalité ainsi que ses nouvelles formes d'expression.

Cette possibilité d'obtenir les données PNR par le biais du nouveau projet de loi est de triple importance pour le SRE.

– D'une part, les données PNR visées par le projet de loi constituent un moyen permettant désormais d'avoir accès à tous les renseignements concernant son voyage, les vols d'aller et de retour, les correspondances éventuelles et les services particuliers souhaités à bord et elles comportent, par exemple, hormis les noms et les dates du voyage, également l'itinéraire, les coordonnées du passager, ses accompagnateurs ou le moyen de paiement utilisé.
– Le SRE pourra également être amené à demander des données PNR d'une personne qui voyage via le Luxembourg sur demande d'un service de renseignement partenaire. Le SRE est obligé dans ce cas à coopérer avec ce service de renseignement partenaire sur hase de l'article 9, paragraphe 4, de la loi précitée du 5 juillet 2016.
– Finalement, les données PNR ne sont plus collectées directement auprès des transporteurs aériens, mais le SRE peut demander la communication auprès de l'UIP qui est en charge « *de la collecte centralisée des données PNR transférées par les transporteurs aériens, ainsi que de la conservation et du traitement de ces données* ».

  Cette mesure permettra dès lors d'accéder aux données de manière plus discrète, d'une part et, plus rapide, d'autre part. La vitesse de réaction est d'autant plus importante en cas d'urgence. Les demandes des services de renseignement étranger se font d'ailleurs le plus souvent dans l'urgence en matière de lutte contre le terrorisme.

  C'est dans ce même contexte que, la demande de communication des données PNR sur base du deuxième amendement est désormais soumise à une autorisation préalable du directeur du SRE, contrairement à la procédure complexe visée à l'article 7, paragraphe 4, de la loi précitée du 5 juillet 2016. Cette procédure d'autorisation permettra au SRE d'agir plus rapidement et ceci notamment dans le cadre de la lutte contre le terrorisme qui nécessite une grande réactivité et une flexibilité accrue. Les demandes demeurent néanmoins soumises à un contrôle du Comité ministériel tous les six mois.

En vue de l'entrée en vigueur de ce projet de loi et suite à l'introduction d'un nouveau paragraphe 4, à l'article 5 de la loi précitée du 5 juillet 2016 par le deuxième amendement, l'article 8, paragraphe 1er, point a), de la loi précitée du 5 juillet 2016 sera partant vidé de sa substance.

Dans un souci de cohérence entre les deux textes et afin que les dispositions de la directive transposée par le projet de loi puissent sortir tous leurs effets, le Gouvernement propose dès lors de supprimer le point a) de l'article 8, paragraphe 1er, de la loi précitée du 5 juillet 2016.

Suite à la suppression du point a) de l'article 8, paragraphe 1er, la numérotation des points subséquents change en conséquence.

*

TEXTE COORDONNE

Chapitre 1er – *Dispositions générales*

Art. 1er. La présente loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Art. 2. Pour l'application de la présente loi, on entend par:

a) „transporteur aérien": toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes;

b) „passager": toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers;

c) „dossier passager": le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités;

d) „système de réservation": le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations;

e) „système de contrôle des départs": le système utilisé pour contrôler les passagers lors de l'embarquement;

f) „données PNR": les données contenues dans le dossier passager et énumérées à l'annexe I;

g) „méthode push": la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'information passagers;

h) „infractions terroristes": les infractions visées au Livre II, Titre 1ier, Chapitre III-1 du Code pénal;

i) „formes graves de criminalité": les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans;

j) „dépersonnaliser par le masquage d'éléments des données": rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée.

Chapitre 2 – *Unité d'information passagers*

Art. 3. Il est créé au sein de la Police grand-ducale une Unité d'informations passagers, ci-après désignée „UIP", qui est chargée:

a) de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données;

b) du transfert de ces données et des résultats de leur traitement aux services compétents;

c) de l'échange de ces données et des résultats de leur traitement avec les unités d'information passagers des autres Etats membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4. Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel détaché de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Art. 5. Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la

méthode push, les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg dont ils disposent.

Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens l'obligation de transférer les données PNR incombe au transporteur aérien qui assure le vol.

Art. 6. (1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes:

a) 48 heures avant l'heure de départ programmée du vol;

b) 24 heures avant l'heure de départ programmée du vol;

c) 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 qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point c), peut se limiter à une mise à jour des transferts visés à l'alinéa 1er, points a) et b).

(2) Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP peut demander, au cas par cas, le transfert de données PNR en dehors des délais prévus au paragraphe 1er.

Art. 7. (1) Les données PNR sont transférées à l'UIP par voie électronique au moyen des protocoles communs et des formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la Directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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. Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg dès leur publication au Journal officiel de l'Union européenne.

Les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisés pour leurs transferts.

(2) En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union européenne en matière de protection des données soit pleinement respecté.

Chapitre 4 – *Traitement des données PNR*

Art. 8. Le traitement de données PNR qui révèlent 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 est interdit.

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive.

Art. 9. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données supplémentaires dès réception et de façon définitive.

Art. 10. (1) L'UIP traite les données PNR en vue de réaliser une évaluation des passagers avant leur arrivée prévue sur le territoire national ou leur départ prévu du territoire national afin d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis compte tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

(2) Pour réaliser cette évaluation l'UIP peut comparer les données PNR:

a) aux banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions;

b) à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les ser-

vices compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur 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.

(3) L'UIP réexamine individuellement, par des moyens non automatisés, toute concordance positive obtenue à la suite d'un traitement automatisé des données PNR effectué en vertu du présent article.

(4) L'UIP transmet aux services compétents, au cas par cas, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au présent article ou le résultat du traitement de ces données.

(5) Les conséquences de l'évaluation des passagers ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union européenne à la libre circulation sur le territoire de Luxembourg tel que prévu par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.

(6) Lorsque les évaluations sont réalisées pour des vols entre le Luxembourg et un autre Etat membre de l'Union européenne auquel s'applique le règlement No 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes, les conséquences de ces évaluations doivent respecter ledit règlement.

Art. 11. L'UIP traite les données PNR afin de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations visées à l'article 10.

Art. 12. L'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, dûment motivées et fondées sur des motifs suffisants visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques aux fins visées à l'article 1er, et visant à communiquer aux services compétents ou, le cas échéant, à Europol, le résultat de ce traitement.

Chapitre 5 – *Services compétents*

Art. 13. Sans préjudice des attributions des autorités judiciaires telles que définies par le Code de procédure pénale, sont habilités à demander et à recevoir des données PNR ou le résultat du traitement de ces données, dans le cadre de leurs attributions légales et dans la limite du besoin d'en connaître:

a) les services de la Police grand-ducale;

b) le Service de Renseignement de l'Etat;

c) les services de l'Administration des Douanes et Accises.

Art. 14. Les services compétents ne peuvent traiter les données PNR et le résultat du traitement de ces données que pour les finalités de la présente loi telles que définies à l'article 1er.

L'alinéa 1er est sans préjudice des compétences de la Police et de l'Administration des Douanes et Accises lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement.

Art. 15. Les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Art. 16. Lorsqu'une personne est identifiée conformément à l'article 10, l'UIP communique toutes les données pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP des autres Etats membres de l'Union européenne concernés.

Lorsque l'UIP est destinataire d'informations telles que visées à l'alinéa 1er de la part d'une autre UIP, elle transmet ces informations aux services compétents.

Art. 17. (1) L'UIP transmet, dès que possible, à l'UIP d'un autre Etat membre de l'Union européenne qui en fait la demande, les données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par masquage conformément à l'article 26, et, si nécessaire, le résultat de tout traitement de ces données, s'il a déjà été réalisé conformément à l'article 10.

La demande, dûment motivée, peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière.

Si les données demandées ont été dépersonnalisées par masquage conformément à l'article 26, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que le transfert est nécessaire aux fins visées à l'article 12 et si elle y est autorisée par le procureur d'Etat de Luxembourg ou son délégué.

(2) Dans des cas d'urgence, les autorités compétentes des autres Etats membres, désignées conformément à l'article 7, paragraphe 1er, de la Directive (UE) 2016/661 du Parlement européen et du Conseil du 27 avril 2016 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 et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe (1) sont applicables.

(3) A titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un Etat membre a le droit de demander à ce que l'UIP obtienne des données PNR conformément à l'article 6, paragraphe (2), et les communique à l'UIP requérante.

Art. 18. L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres Etats membres de l'Union européenne des données PNR ou les résultats du traitement de ces données. Les demandes sont introduites et traitées conformément au droit national de l'Etat membre requis.

Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre Etat membre de l'Union européenne, il transmet copie de sa demande à l'UIP.

Art. 19. L'échange de données effectué en application du présent chapitre peut avoir lieu par l'intermédiaire de tous les canaux de coopération policière existant entre les autorités compétentes des Etats membres de l'Union européenne.

La langue utilisée pour la demande et l'échange des données est celle applicable au canal utilisé.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Art. 20. (1) Dans les limites de ses compétences et pour l'accomplissement de ses missions, Europol peut présenter à l'UIP, au cas par cas, par l'intermédiaire de son unité nationale, une demande électronique dûment motivée visant à obtenir des données PNR spécifiques ou le résultat du traitement de ces données:

a) lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des Etats membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme gave de criminalité spécifique, ou de mener des enquêtes dans la matière et;

b) dans la mesure où ladite infraction relève de la compétence d'Europol.

(2) La demande énonce les motifs sur lesquels s'appuie Europol pour estimer que la transmission de données PNR ou du résultat de traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée ou à des enquêtes en la matière.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Art. 21. Sans préjudice des dispositions de l'article 35, paragraphe (1), point (d), et des articles 36 à 38 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, l'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si:

a) l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité;

b) le transfert est nécessaire aux fins telles que définies à l'article 1er;

c) le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er;

d) les conditions prévues à l'article 17, paragraphe (1) sont remplies.

Art. 22. (1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre Etat membre de l'Union européenne à un pays non membre de l'Union européenne que si l'Etat membre auprès duquel les données ont été collectées a donné son accord au transfert.

(2) Dans des circonstances exceptionnelles, les données PNR peuvent être transférées à un pays non membre de l'Union européenne sans l'accord du pays membre de l'Union européenne auprès duquel les données ont été collectées si les conditions suivantes sont remplies:

a) 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 Etat membre de l'Union européenne ou un pays tiers;

b) l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'Etat membre de l'Union européenne, qui n'a pas pu donner son accord en temps utile, est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

Art. 23. L'UIP ne peut transférer des données PNR et les résultats du traitement de ces données aux autorités compétentes de pays non membres de l'Union européenne que dans les conditions compatibles avec la présente loi et après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte ces conditions et garanties.

Art. 24. Le délégué à la protection des données est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Art. 25. L'UIP conserve les données PNR pendant une durée maximale de cinq ans à compter du transfert par le transporteur aérien.

A l'issue de cette période de cinq ans, elle efface les données PNR de manière définitive. Cette disposition ne s'applique pas si les données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière.

Art. 26. (1) A l'expiration d'une période de six mois à compter du transfert par le transporteur aérien, l'UIP dépersonnalise les données PNR par le masquage des éléments suivants:

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;

b) l'adresse et les coordonnées;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne;

d) les informations „grands voyageurs“;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte;

f) toute donnée API qui a été recueillie.

(2) A l'expiration de la période de six mois visée au paragraphe (1), la communication de l'intégralité des données PNR n'est autorisée que sous les conditions suivantes:

a) elle est nécessaire aux fins visées à l'article 12;

b) elle a été approuvée par le procureur d'Etat de Luxembourg ou son délégué ou, si les données sont destinées à être communiquées au Service de Renseignement de l'Etat, par la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Art. 27. L'UIP ne conserve le résultat de l'évaluation réalisée en vertu de l'article 10 que le temps nécessaire pour informer les services compétents et, s'il y a lieu, les UIP des autres Etats membres de l'Union européenne de l'existence d'une concordance positive.

Lorsque, à la suite du réexamen individuel par des moyens non automatisés conformément à l'article 10, paragraphe (3), le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées en vertu de l'article 25, de manière à éviter de futures „fausses“ concordances positives.

Chapitre 10 – *Protection des données à caractère personnel*

Art. 28. Sans préjudice de l'article 41 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, l'autorité de contrôle instituée par l'article 1er de la loi du jj/mm/aaaa relative à la création de la Commission nationale pour la protection des données et au régime général sur la protection des données est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 10 de la même loi et elle dispose, à cette fin, des pouvoirs prévus à l'article 16 de la même loi.

Art. 29. (1) Le responsable de l'UIP désigne un délégué à la protection des données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

(2) Le délégué à la protection des données contrôle le traitement des données PNR et met en oeuvre les garanties pertinentes au sein de l'UIP.

Il informe et conseille le responsable et le personnel de l'UIP sur les obligations qui leur incombent en matière de protection des données.

Il fait office de point de contact pour les personnes concernées pour toutes les questions relatives au traitement de leurs données PNR et pour la Commission nationale pour la protection des données.

(3) Le délégué à la protection des données effectue ses missions en toute indépendance.

Il fait directement rapport au responsable de l'UIP.

Par dérogation à l'alinéa 2, et sans préjudice du paragraphe (4), alinéa 2, en cas de problèmes relevant de la protection des données, le délégué à la protection des données rapporte directement au Directeur général de la Police ou, s'il juge nécessaire, au Ministre ayant la Police dans ses attributions.

(4) Le délégué à la protection des données a accès à toutes les données traitées par l'UIP.

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données.

Art. 30. L'UIP met à la disposition du public, par les moyens de communication appropriés les informations suivantes:

a) ses coordonnées;

b) les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données PNR;

d) le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité;

e) l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31. (1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 14 à 18 du projet de loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 45 à 48 du projet de loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 32. L'UIP conserve, traite et analyse les données PNR en un ou des endroits sécurisés situés sur le territoire du Luxembourg.

Art. 33. Le responsable de l'UIP met en oeuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et la nature des données PNR.

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en oeuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 29, paragraphe (2) de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 34. L'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

Cette documentation comprend:

a) Le nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès;

b) Les demandes formulées par les services compétents et les UIP des autres Etats membres de l'Union européenne;

c) Toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Art. 35. L'UIP tient des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

Les registres des opérations de consultation et de communication indiquent la finalité, la date et l'heure de l'opération et l'identité de la personne qui a consulté ou communiqué les données PNR ainsi que l'identité des destinataires de ces données.

Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit.

L'UIP met les registres à la disposition de l'autorité de contrôle, à la demande de celle-ci. Les registres sont conservés pendant cinq ans.

Art. 36. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe sans retard injustifié la personne concernée et l'autorité de contrôle de cette atteinte.

Chapitre 11 – *Sanctions*

Art. 37. La violation des articles 8, 15 et 36 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent alinéa sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 49, paragraphe 1er et paragraphes 3 à 5 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38. (1) Est puni d'une amende d'un montant maximum de 50.000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements y visés, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

(2) Le manquement est constaté par un procès-verbal établi par la Police grand-ducale. Copie en est transmise au transporteur aérien.

Le transporteur aérien a accès au dossier et est mis à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction.

L'amende est prononcée par le Ministre ayant la Police dans ses attributions.

(3) La décision du ministre qui est motivée est susceptible d'un recours en réformation à introduire devant le Tribunal administratif dans un délai d'un mois à compter de la notification.

Chapitre 12 – *Dispositions modificatives*

Art. 39. Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

«(4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes ou de cyber-menace dans la mesure où elle est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12 de la loi du jj.mm.aaaa relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Le directeur du SRE rapporte tous les six mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en oeuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Art. 40. A l'article 8, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, le point a) est supprimé.

Impression: CTIE – Division Imprimés et Fournitures de bureau
7151 - Dossier consolidé : 103

7151/06

N° 7151[6]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

AVIS DU CONSEIL D'ETAT

(30.3.2018)

Par dépêche du 20 juin 2017, le Premier ministre, ministre d'État, a soumis à l'avis du Conseil d'État le projet de loi sous rubrique élaboré par le ministre de la Sécurité intérieure.

Au texte du projet de loi étaient joints un exposé des motifs, un commentaire des articles, une fiche d'évaluation d'impact, une fiche financière, le texte de la directive (UE) 2016/681 que le projet de loi est appelé à transposer ainsi qu'un tableau de correspondances entre les dispositions à transposer et les textes y correspondant dans le projet.

Par dépêches respectives des 10 novembre, 15 et 19 décembre 2017, les avis du Parquet général, des Parquets de Luxembourg et de Diekirch, du Tribunal d'arrondissement de Luxembourg, de la Cour supérieure de Justice, ainsi que de la Commission nationale pour la protection des données (ci-après : CNPD) et de la Chambre de commerce ont été transmis au Conseil d'État.

Par dépêche du 27 février 2018, le Premier ministre, ministre d'État, a encore fait parvenir au Conseil d'État trois amendements gouvernementaux au projet sous examen, auxquels étaient joints un commentaire ainsi qu'un texte coordonné du projet de loi sous examen. Par contre, aucune version coordonnée de la disposition que l'amendement est appelé à modifier, à savoir les articles 5 et 8 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État (ci-après : SRE), n'accompagnait ladite dépêche.

*

CONSIDERATIONS GENERALES

Le projet de loi sous examen a, aux termes de l'exposé des motifs, pour objet « de transposer en droit national la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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 des enquêtes et des poursuites en la matière, ci-après la « directive ». Cette directive a été publiée au Journal officiel de l'Union européenne le même jour que le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016[1] relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, plus connue sous la désignation de « règlement général sur la protection des données » ainsi que la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016[2] relative à la protection des données physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites en la matière d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre

1 Voir projet de loi de transposition n°7184.

2 Voir projet de loi de transposition n°7168.

2008/979/JAI du Conseil[3]. Ensemble, ces trois textes forment le paquet « Protection des données personnelles » qui, à dater de leur entrée en vigueur, est appelé à assurer sur tout le territoire de l'Union européenne une protection uniforme des données personnelles.

La directive règle le transfert tant au niveau national qu'au niveau international des données PNR (*Passenger Name Records*) recueillies par les opérateurs de transport de personnes pour leur usage commercial vers une unité dédiée, l'Unité d'information passagers (ci-après : UIP), qui les collecte et les traite à des fins de prévention, de recherche, de constatation et de poursuite d'infractions particulièrement graves, à savoir les infractions terroristes et les infractions ressortissant de certaines formes graves de criminalité. La directive impose encore des règles spécifiques tenant au respect de la vie privée des personnes concernées, notamment pour ce qui est du traitement ultérieur des données transférées ainsi que de leur effacement soit pendant le traitement – s'il s'agit de certaines données spécifiques particulièrement sensibles – soit après celui-ci.

La directive étend ainsi le contenu de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (directive API) qui a été transposée au Luxembourg par la loi du 21 décembre 2006 portant 1. transposition – de la directive 2001/40/CE du Conseil du 28 mai 2001 relative à la reconnaissance mutuelle des décisions d'éloignement des ressortissants de pays tiers ; – de la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 ; – de la directive 2002/90/CE du Conseil du 28 novembre 2002 définissant l'aide à l'entrée, au transit et au séjour irréguliers ; – de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers ; 2. modification de la loi modifiée du 28 mars 1972 concernant 1. l'entrée et le séjour des étrangers ; 2. le contrôle médical des étrangers ; 3. l'emploi de la main-d'œuvre étrangère[4]. En effet, si la directive API visait les renseignements relatifs aux passagers transportés par des entreprises de transport aérien vers un point de passage frontalier en provenance d'un pays non membre de l'Union européenne, la directive PNR, quant à elle, prévoit une possibilité pour les États membres d'étendre cette obligation également aux vols inter-UE. Dans le cadre d'une déclaration commune du 4 décembre 2015, les ministres de la Justice et des Affaires intérieures de l'Union européenne se sont par ailleurs engagés à élargir, dans la mesure du possible, la collecte des données PNR auprès d'autres opérateurs de transport, et notamment les transporteurs ferroviaires et maritimes. Si cette voie a été retenue par les législateurs belge et français, le projet de loi sous examen ne vise que les seuls transports aériens.

Le Conseil d'État n'entend pas réitérer les considérations générales qui figurent déjà tant dans le projet de loi initial que dans la plupart des avis rendus dans le cadre de ce projet de loi. Il procédera par ailleurs à l'analyse des différentes dispositions en projet sans faire une appréciation de la directive elle-même au regard des critères établis dans l'avis 1/15 rendu par la Cour de justice des Communautés européennes en date du 26 juillet 2017 relative à la compatibilité du projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers avec l'article 16 du TFUE et les articles 7, 8 et l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne[5].

Dans le cadre de l'examen des articles du projet, le Conseil d'État a pris connaissance des actes de transposition belge et français, à savoir, pour ce qui est de la Belgique, de la loi du 25 décembre 2016 relative au traitement des données des passagers[6] et, pour ce qui est de la France, de la loi 2017-1510 du 30 octobre 2017[7], qui a introduit dans le code de la sécurité intérieure les dispositions transposant la directive.

Le Conseil d'État procédera d'abord à l'examen des articles du projet de loi initial transmis par la dépêche du 20 juin 2017 pour procéder ensuite à l'examen des amendements transmis en date du 27 février 2018.

---

3 JOUE L 119 du 4 mai 2016.

4 Mémorial A n° 230 du 27 décembre 2006, p. 4101.

5 http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=FR&mode=lst& dir=&occ=first&part=1&cid=886432 (consulté le 1er février 2018).

6 Moniteur belge, p. 12.905, 25 janvier 2017.

7 JORF 2017 du 31 octobre 2017, loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (NOR : *INTX1716370L*).

EXAMEN DES ARTICLES DU PROJET DE LOI INITIAL

Article 1er

L'article 1er, qui transpose l'article 1er de la directive, cadre l'objet du projet de loi sous examen. Dès lors qu'il limite le champ d'application de la loi tant par rapport aux personnes concernées (les transporteurs aériens), que par rapport aux données concernées (les seules données PNR) et enfin par rapport à la finalité du traitement (prévention, recherche, constatation et poursuite des infractions y visées), il dispose d'une valeur normative propre qui, par ailleurs, n'appelle pas d'observation.

La directive, en son article 2, paragraphe 1er, prévoit qu'un État membre peut décider d'appliquer les obligations en découlant également aux vols intra-UE, en notifiant cette décision par écrit à la Commission. Si l'article 1er ne le dit pas expressément, le défaut d'indiquer une limitation du transfert aux données PNR relatives aux seuls vols extra-UE implique nécessairement que les données relatives aux vols intra-UE devront également être communiquées. Il y a dès lors lieu de procéder à la notification de cette décision à la Commission dès l'entrée en vigueur de la loi de transposition.

Article 2

L'article 2 contient un certain nombre de définitions, reprises pour l'essentiel de l'article 3 de la directive. Le Conseil d'État s'interroge sur les raisons qui ont motivé les auteurs à remplacer les chiffres utilisés par la directive par des lettres[8]. Il suggère par ailleurs de compléter la liste des définitions par celle de l'UIP, qui est citée dans le cadre du point g) de l'article sous examen, sans avoir été définie auparavant. Alternativement, le point g) pourrait être complété par les termes « créée à l'article 3 de la présente loi ».

Article 3

L'article 3 met en place au sein de la Police grand-ducale, sous la dénomination « Unité d'information passagers » (UIP), une unité spécialement dédiée à la collecte, à la conservation, au traitement, au transfert et à l'échange des données PNR transmises en application de la loi en projet.

Le choix de la Police grand-ducale en tant qu'administration de rattachement de l'UIP est, en soi, conforme à l'article 4, paragraphe 1er, de la directive qui prévoit que cette entité doit être mise en place auprès « d'une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité ». Il tient également compte de ce que la Police grand-ducale est déjà à l'heure actuelle destinataire des données transférées en vertu de la loi précitée du 21 décembre 2006[9]. Le projet de loi sous avis précise cependant que l'unité nouvellement créée sera composée non seulement de personnel provenant de la Police, mais encore de personnel pouvant être détaché de l'Administration des douanes et accises ainsi que du SRE.

Le Conseil d'État s'interroge sur le statut de ce personnel « détaché » et sur ses compétences. L'article 7 du Statut général des fonctionnaires de l'État définit le détachement comme « l'assignation au fonctionnaire d'un autre emploi correspondant à sa catégorie et à son grade dans une autre administration, dans un établissement public ou auprès d'un organisme international », qui a comme conséquence que « le fonctionnaire relève de l'autorité hiérarchique de l'administration, respectivement de l'établissement ou de l'organisme auquel il est détaché ». En application de cette disposition, les fonctionnaires détachés des deux administrations visées au projet de loi ne feront plus partie de celles-ci, mais relèveront entièrement de la Police grand-ducale. Dès lors, en précisant que les personnes concernées continueront à agir « dans les limites des attributions légales de l'administration dont (elles) relève(nt) » le projet de loi sous examen est en contradiction avec la disposition précitée du Statut général, de telle sorte que le Conseil d'État doit s'y opposer formellement pour incohérence et, partant, insécurité juridique.

Par ailleurs, le Conseil d'État souligne que, une fois détachées à l'UIP, les personnes concernées ne sont plus en droit d'accéder aux données et informations traitées dans leur service d'origine sur base de leur première affectation, étant donné qu'en vertu de leur détachement ils n'en font plus partie, sauf

---

8 La même question est d'ailleurs permise par rapport aux deux annexes qui figurent au projet sous examen.

9 Ainsi que de celles transférées en vertu de l'article 106 de la loi modifiée du 29 août 2008 relative à la libre circulation des personnes et l'immigration pour prévenir un refus d'entrée sur le territoire.

si des dispositions spécifiques qui, non seulement, autoriseraient de tels accès, mais encore en fixeraient les conditions et les limites, étaient ajoutées au projet de loi sous avis.

Le Conseil d'État relève que le législateur belge, dans le chapitre 7 de la loi précitée du 25 décembre 2016 a créé l'UIP belge en tant que service établi au sein du Service Public Fédéral Intérieur et sous la direction d'un fonctionnaire issu de ce service public, assisté par un service d'appui émanant de la même administration, ainsi que de membres détachés des services compétents énumérés à la loi. L'article 14, paragraphe 1er, de cette loi précise en son dernier alinéa que « les membres des services compétents sont placés sous l'autorité fonctionnelle et hiérarchique du fonctionnaire dirigeant de l'UIP. Toutefois, ceux-ci gardent le statut de leur service d'origine. ».

Il découle des travaux parlementaires belges que cette disposition est motivée comme suit : « Les membres détachés feront partie de l'UIP et auront à ce titre, la mission d'interroger la banque de données des passagers au profit de leur service. Ces membres détachés auront accès à la banque de données sur la base de profils individuels d'accès. Ceux-ci vérifieront, sous l'autorité fonctionnelle du fonctionnaire dirigeant, si les conditions légales de consultation sont remplies (par exemple liste 90*ter*, délais d'accès, apostille,…). Le modèle proposé offre la garantie que la banque de données des passagers n'est pas gérée par les services compétents mais par un service au sein du SPF Intérieur. Les services compétents n'auront dès lors pas accès à la masse d'informations des passagers mais pourront l'interroger uniquement sur la base de requêtes par le biais de leurs membres détachés. »[10]

Le Conseil d'État comprend l'utilité d'une disposition qui prévoit que les différents services compétents disposent d'un représentant en tant qu'« agent de liaison » au sein de l'UIP. Il comprend également l'utilité d'une solution qui assure que ces agents gardent un accès aux traitements de données propres aux différents services d'origine. Il estime cependant que, à l'instar de la solution retenue en Belgique, il y a lieu, afin d'éviter la disparition des prédits accès suite au détachement administratif, de compléter l'article sous examen par une disposition qui maintient lesdits accès, dans les limites toutefois tracées par les lois régissant leur service d'origine respectif à moins que les auteurs du projet de loi ne préfèrent mettre en place, à l'instar toujours du modèle belge, une unité indépendante de la Police grand-ducale et dont la structure pourrait s'inspirer, *mutatis mutandis*, de la Cellule de renseignement financier établi auprès du parquet de Luxembourg.

Pour ce qui est du contenu de la disposition sous examen, celle-ci se limite à la création de l'UIP ainsi qu'à la description de sa compétence. Le Conseil d'État n'a pas d'observation à formuler par rapport à la première de ces compétences, à savoir la collecte des données PNR recueillies par les transporteurs aériens ainsi que la conservation et le traitement de ces données. Pour ce qui est de la deuxième compétence, à savoir le transfert de ces données et des résultats de leur traitement « aux services compétents », le Conseil d'État s'interroge sur la définition de ces services. Le projet de loi limitant le traitement des données à une finalité de prévention et de répression du terrorisme et de la criminalité grave, ces services compétents (visés plus spécifiquement à l'article 13 du projet sous avis) ne sauraient être que, selon la situation procédurale, la Police grand-ducale, sinon les autorités judiciaires, à l'exclusion d'autres services de l'État, ce qui est de nature à remettre en cause notamment la présence du SRE au sein de l'UIP, de même que son rôle dans le cadre du traitement des données PNR, points sur lesquels le Conseil d'État reviendra dans le cadre de l'examen de l'article 13 du projet de loi.

Enfin, pour ce qui est de l'activité *sub* c), à savoir l'échange, respectivement, des données et des résultats de leur traitement, avec d'autres unités dans les autres États membres de l'Union européenne ainsi qu'avec Europol et avec les pays tiers, le Conseil d'État renvoie à ses considérations faites à l'endroit des différentes dispositions du projet de loi ayant trait à l'échange des données collectées.

Article 4

L'article 4, alinéa 1er, désigne le responsable de l'UIP comme responsable du traitement des données PNR, tandis que le deuxième alinéa indique la composition de ladite unité. Il en découle que cette unité pourra être composée de personnel de provenances diverses, à savoir, tant, de la Police grand-ducale, de l'Administration des douanes et accises ainsi que du SRE.

Le Conseil d'État note que la disposition ne donne aucune indication sur les conditions, notamment de grade ou de fonction, que doit remplir le responsable de l'unité. N'y figure même pas la précision

10 Doc. parl. belge 54/2069/001 du 4 octobre 2016, exposé des motifs, p. 23.

s'il doit s'agir d'un membre du cadre policier ou bien si un membre du cadre civil peut également remplir cette tâche de direction.

Dans leurs avis respectifs, tant la Cour supérieure de justice que les deux parquets d'arrondissement ont estimé que l'UIP devrait également comprendre, parmi son personnel, un magistrat détaché à cette fin ; les parquets se sont même demandés « s'il ne serait pas recommandable de faire présider cette unité » par un tel magistrat. Le Conseil d'État soulève que le détachement de magistrats au sein de cette unité y compris à sa direction, équivaudrait à un changement de statut de l'UIP, sans que ce changement contienne une plus-value évidente. Une telle possibilité ne serait par ailleurs envisageable que si l'UIP était mise en place en tant qu'unité indépendante des structures de la Police grand-ducale et le Conseil d'État renvoie à ses considérations faites à l'endroit de l'article 3 du projet de loi sous avis.

Article 5

L'article 5 met à la charge des transporteurs aériens le transfert à l'UIP des données PNR relatives à tous les passagers de vols à destination ou en provenance de Luxembourg dont ils disposent. Il ne crée donc pas une obligation pour ces transporteurs de recueillir des informations supplémentaires, respectant en cela l'article 8 de la directive.

Par contre, en ne visant que les données des passagers de vols à destination ou en provenance de Luxembourg, les données relatives aux passagers ne faisant que transiter par le territoire national ne sont pas visées par la disposition sous examen. Il y a dès lors lieu de compléter, sous peine d'opposition formelle pour transposition incomplète de la directive, le projet de loi sous examen, à l'instar de l'article 5 de la loi belge précitée du 25 décembre 2016, par une référence aux données des passagers « transitant par le territoire national ».

Le projet de loi précise encore que la transmission à l'UIP des données PNR est effectuée « sans préjudice des obligations imposées » par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration. Il s'agit là des données API déjà recueillies à l'heure actuelle pour les passagers provenant d'un pays qui n'est pas membre de l'Union européenne. Le Conseil d'État rend les auteurs du projet de loi attentifs à la disposition figurant à l'article 8, paragraphe 2, de la directive et qui a trait à l'obligation pour les États d'adopter les mesures nécessaires afin que le transfert des données API à l'UIP se fasse par des méthodes techniques identiques au transfert des données PNR. Afin de vérifier que la transposition de la directive est faite correctement sur ce point, le Conseil d'État devrait disposer de tous renseignements de nature à établir que ce transfert est effectué dans les conditions requises par le législateur européen. Dans l'attente de ces renseignements, il doit réserver sa position quant à la dispense du second vote constitutionnel.

Article 6

L'article 6 a trait aux moments auxquels les transporteurs doivent communiquer les données PNR à l'UIP et prévoit trois échéances précises.

Le Conseil d'État relève, ainsi qu'il a également été signalé dans plusieurs avis lui transmis, que l'article 8, paragraphe 3, de la directive ne prévoit que deux échéances, la première se situant dans une période entre vingt-quatre et quarante-huit heures avant l'heure de départ programmé du vol et la deuxième se situant immédiatement après la clôture du vol. En ajoutant une obligation supplémentaire à celles prévues à la directive, risquant ainsi en outre de créer une charge administrative supplémentaire pour les transporteurs qui utilisent l'aéroport de Luxembourg par rapport à ceux qui ont recours à des aéroports situés dans des pays n'imposant pas un même niveau d'obligations, l'article sous revue ne constitue pas une transposition correcte de la directive, de telle sorte que le Conseil d'État doit s'y opposer formellement.

Dans ce cadre, le Conseil d'État constate que l'arrêté royal belge du 18 juillet 2017 « relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données de passagers, reprenant les obligations pour les compagnies aériennes », en son article 3, paragraphe 2, ne prévoit qu'une transmission 48 heures avant leur départ programmé du vol et immédiatement après la clôture de ce

vol[11], tandis que le dispositif français se limite à un seul envoi, qui doit être effectué « dès la clôture du vol »[12].

Le paragraphe 2 n'appelle pas d'observation.

Article 7

L'article 7 a trait aux procédés techniques par lequel les données doivent être transférées à l'UIP. Il transpose l'article 16 de la directive

La phrase finale de l'article 7, paragraphe 1er, alinéa 1er, est à omettre, sous peine d'opposition formelle, au regard de l'article 297, paragraphe 1er, alinéa 3[13], du TFUE.

Article 8

L'article 8 introduit le chapitre 4 du projet de loi sous avis, consacré au traitement des données PNR. Il transpose l'article 13, paragraphe 4, de la directive et n'appelle en soi pas d'observation. Le Conseil d'État renvoie cependant à ses observations faites à l'endroit de l'article 37.

Article 9

L'article 9 impose une obligation d'effacement de certaines données transmises par les transporteurs aériens. Le Conseil d'État note que, contrairement à l'article 8, l'article 9 ne figure pas à l'article 37 du projet de loi sous examen parmi les articles dont la violation peut entraîner une sanction pénale. Étant donné cependant que le défaut d'effacement visé à l'article 9 vise un comportement similaire au défaut d'effacement visé à l'article 8, alinéa 2, le Conseil d'État suggère d'inclure cette disposition également à l'article 37 même si le Conseil d'État admet qu'un défaut d'effacement de données légalement collectées et transférées, mais ne figurant pas à l'annexe I du projet, est un comportement qui n'atteint pas le même seuil de gravité qu'une violation de l'article 8, de telle sorte que la sanction devrait être adaptée à cette gravité moindre. En effet, s'il est vrai que l'article 14, paragraphe 1er, de la directive n'oblige pas expressément les États à incriminer le comportement en question, une disposition prévoyant une sanction n'y est cependant pas contraire et sera indiquée pour assurer une meilleure protection des données personnelles.

Article 10

L'article 10 précise l'étendue et la finalité du traitement des données PNR au sein de l'UIP.

Le paragraphe 1er prévoit que le traitement a pour but d'identifier, parmi les différents passagers, les personnes « pour lesquelles un examen plus approfondi par les services compétents », voire par Europol, serait requis. Le Conseil d'État croit à ce propos comprendre qu'il s'agit des autorités visées à l'article 13 du projet. Il estime toutefois qu'il aurait été utile d'ajouter une définition de ces services au niveau de l'article 2 du projet.

Le paragraphe 2 indique les éléments sur base desquels l'UIP procède à ces évaluations, à savoir une comparaison des données PNR avec certains traitements de données effectués sur base de critères établis.

Le Conseil d'État relève, tout d'abord, que l'utilisation des termes de « banques de données » ne correspond pas à la terminologie utilisée dans le cadre du droit luxembourgeois de la protection des données, et qu'il y a lieu de remplacer ces termes par ceux de « traitements de données ». Ensuite, il s'interroge sur la portée de ce texte.

Si le droit d'accéder « aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité (…) » figure à l'article 6, paragraphe 3, point a), de la directive, et doit dès lors faire l'objet d'une transposition, cette transposition doit se faire dans le respect des droits découlant de la protection de la vie privée telle que celle-ci est prévue tant à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (article 8) qu'à la Constitution (article 11, paragraphe 3).

---

11 Moniteur belge du 28 juillet 2017, p. 75.934.

12 Art. R232-1 du Code de la sécurité intérieure.

13 Article 297, paragraphe 1er, alinéa 3, du TFUE : « Les actes législatifs sont publiés dans le Journal officiel de l'Union européenne. Ils entrent en vigueur à la date qu'ils fixent ou, à défaut, le vingtième jour suivant leur publication. »

Le Conseil d'État relève que le projet de loi sous avis ne met pas en place un accès direct qui serait propre à l'UIP, mais un accès indirect qui se base sur ceux des services qui la composent. Les traitements susceptibles d'une utilisation sont ainsi déterminés par les bases légales respectives des différents services, ce qui répond à l'interrogation formulée par la CNPD dans son avis[14].

La première vérification se fera ainsi au travers d'une comparaison automatisée des données PNR avec tous les traitements visés au paragraphe 2, point a), de la disposition sous revue. Le Conseil d'État s'interroge cependant si une telle comparaison automatisée est, dans tous les cas, compatible avec les finalités ayant motivé l'accessibilité des différents services. De même, il s'interroge sur la manière selon laquelle seront remplies – sauf la mise en place dans les différentes lois d'une disposition légale spécifique à cet effet – les conditions accompagnant ces accès et, notamment, les conditions de contrôle des accès mis en place par les différentes législations[15]. Il s'interroge encore sur la façon dont s'effectuera un tel accès automatisé aux traitements effectués par des institutions ou organismes internationaux, et par rapport à des informations provenant de services étrangers.

La deuxième vérification, qui a uniquement pour but de détecter parmi toutes les concordances positives celles qui seront continuées aux services compétents, sera, quant à elle, conditionnée par les accès propres dont peut bénéficier le membre de l'UIP en raison de sa provenance et dans les limites de celle-ci. Dans ce cas, comment se fera la transmission des informations entre les différents membres qui, en vertu de la l'article 4, alinéa 2, ne peuvent agir que « dans la limite des attributions légales de l'administration » dont ils relèvent et qui, le cas échéant ne sont pas autorisés à communiquer les informations dont ils disposent aux autres membres de l'UIP ?

En second lieu, l'UIP effectuera son évaluation par rapport à des critères préétablis, qui, d'après le projet de loi sous avis, « sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents », et cela sur base des éléments de choix figurant au projet. Transposant l'article 6, paragraphe 4, de la directive, le dernier alinéa du paragraphe 2 ne donne pas lieu à observation.

Le paragraphe 4 de l'article sous revue prévoit une transmission des données PNR de certaines personnes « aux services compétents », et cela « en vue d'un examen plus approfondi ». Le texte proposé correspond à l'article 6, paragraphe 6, de la directive. Le Conseil d'État relève que la communication de données PNR ou du résultat du traitement de ces données figure encore à l'article 13 du projet de loi sous examen. Ce n'est dès lors qu'à travers une lecture combinée de ces deux textes que la finalité de cette transmission apparaît, à savoir que « l'examen plus approfondi » correspond à un traitement des données transmises par les services compétents « dans le cadre de leurs attributions légales ». Le Conseil d'État se réfère aux développements qu'il sera amené à faire dans le cadre de l'examen de l'article 13.

L'article sous revue ne donne pas lieu à d'autres observations.

Article 11

L'article 11 a trait aux critères visés à l'article 10, paragraphe 2, alinéa 2, et ne donne pas lieu à observation.

Article 12

L'article 12 ajoute une finalité supplémentaire au traitement des données PNR, à savoir celle de pouvoir répondre aux demandes des services compétents. La loi précise que ces demandes doivent être « dûment motivées et fondées sur des motifs suffisants ». Le Conseil d'État s'interroge sur les contours exacts de la motivation, sur les critères que l'UIP devra appliquer, et sur les sanctions frappant une

---

14 Doc. parl. 7151[2], avis de la CNPD, p. 5.

15 voir, à titre d'exemple, art. 48-24, paragraphe 4, du Code de procédure pénale: Le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que:

(a) les magistrats et les membres du personnel de l'administration judiciaire ne puissent consulter les fichiers auxquels ils ont accès qu'en indiquant leur identifiant numérique personnel, et

(b) que les informations relatives aux magistrats et aux membres du personnel de l'administration judiciaire ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de 3 ans, afin que le motif de la consultation puisse être retracé. Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation.

motivation insuffisante. Est-ce qu'une demande insuffisamment motivée devra être rejetée ? Si oui, par qui ? Quelle procédure sera alors applicable ?

Article 13

L'article 13 et les articles 14 et 15, forment le chapitre 5 du projet de loi sous avis consacré aux services habilités à demander et à recevoir des données PNR ou le résultat du traitement de ces données.

Il prévoit que les services de la Police grand-ducale, le SRE[16] ainsi que les services de l'Administration des douanes et accises sont à considérer comme services compétents au sens du projet de loi sous avis et vise à transposer l'article 7 de la directive et ne donne pas lieu à observation.

Si la précision que les services figurant à la disposition sous avis ne peuvent recevoir ces données que « dans le cadre de leur attribution légale » est en soi superflue, celle stipulant que la communication ne peut avoir lieu que « dans la limite du besoin d'en connaître » dans le chef du service en question pose problème. En effet, ainsi que le rappellent à juste titre les autorités judiciaires dans leurs avis, aucune disposition légale ne précise la notion de « besoin d'en connaître », certes tirée du langage des habilitations de sécurité, mais non définie dans le cadre de la transmission de données personnelles.

Le Conseil d'État note que l'article 7, paragraphe 1er, de la directive, que la disposition sous avis est appelée à transposer, est plus précis étant donné qu'il détermine avec précision la finalité de la transmission des données aux services concernés, finalité qui, non seulement, s'inscrit nécessairement dans les limites des compétences que la loi a entendu conférer auxdits services, mais encore délimite leurs besoins de connaissance. En ne suivant pas la directive sur ce point, le projet de loi sous avis procède à une transposition incorrecte de la directive, de telle sorte que le Conseil d'État doit émettre une opposition formelle quant à la formulation retenue.

Le Conseil d'État relève que l'article 13 précise que la transmission des données est effectuée « sans préjudice des attributions des autorités judiciaires » compétentes en matière pénale. Il comprend cette précision comme voulant dire que les autorités judiciaires peuvent, dans les conditions posées par le Code de procédure pénale et d'éventuelles lois spéciales, demander et recevoir les renseignements détenus par l'UIP.

Ainsi que le souligne le procureur général d'État dans son avis, la loi belge du 25 décembre 2016, précitée, a, à ce propos, introduit par son article 50 une disposition spécifique au Code d'instruction criminelle belge, autorisant le procureur du Roi à « par une décision écrite et motivée, charger l'officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers (…) » dans le cadre procédural spécifié au nouvel article 46*septies* dudit code[17]. Dans le cadre juridique luxembourgeois, une telle disposition permettrait aux procureurs d'État d'avoir un accès simplifié aux données PNR détenues par l'UIP en leur évitant d'avoir à saisir le juge d'instruction ne fût-ce que par le biais d'une procédure dite « mini-instruction », tout en sachant qu'en tant qu'acte d'enquête, la réquisition serait susceptible du recours inscrit à l'article 48-2 du Code de procédure pénale.

Enfin, il y a lieu de se référer non pas aux « services de la Police grand-ducale », ni aux « services de l'Administration des Douanes et Accises », mais à la « Police grand-ducale » et à l'« Administration des douanes et accises », les pouvoirs n'étant pas accordés à des services spécifiques, mais à l'administration concernée.

---

16 Le Conseil d'État attire cependant l'attention sur les développements faits au sujet du 2e amendement transmis en date du 27 février 2018 quant à la communication des informations au SRE.

17 Art. 46*septies* du code d'instruction criminelle belge : « En recherchant les crimes et délits visés à l'article 8, § 1er, 1°, 2° et 5°, de la loi du 25 décembre 2016 relative au traitement des données des passagers, le procureur du Roi peut, par une décision écrite et motivée, charger l'officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers. La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. La mesure peut porter sur un ensemble de données relatives à une enquête spécifique. Dans ce cas, le procureur du Roi précise la durée de la mesure qui ne peut excéder un mois à dater de la décision, sans préjudice de renouvellement. En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et, par une décision motivée et écrite, requérir du fonctionnaire dirigeant de l'UIP la communication des données des passagers. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence. »

Article 14

Sans observation.

Article 15

L'article 15 est appelé à transposer l'article 7, paragraphe 6, de la directive. Le Conseil d'État s'interroge sur les raisons qui ont amené les auteurs du projet de loi à ne reprendre que la première phrase de ce paragraphe. En effet, même s'il est vrai que l'article 8 du projet de loi sous avis interdit le traitement des données y visées, il est dans l'intérêt de la protection de la vie privée de rappeler l'interdiction de prendre des décisions qui seraient basées sur ces données, si celles-ci avaient néanmoins, en contravention à la loi, été collectées. Tant que le texte n'aura pas été complété sur ce point, le Conseil d'État doit s'y opposer formellement pour transposition incorrecte de la directive.

Article 16

L'article 16 introduit le chapitre 6, consacré à l'échange d'informations entre les États membres de l'Union européenne.

Il transpose l'article 9, paragraphe 1er, de la directive et n'appelle pas d'observation.

Article 17

L'article 17 transpose l'article 9, paragraphe 2, de la directive.

L'alinéa 3 du paragraphe 1er prévoit que le transfert de données dépersonnalisées par masquage ne peut être effectué que sur autorisation du procureur d'État de Luxembourg ou de son délégué. Or, ainsi que le procureur général d'État le soulève dans son avis, c'est ce magistrat qui « est traditionnellement l'autorité centrale pour tous les instruments relatifs à l'entraide judiciaire ». Ainsi, à titre d'exemple récent, dans la loi du 17 mai 2017 portant approbation de l'accord entre le Gouvernement du Grand-duché de Luxembourg et les États-Unis aux fins de renforcer la coopération en matière de prévention et de lutte contre le crime grave[18], qui met en place un mécanisme de communication d'informations entre les services compétents des deux pays concernés, le procureur général d'État est désigné comme autorité compétente pour autoriser la communication des données visées aux dits accords dans une optique de prévention, de détection et d'enquête concernant un crime grave.

Il y a par conséquent lieu de remplacer la mention du procureur d'État de Luxembourg par celle du procureur général d'État en tant qu'autorité centrale, en gardant toutefois la possibilité pour le procureur général d'État d'avoir recours à un délégué.

Article 18

L'article 18 vise les demandes adressées par l'UIP et les services compétents nationaux aux UIP des autres États membres. Pour ce qui est de l'alinéa 1er, le Conseil d'État rappelle que celui-ci est une disposition qui, en réglant la collaboration entre des services de plusieurs États membres, empiète sur le terrain de compétence de l'instrument de droit européen qu'est la directive, et doit dès lors être omise. La situation se trouve par ailleurs réglée à l'article 9 de cette dernière.

Si les auteurs entendaient cependant maintenir l'alinéa 1er au projet de loi afin de clarifier à l'attention des services concernés qu'ils disposent de la possibilité de formuler la demande y décrite, il y aurait en tout cas lieu de faire abstraction de sa deuxième phrase, dépourvue de valeur normative.

L'alinéa 2 de l'article 18 n'appelle pas d'observation.

Article 19

L'article 19 vise à transposer l'article 9, paragraphe 5, de la directive et instaure le principe d'un échange de données par l'intermédiaire de tous les canaux de coopération policière existant entre les autorités compétentes. Il est dès lors plus restrictif que la disposition à transposer, qui prévoit que l'échange peut avoir lieu « par l'intermédiaire de n'importe quel canal de coopération » existant entre ces autorités. Limitant ainsi la portée du texte à transposer, le projet de loi ne procède pas à une trans-

18 JOGDL A 505 du 23 mai 2017, art 5. : « Pour le Grand-Duché de Luxembourg, le procureur général d'État est l'autorité compétente au sens de l'article 2, point 5), de l'Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites pénales, signé à Amsterdam le 2 juin 2016. »

position correcte de celui-ci, de telle sorte que le Conseil d'État doit s'y opposer formellement. Par ailleurs, il y a lieu de remplacer la mention des « autorités compétentes » par celle des « services compétents », les services de police n'étant pas à considérer comme des autorités au sens constitutionnel du terme. La même remarque vaut d'ailleurs également pour l'ensemble des autres occurrences du même terme.

Article 20

L'article 20 constitue l'article unique du chapitre 7 relatif aux conditions d'accès aux données PNR par Europol et entend transposer l'article 10 de la directive. Cette disposition est cependant superfétatoire, sauf à lui reconnaître une pure valeur déclaratoire, étant donné que les compétences d'Europol ainsi que ses droits et obligations dans le cadre desdites compétences, font l'objet d'instruments européens et ne nécessitent pas de mesures de transposition particulières en droit national.

Article 21

L'article 21 introduit le chapitre 8 relatif au transfert de données vers des pays non membres de l'Union européenne et vise à transposer l'article 11 de la directive. Ainsi qu'il découle du commentaire de l'article, un tel transfert est tout d'abord « subordonné à l'existence d'une décision d'adéquation de la Commission européenne ou, en absence d'une telle décision, à l'existence de garanties appropriées », conditions que le projet entend introduire en recourant aux termes de « sans préjudice des dispositions de l'article 35, paragraphe (1), point (d), et des articles 36 à 38 » du projet de loi n° 7168 transposant la directive (UE) 2016/680 relative au transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales.

L'expression « sans préjudice de » signifie que la règle qui va être énoncée est sans incidence sur l'application d'une autre règle qu'on entend précisément ne pas écarter et qui pourra s'appliquer également. Elle est synonyme de « indépendamment de ». Dans la mesure où la disposition à laquelle cette locution se réfère s'applique également dans la situation visée, ce qui devrait normalement découler de la structure même du texte, on peut généralement s'en dispenser. Dans certains cas, l'emploi de l'expression « sans préjudice de » peut néanmoins s'avérer utile pour éviter des questions d'interprétation quant à l'applicabilité simultanée de deux régimes à une situation donnée.

Telle qu'utilisée dans le projet sous examen, elle est comprise par le Conseil d'État comme signifiant que la règle édictée au projet de loi n° 7168 constitue la norme générale, qui doit être remplie pour tout transfert, et à laquelle viennent s'ajouter des conditions spéciales, supplémentaires, reprises aux points a) à d) de l'article 21 sous examen. Il y a dès lors lieu à application cumulative des deux jeux de conditions, la responsabilité de la vérification que ces conditions sont remplies étant de la compétence première de l'UIP.

Le Conseil d'État note que l'article 11 de la directive, dans son paragraphe 1er, point a), fait figurer parmi les conditions à remplir pour permettre le transfert à un pays tiers des données PNR ainsi que le résultat de traitement de ces données, le respect « des conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI », qui fait l'objet du projet de loi de transposition n° 7168. Or, cette décision-cadre a été abrogée avec effet au 6 mai 2018, par l'article 59 de la directive (UE) 2016/680, qui précise que « les références faites à la décision abrogée (…) s'entendent comme faites à la présente directive », de telle sorte que, en admettant une entrée en vigueur pour le moins concomitante des deux lois de transposition, la référence faite dans le projet sous avis au chapitre V du projet de loi n° 7168 est conforme au texte à transposer.

Le texte sous examen n'appelle pas d'autre observation quant au fond.

Pour donner une meilleure lisibilité à la disposition sous examen, le Conseil d'État suggère cependant de remplacer le début de l'article par une énumération des conditions figurant aux dispositions de la loi de transposition y visée, qui se situerait avant le point a) actuel, et en procédant à une renumérotation de la suite, ainsi que de commencer l'article par « L'UIP peut transférer (…) ».

Article 22

Sans observation.

Article 23

L'article 23 vise à transposer l'article 11, paragraphe 3, de la directive dont il reprend les termes. Le Conseil d'État s'interroge cependant sur le contenu de la notion de transfert « dans des conditions

compatibles avec la présente loi », termes figurant certes à la directive, mais dont la valeur normative est des plus réduites étant donné que, pour leur donner une portée tant soit peu utile, le projet devrait préciser quelles dispositions de la loi, en plus de celles figurant au chapitre 8, seraient à respecter pour que le transfert de données et le résultat du traitement de données puissent être possibles. Le Conseil d'État s'interroge également sur la sanction à appliquer si le transfert a eu lieu dans des conditions qui n'ont pas été compatibles avec la loi sous avis. Est-ce que le responsable du transfert sera sanctionné ? Si oui, comment ? Quel sera le sort des données communiquées dans le pays qui les aura reçues ?

Article 24

L'article 24 transpose l'article 11, paragraphe 4, de la directive, qui prévoit que « chaque fois qu'un État membre transfère des données PNR en vertu du présent article, le délégué à la protection des données de l'UIP de cet État membre doit en être informé ». Étant donné que le délégué à la protection des données au sein de l'UIP n'apparaît une première fois qu'à l'article 29 du projet sous examen, il y a lieu de compléter l'article 24 par un renvoi à cette disposition pour une meilleure lisibilité du texte.

Article 25

L'article 25 introduit le chapitre 9, consacré à la durée de conservation et à la dépersonnalisation des données, et limite la conservation des données PNR par l'UIP à une durée maximale de cinq ans à compter du transfert par le transporteur aérien, sauf pour les données transférées à un service compétent dans les conditions visées au projet. Transposant quasi textuellement l'article 12, paragraphes 1er et 4, de la directive, la disposition sous examen ne donne pas lieu à observation.

Article 26

L'article 26 transpose l'article 12, paragraphe 2, de la directive, dont il reprend les termes. Au paragraphe 2, point b), il y a lieu de remplacer la référence au procureur d'État de Luxembourg par une référence au procureur général d'État, et le Conseil d'État de se référer aux considérations faites à l'endroit de l'article 17.

Article 27

L'article 27 transpose l'article 12, paragraphe 5, de la directive. S'il est vrai qu'il a recours à un certain nombre de termes relativement imprécis, comme par exemple ceux de « (conservation pour) le temps nécessaire pour informer les services compétents », ou encore « futures « fausses » concordances positives », ces formulations correspondent néanmoins à celles du texte à transposer, et le Conseil d'État n'a pas d'observation à formuler.

Article 28

L'article 28 introduit le chapitre 10, consacré à la protection des données à caractère personnel et vise à transposer l'article 13 de la directive. Cette dernière disposition place les traitements des données PNR dans le champ d'application de la décision-cadre 2008/977/JAI. Ainsi qu'il a été rappelé à l'endroit de l'article 21, cette décision-cadre est remplacée avec effet au 6 mai 2018 par la directive (UE) 2016/680, précitée, et dont la transposition fait l'objet du prédit projet de loi n° 7168.

Le Conseil d'État note cependant que le projet sous avis, contrairement à l'article 13 de la directive, retient le principe de la compétence de la CNPD ainsi que l'application du régime général sur la protection des données[19] aux données PNR collectées, pour ne mentionner la loi de transposition de la directive (UE) 2016/680 qu'en début de la disposition pour réserver les droits des autorités judiciaires. Il est dès lors en porte-à-faux avec le texte à transposer qui vise expressément la décision-cadre 2008/977/JAI, remplacée par la directive (UE) 2016/680, et ne retient l'application du régime de droit commun de la protection des données que pour le traitement des données à caractère personnel effectué par les transporteurs aériens[20], de telle sorte que le Conseil d'État doit s'opposer formellement au texte actuel, qui constitue une transposition incorrecte de la directive.

19 Projet de loi n° 7184.

20 Directive (UE) 2016/681, article 13, paragraphe 3.

Article 29

L'article 29 est consacré au délégué à la protection des données que le responsable de l'UIP doit désigner au sein de cette unité. Le statut mis en place pour ce délégué n'appelle pas d'observation particulière, sauf qu'il semble encore utile de compléter le paragraphe 4, alinéa 2, par l'indication des bases légales permettant la saisine de la CNPD telles que celles-ci découlent de la loi de transposition du règlement (UE)2016/679, précité.

Article 30

L'article 30 est consacré aux informations que l'UIP doit mettre à la disposition du public en application des dispositions de transposition de la directive (UE) 2016/680. La CNPD, dans son avis, estime que l'article correspondant du projet de loi n° 7168 serait plus complet que l'article 30 sous avis, en ce qu'il comprendrait un deuxième paragraphe consacré à la mise à disposition d'informations supplémentaires. Le Conseil d'État note cependant que ce deuxième paragraphe n'est applicable qu'à des cas particuliers, ce qui, selon le commentaire de la disposition dans le prédit projet de loi correspondrait à « l'hypothèse de la fourniture d'informations dans les cas où la personne concernée a formulé préalablement une demande en ce sens »[21]. Par ailleurs, il découle de la lecture des quatre cas de figure figurant à l'article 13, paragraphe 2, du projet de loi n° 7168 que ces éléments sont des éléments qui découlent nécessairement de la loi sous avis, et qui sont à la disposition de tout intéressé au travers d'une simple lecture de cette loi, celle-ci une fois votée. Dans le même ordre d'idées, le Conseil d'État note que le projet sous avis ne contient pas non plus l'équivalent du paragraphe 3 du même article 13, relatif au retard ou à une limite dans la fourniture des informations visées au deuxième paragraphe, non repris au projet sous examen étant donné que chaque passager sait pertinemment bien quelles données PNR sont collectées et à quelles fins. Le Conseil d'État peut par conséquent marquer son accord avec la disposition sous examen.

Article 31

Le Conseil d'État, qui n'a pas d'observation à formuler quant au fond de cette disposition, note que celle-ci est placée, en transposition correcte de la directive, dans le champ d'application du projet de loi n° 7168, et non pas dans celui du projet de loi n° 7184, précité.

Article 32 à 35

Sans observation.

Article 36

Si le texte de l'article 36 ne donne pas lieu à observation quant à son fond, le Conseil d'État estime qu'il y a lieu de remplacer la mention de « l'autorité de contrôle » par la désignation précise de celle-ci, et de mentionner par conséquent la CNPD. Si la disposition sous avis correspond au texte de la directive, le Conseil d'État se pose cependant des questions quant à la faisabilité matérielle de l'information de la personne concernée qui, dans la grande majorité des cas, risque de ne pas résider sur le territoire national, ce qui mettrait l'UIP devant une impossibilité matérielle de remplir cette obligation légale.

Article 37

L'article 37 introduit le chapitre 11 du projet de loi, consacré aux sanctions en cas de violation des différents prescrits de la loi en projet, et punit de sanctions pénales les comportements y déterminés.

L'alinéa 1er punit des peines y prévues « la violation des articles 8, 15 et 36 » de la loi en projet.

L'article 8 interdit le traitement de données révélant des données découlant de la sphère d'intimité du passager et crée une obligation d'effacement définitif si de telles données étaient néanmoins collectées. Le Conseil d'État estime qu'afin d'assurer le respect du principe constitutionnel de la légalité de la peine, il y a lieu de préciser lequel des deux comportements visés à l'article 8 est sanctionné : le traitement illicite ou bien le défaut d'effacement, ou bien les deux comportements ? Il y a également lieu de préciser s'il s'agit d'une infraction intentionnelle, nécessitant la volonté déterminée de contrevenir à la disposition légale, ou bien si le simple fait de procéder à un tel traitement (ou non-effacement)

21 Doc. parl. n° 7168, commentaire des articles, p. 35.

est suffisant pour encourir la peine prévue par la loi sous avis sans que la preuve d'un dol spécial doive être rapportée. Le Conseil d'État considère en effet qu'un simple dysfonctionnement au sein de l'unité, dépourvu de toute intention criminelle, qui serait éventuellement sanctionnable du point de vue disciplinaire, n'est pas de nature à entraîner la responsabilité pénale, que ce soit du responsable de l'unité ou du fonctionnaire à l'origine du traitement en question, et renvoie à ses considérations faites dans le cadre du projet de loi n° 6913 sur l'archivage[22].

Le Conseil d'État rappelle ses considérations faites à l'endroit de l'article 9, aux termes desquelles il estime que la violation de l'obligation d'effacement des données reprises à cette disposition doit également figurer parmi les comportements sanctionnés pénalement, sous réserve d'une adaptation de la sanction à la moindre gravité d'une méconnaissance de l'obligation d'effacement y prévue.

L'article 15 interdit de prendre une décision telle que visée au texte sur la seule base du traitement automatisé de données PNR. L'infraction consisterait dès lors dans la prise d'une décision dans ces conditions et malgré l'interdiction légale. Se pose dès lors à nouveau la question de l'intention que doit remplir l'auteur du fait incriminé.

L'article 36 oblige l'UIP à informer sans retard injustifié tant la personne concernée que l'autorité de contrôle d'une atteinte aux données à caractère personnel. Le Conseil d'État rappelle ses considérations à l'endroit de cette disposition quant aux problèmes matériels auxquels risque d'être confrontée l'UIP. Est-ce que l'impossibilité matérielle de contacter la personne concernée serait une cause de justification suffisante pour éluder la sanction pénale ?

La seconde phrase de l'alinéa 1er de la disposition sous examen, prévoit encore que « la juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent alinéa sous peine d'astreinte ». Le Conseil d'État remarque en premier lieu, ainsi que l'ont déjà fait les autorités judiciaires, que le traitement ne peut être contraire aux dispositions de l'article sous avis, mais seulement contraire aux articles de la loi auxquels l'article 37 fait référence. En deuxième lieu, il estime que, si traitement illicite il y a, sa cessation ne doit pas être une faculté pour le juge mais une obligation, afin d'assurer une sanction effective, proportionnée et dissuasive telle que prévue à l'article 14, alinéa 3, de la directive.

En troisième lieu, le Conseil d'État constate que l'astreinte n'est pas plafonnée, et renvoie à ses considérations faites dans le cadre de son avis de ce jour au projet de loi n° 7184 relatives à sa section XIII.

Le dispositif prévu n'étant pas conforme à la directive, le Conseil d'État est amené à s'opposer formellement à l'article 37, alinéa 1er, du projet sous avis.

L'alinéa 2 rend applicable la disposition de l'article 49 du projet de loi n° 7168. Le Conseil d'État note que l'article 49, paragraphe 2, de ce dernier texte prévoit également des sanctions pénales qui recoupent partiellement celles prévues à l'alinéa 1er de l'article 37, mais sans pour autant leur correspondre intégralement. Le Conseil d'État invite les auteurs à veiller à la cohérence des dispositions pénales mises en place pour des situations analogues. Il attire encore l'attention du Gouvernement sur le fait que les trois projets composant le « Paquet protection des données » contiennent des approches différentes dans la mesure où les méconnaissances des règles imposées sont sanctionnées tantôt par des dispositions pénales classiques, tantôt par des sanctions administratives imposées par la CNPD.

Article 38

L'article 38 punit d'une peine d'amende d'un montant maximum de 50 000 euros le transporteur aérien à raison de chaque vol pour lequel il n'a pas transmis les renseignements visés à la loi sous examen, ne les a pas transmis dans les délais prévus ou n'a pas respecté les modalités ou les formes prescrites. Cette amende est prononcée par le ministre ayant la Police grand-ducale dans ses attributions, après que le manquement a été constaté par un procès-verbal établi par la Police grand-ducale et dont copie est transmise au transporteur aérien.

Le Conseil d'État constate que le droit positif connaît déjà à l'heure actuelle une disposition qui règle une situation tout à fait analogue.

En effet, l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration punit d'une amende d'un montant maximum de 5 000 euros les entreprises de transport

22 Avis du Conseil d'État du 21 juillet 2016 concernant le projet de loi sur l'archivage (doc. parl. n° 6913[6]) ;

aérien visées à l'article 108 de la même loi « à raison de chaque voyage pour lequel l'entreprise, par faute, n'a pas transmis les renseignements y visés ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis des renseignements incomplets ou erronés », amende qui est prononcée par le ministre ayant l'Immigration dans ses attributions. L'article 108, quant à lui, dispose en son paragraphe 1er qu'encourt les sanctions prévues aux articles 147 et 148 toute « entreprise de transport aérien qui (…) n'a pas transmis les renseignements visés à l'article 106 ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis les renseignements incomplets ou erronés ». L'article 106, de son côté, prévoit en son paragraphe 1er qu'« afin de prévenir un refus d'entrée sur le territoire, les entreprises de transport aérien ont l'obligation de transmettre à la Police grand-ducale les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire du Grand-duché de Luxembourg en provenance d'un pays non-membre de l'Union européenne ».

S'il est vrai que la disposition sous examen vise la transmission de données relatives à des vols en provenance non pas d'États non membres de l'Union européenne, mais provenant d'États membres, que la communication doit se faire non pas à la Police grand-ducale mais à l'UIP, qui fait cependant partie de cette même police, et que le ministre sanctionnateur est un autre, les faits incriminés sont identiques sur tous les autres points, de telle sorte que le Conseil d'État s'interroge sur les raisons qui ont fait que le projet sous avis prévoit une amende dont le maximum est le décuple des sanctions prévues dans la disposition déjà existante, créant ainsi une inégalité de traitement selon l'origine du passager transporté, toutes autres choses étant égales par ailleurs.

Dans l'attente de recevoir des explications sur cette différence de traitement, le Conseil d'État est obligé de réserver sa position quant à la dispense du second vote.

Annexes I et II au projet

À la suite de l'article 38, le projet sous examen contient encore deux annexes, à savoir une première annexe relative aux listes des données PNR que les transporteurs aériens devront collecter, et une deuxième annexe relative à la liste des infractions visées à l'article 2, point i). Ces deux annexes n'appellent pas d'observation complémentaire à celles faites à l'endroit de l'article 2.

*

EXAMEN DES AMENDEMENTS DATES DU 27 FEVRIER 2018

Les amendements sous examen ont pour but de compléter le projet initial par deux dispositions apportant des modifications à la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, à l'effet d'autoriser le directeur de ce service à demander à l'UIP la communication de données PNR.

À titre de considérations générales, le Conseil d'État note que les auteurs des amendements sous examen invoquent l'article 51 de la loi belge du 25 décembre 2016, précitée, qui a inséré une disposition analogue dans la loi belge du 30 novembre 1998 organique des services de renseignement et de sécurité, et se doit de rappeler les considérations qu'il a faites à l'endroit de l'article 13 du projet de loi initial à l'effet de proposer l'introduction dans le projet sous avis d'une disposition permettant un accès des autorités judiciaires luxembourgeoises aux données collectées par l'UIP, également en suivant le modèle belge. L'existence même des amendements sous examen apporte à suffisance la preuve de la nécessité de l'introduction d'une disposition similaire pour ce qui est des autorités judiciaires.

Amendement 1

L'amendement n° 1 insère au projet de loi sous avis un nouveau chapitre 12 intitulé « Dispositions modificatives ». Le Conseil d'État n'a pas d'observation à faire.

Amendement 2

L'amendement 2 ajoute un article 39 au projet de loi sous avis, qui a pour objet d'ajouter un paragraphe 4 à l'article 5 de la loi précitée du 5 juillet 2016.

L'article 5 de ladite loi énumère les moyens et mesures de recherche dont dispose le SRE et qui, pour leur mise en œuvre, nécessitent une autorisation écrite du directeur du service, suite à une demande motivée et écrite de l'agent du SRE chargé du dossier. La nouvelle disposition ajoute à ces moyens et

mesures de recherche la possibilité pour le SRE de demander à l'UIP la communication des données PNR dans le cadre de ses activités.

L'amendement 2 est à lire avec l'amendement 3, qui tend à supprimer le point a) de l'article 8 de la loi précitée du 5 juillet 2016, prévoyant que le SRE peut être autorisé par le Comité ministériel du renseignement, instauré par le paragraphe 2 de l'article 2 de ladite loi, de « solliciter (…) les données des dossiers passagers relatives à une ou plusieurs personnes identifiées ou identifiables au sujet desquels le SRE dispose d'un ou de plusieurs indices concordants relatifs à une menace actuelle ou potentielle visant la sécurité nationale ou les intérêts visés à l'article 3. Le transporteur de personnes par voie aérienne visé par la demande doit fournir sa réponse sans délai. ». Cette mesure ne peut cependant être autorisée par ledit comité, au vœu du paragraphe 1er de l'article 8, que « si les moyens et les mesures de recherche dont dispose le SRE en vertu des articles 5, 6, et 7 (de la loi précitée) s'avèrent inopérants en raison de la nature des faits et des circonstances spécifiques de l'espèce ».

Il résulte de la combinaison de ces deux amendements que la mesure de l'article 8, permettant au SRE de contacter directement les opérateurs de transports aériens, sera remplacée par la possibilité pour ledit service de demander des renseignements à l'UIP et ne pourra plus être utilisée en conséquence.

Cet amendement pose cependant problème en ce que, en limitant les finalités de l'accès du SRE aux données de l'UIP, il reste en deçà de l'article 13 du projet de loi sous examen et en réduit par conséquent la portée, entraînant ainsi une transposition incorrecte de la directive, à laquelle le Conseil d'État doit s'opposer formellement. Les auteurs de l'amendement sous examen pourraient cependant éviter une telle transposition incorrecte en complétant l'article 13 du projet sous examen par une référence à l'article 5, paragraphe 4, de la loi précitée du 5 juillet 2016, tel que proposé par l'amendement sous avis.

Par ailleurs, le Conseil d'État estime que le fait de prévoir au même amendement que le directeur du SRE « rapporte tous les six mois par écrit » au prédit comité « la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquelles l'exercice des missions a exigé la demande de communication » n'est pas de nature à garantir suffisamment les droits des personnes concernées, cela d'autant plus que la procédure invoquée par les auteurs de l'amendement et prévue à l'article 5, paragraphe 3, de la loi précitée du 5 juillet 2016, qui a trait aux observations dans les lieux publics ainsi qu'aux inspections de lieux publics, prévoit un rapport par écrit au comité une fois par mois, et non pas une fois chaque semestre.

Il s'oppose par conséquent formellement à l'amendement sous avis pour contravention à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 11, paragraphe 3, de la Constitution pour autant qu'il réduit la fréquence du prédit rapport à un rapport semestriel, ce qui est totalement insuffisant pour garantir les droits des personnes concernées.

Amendement 3

L'amendement 3 est la conséquence logique de l'amendement 2 en ce qu'il supprime l'article 8, paragraphe 1er, point a), de la loi précitée du 5 juillet 2016, de telle sorte que le Conseil d'État renvoie aux développements faits à l'endroit de cet amendement.

*

OBSERVATIONS D'ORDRE LEGISTIQUE

Observations générales

La subdivision de l'article se fait en alinéas, voire en paragraphes. Les paragraphes se distinguent par un chiffre arabe, placé entre parenthèses : (1), (2),… Les subdivisions complémentaires en points, caractérisés par un numéro suivi d'un exposant « ° » (1°, 2°, 3°,…), eux-mêmes éventuellement subdivisés en lettres minuscules suivies d'une parenthèse fermante (a), b), c),…), sont utilisées pour caractériser des énumérations. Par ailleurs, les énumérations sont introduites par un deux-points. Chaque élément commence par une minuscule et se termine par un point-virgule, sauf le dernier qui se termine par un point final. En procédant de cette manière, les renvois à l'intérieur du dispositif sont à adapter en conséquence.

Lorsqu'il est renvoyé à un paragraphe dans le corps du dispositif d'un article, il faut omettre les parenthèses entourant le chiffre faisant référence au paragraphe dont il s'agit. Il convient donc de

systématiquement renvoyer au « paragraphe 1er » et non pas au « paragraphe (1) » ou encore au « premier paragraphe ».

Les intitulés ne sont pas à faire suivre par un point final, étant donné qu'ils ne forment pas de phrase. Ceci vaut non seulement pour l'intitulé du projet de loi sous examen, mais également pour les intitulés de ses chapitres.

Les textes normatifs sont en principe rédigés au présent et non au futur.

Pour ce qui est des renvois à des lettres alphabétiques, il convient de se référer aux « lettres [a) et b)] » et non pas aux « points [a) et b)] ».

À plusieurs endroits de la loi en projet, il est question de « la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ». Le Conseil d'État signale que la date relative à l'acte dont question fait défaut. Une fois celle-ci connue, elle devra être insérée aux endroits pertinents. Par ailleurs, la référence à une loi à plusieurs endroits du dispositif doit en principe comporter l'intitulé complet de l'acte auquel il s'est référé. Toutefois, afin de faciliter la lecture du dispositif, il peut exceptionnellement être recouru à la formule « loi précitée du […] » si dans le dispositif il a déjà été fait mention de l'intitulé complet de l'acte visé, à condition toutefois que le dispositif ne comporte pas ou ne sera pas susceptible de comporter à l'avenir de référence à un acte de nature identique et ayant la même date. Partant, il est indiqué de recourir à cette formule et d'insérer, à travers tout le texte en projet, le terme « précitée » entre la nature et la date de l'acte dont l'intitulé complet a déjà été mentionné.

Les institutions, administrations, services, etc., prennent une majuscule au premier substantif. Lorsque les termes génériques sont visés, tous les substantifs s'écrivent en lettres minuscules. Aussi, dans le dispositif des actes normatifs, les qualificatifs des fonctions gouvernementales et d'autres charges publiques prennent la minuscule. Dès lors, il y a lieu d'écrire « Administration des douanes et accises », « ministre ayant la Police grand-ducale dans ses attributions », « directeur général de la Police grand-ducale », « Service de renseignement de l'État », « commission spéciale ».

Il faut écrire « Police grand-ducale ».

En ce qui concerne les montants d'argent, les tranches de mille sont séparées par une espace insécable pour lire « 251 à 125 000 euros » et « 50 000 ».

Intitulé

En raison des modifications que les amendements gouvernementaux du 27 février 2018 proposent d'apporter à la loi précitée du 5 juillet 2016, il convient d'adapter l'intitulé de la loi en projet comme suit :

> « Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Examen des articles du projet de loi initial

Chapitre 2

À l'intitulé du chapitre sous avis, il convient d'écrire « Unité d'informations passagers » tel que repris à l'article 4 de la directive qu'il s'agit de transposer.

Article 7

Au paragraphe 1er, il convient d'écrire « au moyen de protocoles communs et de formats de données reconnus ».

Article 10

Au paragraphe 5, il convient d'écrire « sur le territoire du Grand-Duché de Luxembourg ».

Au paragraphe 6, les auteurs renvoient au règlement (CE) n° 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen). Le règlement (CE) du 15 mars 2006 précité a été abrogé et remplacé par le règlement (UE) 2016/399 du Parlement européen et du Conseil du

9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen). Le renvoi est à corriger.

Article 17

Au paragraphe 1er, alinéa 2, de l'article 17, il y a lieu d'écrire « en ces matières » et non pas « en la matière ».

Au paragraphe 2, il faut lire « directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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 ».

Article 22

Au paragraphe 2, alinéa 2, les locutions ou mots en latin sont à écarter.

Article 27

À l'alinéa 2, les guillemets autour du terme « fausses » sont à omettre.

Article 29

Au paragraphe 1er, alinéa 1er, les termes « en particulier » ont pour but d'illustrer un principe établi par le texte et sont à écarter comme étant superfétatoires. Une énonciation d'exemples est en effet sans apport normatif.

Article 32

L'observation relative à l'article 10, paragraphe 5, vaut également pour l'article sous avis.

Article 34

Les différents éléments de l'énumération relative à la documentation dont question sont à commencer par une lettre minuscule.

Annexes I et II

L'énumération alphabétique est à remplacer par une numérotation en chiffres arabes (1°, 2°, 3°,…).

Examen des amendements gouvernementaux datés du 27 février 2018

Amendement 2

À l'article 39 visant à introduire à l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État un nouveau paragraphe 4, il convient d'insérer une virgule entre les termes « y afférentes » et « ou », de même qu'après les termes « l'article 12 ». Le Conseil d'État propose d'écrire « dans la mesure où celle-ci est liée aux activités précitées ».

Toujours au nouveau paragraphe 4, la date relative à l'acte dont question fait défaut. Une fois celle-ci connue, elle devra être insérée à l'endroit pertinent.

Amendement 3

À l'article 40 nouveau, il convient d'écrire « la lettre a) est supprimée » en non pas « le point a) est supprimé ».

Ainsi délibéré en séance plénière et adopté à l'unanimité des 19 votants, le 30 mars 2018.

Le Secrétaire général, — *Le Président,*

Marc BESCH — Georges WIVENES

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/07

N° 7151[7]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant organisation du Service de renseignement de l'Etat

* * *

SOMMAIRE:

page

Amendements gouvernementaux

1) Dépêche du Ministre aux Relations avec le Parlement au Président de la Chambre des Députés (27.4.2018)..... 1
2) Texte et commentaire des amendements gouvernementaux 2
3) Texte coordonné..... 13
4) Texte coordonné avec suivi des modifications..... 23

*

DEPECHE DU MINISTRE AUX RELATIONS AVEC LE PARLEMENT AU PRESIDENT DE LA CHAMBRE DES DEPUTES

(27.4.2018)

Monsieur le Président,

À la demande du Ministre de la Sécurité intérieure, j'ai l'honneur de vous saisir d'amendements gouvernementaux relatifs au projet de loi sous rubrique.

À cet effet, je joins en annexe le texte des amendements avec un commentaire ainsi qu'une version coordonnée du projet de loi tenant compte desdits amendements.

Monsieur le Ministre de la Sécurité intérieure saurait de bien vouloir accorder un traitement prioritaire à l'analyse du projet de loi émargé, étant donné que le délai de transposition de la directive expirera le 25 mai 2018.

Veuillez agréer, Monsieur le Président, l'assurance de ma haute considération.

Le Ministre aux Relations
avec le Parlement,
Fernand ETGEN

*

TEXTE ET COMMENTAIRES DES AMENDEMENTS GOUVERNEMENTAUX

Modifications d'ordre légistique

Aux articles 2, 3, 6, 10, 13, 20, 21, 22, 26, 30, 34 et aux annexes I et II, la numérotation en lettres minuscules est remplacée par une numérotation en chiffres suivis d'un exposant.

Les parenthèses entourant les paragraphes auxquels il est renvoyé sont à chaque fois supprimées.

Les points finaux suivant les intitulés sont à chaque fois supprimés.

Aux articles 14, 29, paragraphe 3 et 38, paragraphe 2 les mots *« grand-ducale »* sont ajoutés après le mot *« Police »*.

Aux articles 4,13 et 26, le mot « *Renseignement »* est écrit avec une minuscule.

Aux articles 4 et 13, les mots *« Douanes »* et *« Accises »* sont écrits avec une minuscule.

A l'article 2, point g, devenant le point 7, dans l'intitulé du chapitre 2 et à l'article 3, point c, devenant le point 3, il est ajouté un « s » à la fin du mot « information ».

Les amendements qui font suite aux observations d'ordre légistique du Conseil d'Etat ne font pas l'objet d'un commentaire particulier.

Amendement 1

Dans l'intitulé du projet de loi, après le mot *« grave »* sont ajoutés les mots *« et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat. »*

Motivation

Comme suite aux amendements gouvernementaux du 27 février 2018 visant à modifier la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, l'intitulé du présent projet de loi doit être adapté.

Amendement 2

L'article 2 est amendé comme suit :

1° Au point g, devenant le point 7, après le mot *« passagers »* sont ajoutés les mots *« créée à l'article 3 de la présente loi »*.

2° Il est ajouté un point 11 qui prend la teneur suivante : *« 11° « services compétents » : les services visés à l'article 13 de la présente loi. »*.

Motivation

L'amendement visé au point 1 fait suite à l'avis du Conseil d'Etat qui propose, soit de compléter la liste des définitions par une définition de l'Unité d'informations passagers, soit de préciser dans la définition de la méthode « push » que l'Unité d'information passagers y visée est celle créée à l'article 3 de la présente loi. La seconde option proposée a été retenue.

L'amendement sub 2 est motivé par le fait que les services compétents ne sont énumérés qu'à l'article 13, alors qu'il en est déjà fait mention antérieurement dans le texte.

Amendement 3

A l'intitulé du chapitre 2, le mot *« information »* est mis au pluriel.

Amendement 4

L'article 4 est amendé comme suit :

1° Il est subdivisé en deux paragraphes. L'alinéa 1er actuel devient l'alinéa 1er du paragraphe 1er et l'alinéa 2 actuel devient l'alinéa 1er du paragraphe 2.

2° Au paragraphe 1er il est inséré un alinéa 2 libellé comme suit : *« Il est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale. »*

3° Au paragraphe 2, alinéa 1er, le mot *« détaché »* est supprimé.

4° Le paragraphe 2 comprendra un alinéa 2 ayant la teneur suivante: *« Les membres du personnel de l'Administration des douanes et accises et du Service de renseignement de l'Etat sont désignés à*

l'UIP par une décision conjointe du ministre ayant la Police grand-ducale dans ses attributions et du ministre du ressort. Ils continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP. »

Motivation

Le Conseil d'Etat s'interroge quant à la définition des *« services compétents »* et estime que ces services ne *« sauraient être que, selon la situation procédurale, la Police grand-ducale, sinon les autorités judiciaires, à l'exclusion d'autres services de l'Etat »*. Il remet dès lors en cause la présence du SRE au sein de l'UIP ainsi que son rôle dans le cadre du traitement des données PNR.

Il échet de noter dans ce contexte que, tel que le précise le Conseil d'Etat, le projet de loi limite le traitement des données à une finalité de prévention et de répression du terrorisme et de la criminalité grave. Conformément à l'article 3, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du SRE, *« le SRE a pour mission de rechercher, d'analyser et de traiter, dans une perspective d'anticipation et de prévention, […] les renseignements relatifs à toute activité qui menace ou pourrait menacer la sécurité nationale […] »*. Le paragraphe 2 de l'article 3 de la loi précitée du 5 juillet 2016 précise qu'on *« entend par toute activité qui menace ou pourrait menacer la sécurité nationale […], toute activité […] qui peut avoir un rapport avec l'espionnage, l'ingérence, le terrorisme, l'extrémisme à propension violente, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, le crime organisé ou la cyber-menace dans la mesure où ces deux derniers sont liés aux activités précitées »*. Il est donc permis de conclure que les missions du SRE, et notamment ses missions de prévention en matière de lutte contre le terrorisme, l'espionnage, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes ou la cyber-menace dans la mesure où elle est liée aux activités précitées, correspondent parfaitement à la finalité définie par le projet de loi sous examen. Le SRE est partant justifié à traiter des données PNR. Le traitement de données PNR par un service de renseignement correspond d'ailleurs aux législations en place des pays européens dans la matière. Par exemple, l'article 14 de la loi belge du 25 décembre 2016 relative au traitement des données des passagers prévoit une UIP composée de la Sûreté de l'Etat visée par la loi organique du 30 novembre 1998 des services de renseignement et de sécurité et du Service général de Renseignement et de Sécurité visé par la loi organique du 30 novembre 1998 organique des services de renseignement et de sécurité.

Par ailleurs, si le Conseil d'Etat approuve le choix de la Police grand-ducale en tant qu'administration de rattachement de l'UIP, il critique le fait que le projet de loi ne donne pas d'indication sur le grade ou la fonction du responsable de l'UIP, ni ne précise s'il doit s'agir d'un membre du personnel du cadre policier ou si un membre du cadre civil de la Police peut également remplir cette tâche de direction. L'alinéa ler a été amendé de manière à préciser que le responsable de l'UIP doit être issu de la catégorie de traitement Al du cadre policier de la Police grand-ducale.

Le Conseil d'Etat comprend l'utilité d'une disposition qui prévoit que les différents services compétents disposent d'un représentant en tant qu' « agent de liaison » au sein de l'UIP. Il a toutefois relevé que la disposition selon laquelle les membres du personnel de l'Administration des douanes et accises (ADA) et du SRE détachés à l'UIP agissent dans les limites des attributions légales de leurs administrations d'origine serait en contradiction avec l'article 7 du statut général des fonctionnaires de l'Etat en vertu duquel les fonctionnaires détachés relèvent entièrement de l'administration auprès de laquelle ils sont détachés et s'est opposé formellement à cette disposition. Le Conseil d'Etat a encore donné à considérer que, du fait de son détachement, le personnel de l'ADA et du SRE ne serait alors plus en droit d'accéder aux données et informations traitées dans son service d'origine et que pour permettre cet accès, dont le Conseil d'Etat ne conteste pas l'utilité, il faudrait prévoir une disposition légale autorisant ces accès et en fixant les conditions et limites.

Le Conseil d'Etat propose deux solutions, la première étant inspirée de la loi belge portant transposition de la directive PNR, la seconde de la Cellule de renseignement financier auprès du parquet de Luxembourg. Le Gouvernement n'entend pas remettre en question la décision de créer l'UIP au sein de la Police, qui résulte d'une consultation des acteurs du terrain concernés. La seconde option suggérée par le Conseil d'Etat n'a dès lors pas été retenue.

Les auteurs des amendements proposent une autre solution, qu'ils pensent être en phase avec notre législation sur la fonction publique et conforme à la directive à transposer. Il importe de préciser dans ce contexte que, si la version française de la Directive parle d'agents détachés, la version allemande utilise les termes *« abgeordnet werden »* et la version anglaise prévoit que *« staff members of a PIU*

may be seconded from competent authorities ». Rien ne s'oppose dès lors, aux yeux des auteurs des amendements, à ce que le Luxembourg opte pour une autre solution que le détachement tel que ce terme est compris dans notre législation nationale. La solution proposée dans le cadre des présents amendements est inspirée de l'article 9, paragraphe 3, de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat qui dispose que *« Les agents du centre peuvent être placés auprès d'un département ministériel ou d'une administration de l'Etat par une décision conjointe du ministre et du ministre du ressort. Dans ce cas, et pendant toute la durée de leur placement, ils continuent de relever de l'autorité hiérarchique du directeur du centre. »* Il ressort du commentaire des articles du projet de loi ayant abouti à la loi précitée du 20 avril 2009 que « *En ce qui concerne le personnel, la seule particularité pour le CTIE est la possibilité de placer certains de ses agents auprès des départements ministériels, administrations ou services de l'Etat sur base d'une décision conjointe des membres du Gouvernement respectifs. Cette mesure est destinée à permettre au CTIE d'envoyer des informaticiens auprès d'autres entités administratives afin de mettre en place et de gérer les systèmes informatiques d'une administration en particulier. Contrairement aux agents détachés, les agents placés par le CTIE continuent de relever de leur autorité hiérarchique d'origine. Ceci est nécessaire en raison du fait qu'ils doivent effectuer leur travail d'après les directives et les critères que le CTIE fixe pour l'ensemble du réseau informatique de l'Etat. (...) Le mécanisme du placement des agents est inspiré de la situation des contrôleurs financiers qui relèvent de l'autorité du Ministre ayant le budget dans ses attributions, mais qui exercent leurs missions auprès des différents départements ministériels.*[1]

Ainsi, le personnel de l'ADA et le personnel du SRE seront désignés à l'UIP comme membres de leurs administrations respectives et agiront comme tels. Cette solution ne remet pas en cause le principe selon lequel l'UIP fonctionne sous forme de « closed box » et que les services désignés comme services compétents n'ont pas un accès direct aux données PNR. Le personnel de l'ADA et du SRE resteront placés sous l'autorité hiérarchique de leur administration d'origine. Pour permettre au responsable de l'UIP d'exercer les responsabilités qui lui incombent en vertu de la présente loi, il aura autorité fonctionnelle sur ce personnel.

Amendement 5

A l'article 5, alinéa 1er, la partie de phrase commençant par *« les données PNR »* et se terminant par *« dont ils disposent »* est remplacée comme suit : *« les données PNR de tous les passagers en provenance de, à destination de ou transitant par le Luxembourg pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien »*.

Motivation

Les données des passagers transitant par le Luxembourg n'ont pas été mentionnées parmi les données à transférer à l'UIP alors que les auteurs du projet de loi estimaient que l'obligation de transférer les données PNR de ces personnes découlait de la lecture combinée de l'article 2, point b, qui vise expressément les passagers en transit et de l'article 5, qui parle des vols au départ et en provenance du Luxembourg. Le texte belge est rédigé dans une autre logique que le présent texte alors qu'il fixe l'obligation de transférer les données non pas par rapport à des vols, mais par rapport aux passagers. C'est dans cette optique que le texte belge mentionne les passagers transitant par son territoire. Le texte luxembourgeois, à l'instar de l'article 8, paragraphe 1er de la directive fixe l'obligation de transfert par rapport aux vols.

Eu égard à l'opposition formelle émise par le Conseil d'Etat pour transposition incomplète de la directive, l'article 5, alinéa 1er a été reformulé de manière à viser expressément les données des passagers transitant par le Luxembourg.

L'article 5 a par ailleurs été amendé afin de tenir compte de l'avis de la Chambre de commerce qui considère que la disposition obligeant les transporteurs aériens à transférer les données PNR *« dont ils disposent »* serait source d'interprétations divergentes et, par conséquent, d'insécurité juridique. Les auteurs des amendements ont repris la formulation de texte suggérée par la Chambre de commerce.

---

1 Projet de loi n° 5912

Amendement 6

L'article 6, paragraphe 1er, est amendé comme suit :

1° A l'alinéa 1er, le point b) est supprimé et le point c) devient le point 2°.

2° A l'alinéa 2, le renvoi au point c) est remplacé par un renvoi au point 2°, le renvoi aux points a) et b) est remplacé par un renvoi au point 1° et les mots *« des transferts visés »* sont remplacés par *« du transfert visé »*.

Motivation

Le Conseil d'Etat a émis une opposition formelle à l'égard de l'article 6 en ce qu'il impose aux transporteurs aériens de communiquer les données à l'UIP à trois échéances précises, alors que la directive à transposer ne prévoit que deux échéances. Ainsi, pour assurer une transposition correcte de la directive, l'article 6 amendé ne prévoit plus que deux transferts, le premier ayant lieu 48 heures avant l'heure de départ programmée du vol et le second immédiatement après la clôture du vol. La disposition selon laquelle le transfert de données PNR après la clôture du vol peut se limiter à une mise à jour du transfert visé à l'alinéa 1er, point 1° est maintenue.

Amendement 7

L'article 7 est amendé comme suit :

1° Au paragraphe 1er, alinéa 1er, le mot « *des* » précédant le mot « protocoles » et le mot « formats » est remplacé par le mot « *de* » et la partie de phrase « *dès leur publication au Journal officiel de l'Union européenne* » est remplacée par « *conformément à l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne* ».

2° Il est ajouté un paragraphe 3 prenant la teneur suivante : « (3) *Dans l'hypothèse où un transporteur aérien ne conserve pas les données API énumérées à l'annexe I, point 18, par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, il transfère également ces données par la méthode « push » à l'UIP. Dans le cas d'un tel transfert, toutes les dispositions de la présente loi s'appliquent à ces données API.* »

Motivation

L'amendement sub 1° vise à tenir compte de l'opposition formelle émise par le Conseil d'Etat à l'égard de la formulation *« dès leur publication au Journal officiel de l'Union européenne »*. Le texte de l'article 7 a été amendé de manière à être conforme à l'article 297, paragraphe 1er, alinéa 3 du TFUE qui dispose que *« les actes législatifs entrent en vigueur à la date qu'ils fixent ou, à défaut, le vingtième jour suivant leur publication »*.

L'amendement sub 2° fait suite à la réserve émise par le Conseil d'Etat à propos de l'obligation imposée aux Etats membres d'adopter des mesures nécessaires afin que les données API visées à l'annexe I soient transférées à l'UIP par des méthodes techniques identiques au transfert des autres données PNR y visées. Au vu de cette réserve, et afin de garantir que toutes les obligations imposées par la directive soient clairement inscrites dans la présente loi, l'article 7 a été précisé en ce sens.

Amendement 8

L'article 10 est amendé comme suit :

1° Au paragraphe 2,' le point a, devenant le point 1°, est remplacé comme suit : *« 1° aux traitements de données à caractère personnel mis en oeuvre par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ; »*.

2° Au paragraphe 5, les mots *« de Luxembourg »* sont remplacés par *« du Grand-Duché de Luxembourg »*.

3° Au paragraphe 6, la référence au règlement 562/2006 du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes est remplacée par une référence au règlement 2016/399 du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen).

Motivation

Le Conseil d'Etat a relevé que les termes *« banques de données »* ne correspondaient pas à la terminologie utilisée dans le cadre juridique national et qu'il y aurait lieu de parler de *« traitement des données »*.

L'accès aux traitements de données à caractère personnel visés au paragraphe 2, point 1°, a lieu selon les conditions applicables aux traitements de données respectifs.

Les amendements sub 2 et 3 ne suscitent pas de commentaire particulier.

Amendement 9

L'article 13 est remplacé comme suit :

*« **Art. 13.** Sont habilités à demander à l'UIP ou à recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, en vue de procéder à un examen approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et poursuites en la matière:*

1° la Police grand-ducale ;

2° le Service de renseignement de l'Etat conformément à l'article 5, paragraphe 4, de la loi du 5 juillet 2016 portant réorganisation du service de renseignement de l'Etat ;

3° l'Administration des douanes et accises.

En recherchant les crimes et délits visés à l'article 2, points 8° et 9°, le procureur d'Etat peut, par une décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 12.

Motivation

Le premier alinéa de l'article 13 a été reformulé afin de tenir compte de l'opposition formelle émise par le Conseil d'Etat en raison de la transposition incorrecte de l'article 7, paragraphe ler de la directive. Compte tenu de cette opposition formelle et des critiques émises par le Parquet général et la Cour supérieure de justice en ce qui concerne la formulation *« dans la limite du besoin d'en connaître »* qu'ils considèrent comme trop imprécise, le texte de l'article 7, paragraphe 1er de la directive a été repris à l'article 13.

Par ailleurs, la lettre b), devenant le point 2° a été complété sur base de la proposition du Conseil d'Etat formulée dans le cadre de l'examen de l'amendement 2 du 27 février 2018 (art. 39 du projet de loi amendé).

Il est par ailleurs ajouté un deuxième alinéa qui tient compte des avis du Conseil d'Etat et du Parquet général en ce qu'ils proposent d'introduire dans le cadre juridique national, à l'instar de la loi belge ayant transposé la directive PNR, un accès simplifié des procureurs d'Etat aux données PNR détenues par l'UIP en leur évitant d'avoir à saisir le juge d'instruction. Dans la mesure où cette disposition ne vise que les données PNR, les auteurs des amendements estiment que la disposition afférente trouve mieux sa place dans la présente loi que dans la Code de procédure pénale. Il importe de préciser dans ce contexte que, comme l'a d'ailleurs relevé le Conseil d'Etat, la décision du procureur d'Etat, à l'instar de tout autre acte d'enquête, est susceptible du recours prévu à l'article 48-2 du code de procédure pénale.

Amendement 10

A l'article 15 est ajouté un alinéa 2 qui prend la teneur suivante *« Les décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peuvent pas être fondées sur 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. »*

Motivation

L'amendement fait suite à l'opposition formelle du Conseil d'Etat qui estime que, même si l'article 8 du projet de loi interdit le traitement des données sensibles y visées, l'interdiction de prendre des décisions qui seraient basées sur de telles données, si celles-ci avaient néanmoins été collectées, doit être inscrite dans la loi.

Amendement 11

L'article 17, paragraphe 1er est amendé comme suit :

1° A l'alinéa 3, les mots *« procureur d'Etat de Luxembourg »* sont remplacés par les mots *« procureur général d'Etat »*.

2° Il est ajouté un alinéa 4 libellé comme suit : *« Les dispositions du présent paragraphe ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale. »*

Motivation

L'amendement sub 1 fait suite aux avis du Conseil d'Etat et du Parquet général qui donnent à considérer que le Procureur général d'État est traditionnellement l'autorité centrale pour tous les instruments relatifs à l'entraide judiciaire, et que dans le cadre de la loi du 17 mai 2017 portant approbation de l'Accord entre le gouvernement du Grand-Duché de Luxembourg et les États-Unis aux fins de renforcer la coopération en matière de prévention et de lutte contre le crime grave signé en date du 3 février 2012, la transmission de certaines données a été soumise à l'autorisation du Procureur général d'État.

Conformément à ces avis, le procureur général d'Etat ou son délégué sera compétent pour autoriser la transmission des données dépersonnalisées par masquage.

L'amendement sub 2 est à voir en relation avec la question, soulevée par le Parquet général à propos de l'article 21 réglant le transfert de données PNR à des Etats non membres de l'Union européenne, de savoir si cet échange échapperait aux dispositions traditionnelles de l'entraide judiciaire. Afin de dissiper toute incertitude à cet égard, une précision afférente a été apportée non seulement en ce qui concerne les échanges de données PNR avec des pays tiers, mais également l'échange de telles données avec d'autres Etats membres.

Amendement 12

La deuxième phrase de l'article 18, alinéa 1er, est supprimée.

Motivation

Le Conseil d'Etat a estimé que la deuxième phrase de l'alinéa 1er n'avait pas de valeur normative et en a demandé la suppression.

Amendement 13

A l'article 19, l'adjectif *« policière »* est supprimé, le mot *« autorités »* est remplacé par le mot *« services »* et l'adjectif *« compétent »* est mis au masculin pluriel.

Amendement 14

L'article 21 est amendé comme suit :

1° La partie de phrase *« Sans préjudice des dispositions de l'article 35, paragraphe (1), point (d), et des articles 36 à 38 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale »* est supprimée et la lettre « I » précédant l'acronyme « UIP » prend une majuscule.

2° Il est ajouté un nouveau point 1 libellé comme suit : *« 1° l'une des conditions prévues à l'article 35, paragraphe 1er, point d) de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est remplie ; »*. Les points suivants sont renumérotés en conséquence.

3° Il est ajouté un alinéa 2 ayant la teneur suivante : *« Les dispositions du présent article ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale. »*

Motivation

L'amendement sub 1° est destiné à clarifier le texte en ce qu'il énonce, parmi les conditions à respecter, celles prévues à l'article 35, paragraphe 1er, point d) de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, à savoir que la Commission européenne doit avoir adopté une décision d'adéquation ou, en l'absence d'une telle décision, que des garanties appropriées ont été prévues ou existent ou, en l'absence de décision d'adéquation et de garanties appropriées, que des dérogations pour des situations particulières s'appliquent. Afin de ne pas surcharger la présente loi avec des dispositions figurant déjà dans une autre loi, les auteurs des amendements ont préféré faire un renvoi à la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, plutôt

que de reprendre le texte de l'article 35, paragraphe 1er, point d, de cette loi ainsi que le texte des articles 36, 37 et 38 auxquels l'article 35, paragraphe 1er, point d) renvoit.

Pour le surplus il est renvoyé au commentaire de l'amendement 11.

Amendement 15

A l'article 22, paragraphe 2, l'expression *« ex post »* est remplacée par *« a posteriori »*.

Amendement 16

A l'article 23, la partie de phrase *« que dans les conditions compatibles avec la présente loi et après »* sont remplacés par *« qu'après »* et le mot *« ces »* précédant le mot *« conditions »* est remplacé par le mot *« les »*. Après le mot *« garanties »* sont ajoutés les mots *« de la présente loi »*.

Motivation

Au vu des interrogations soulevées par le Conseil d'Etat par rapport à la formulation *« que dans les conditions compatibles avec la présente loi »*, qu'il considère au demeurant comme dépourvue de valeur normative, et considérant que les conditions du transfert sont à suffisance réglées par les articles 21 et 22, l'article 23 a été amendé de manière à n'ajouter comme condition supplémentaire par rapport aux conditions fixées aux articles 21 et 22 que celle d'avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données respecte les conditions et garanties de la présente loi.

Amendement 17

A l'article 24 entre le terme *« données »* et les termes *« est informé »* sont insérés les termes *« visé à l'article 29 »*.

Motivation

Vu que le délégué à la protection des données n'apparaît une première fois qu'à l'article 29, le Conseil d'Etat a suggéré de compléter l'article 24 par un renvoi à l'article 29 afin d'améliorer la lisibilité du texte.

Amendement 18

A l'article 26, paragraphe 2, les mots *« procureur d'Etat de Luxembourg »* sont remplacés par *« procureur général d'Etat »*.

Motivation

Pour la motivation de cet amendement il est renvoyé à la motivation de l'amendement 11.

Amendement 19

A l'article 27, les guillemets entourant le mot *« fausses »* sont supprimés.

Amendement 20

L'article 28 est remplacé comme suit : *« **Art. 28.** L'autorité de contrôle visée à l'article 40 de la loi du jj/mm/aaaa jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 10 de la loi du jj/mm/aaaa portant création de la Commission nationale pour la protection des données et du régime général sur la protection des données et elle dispose, à cette fin, des pouvoirs prévus à l'article 16 de la même loi. »*

Motivation

Le Conseil d'Etat considère que l'article 28 transpose incorrectement la directive en ce qu'il retient le principe de la compétence de la CNPD et l'application du régime général sur la protection des données.

Le texte a été reformulé pour tenir compte de l'opposition formelle du Conseil d'Etat. Ainsi, au lieu de faire référence au régime général, il est fait référence aux dispositions pertinentes de la loi portant

transposition de la directive sur la protection des données en matière pénale. Dans la mesure où cette loi désigne la CNPD comme autorité compétente pour contrôler les traitements des données en matière pénale autres que ceux effectués par les juridictions de jugement, ce sera également la CNPD qui sera compétente pour contrôler le traitement des données PNR. Etant donné que les missions et les pouvoirs de cette commission sont définis par la loi portant sur le régime général, il est renvoyé à cette loi pour ce qui est des missions et des pouvoirs de la CNPD.

Amendement 21

L'article 29 est amendé comme suit :

1° Au paragraphe 1er, alinéa 2, la formulation *« en particulier »* et les virgules précédant et suivant cette formulation sont supprimées.

2° Les mots « Directeur » et « Ministre » figurant au paragraphe 3 prennent une minuscule.

3° Au paragraphe 4, alinéa 2, après les mots *« Commission nationale pour la protection des données »* sont ajoutés les mots *«conformément à la loi du jj/mm/aaaa relative à la création de la Commission nationale pour la protection des données et au régime général sur la protection des données »*.

Motivation

L'amendement sub 1 ne suscite pas de commentaire particulier.

L'ajout au paragraphe 4, alinéa 2 fait suite à une proposition du Conseil d'Etat et vise à préciser les bases légales permettant la saisine de la CNPD.

Amendement 22

A l'article 32, les mots *« Grand-Duché de »* sont insérés entre le mot *« du »* et le mot *« Luxembourg »*.

Amendement 23

A l'article 34, alinéa 2, les premières lettres suivant les points d'énumération prennent à chaque fois une minuscule.

Amendement 24

A l'article 36, les mots *« l'autorité de contrôle »* sont remplacés par *« la Commission nationale pour la protection des données »*.

Motivation

Le Conseil d'Etat a proposé de désigner la CNPD dans le texte au lieu de parler de l'autorité de contrôle.

Amendement 25

L'article 37, alinéa 1er est remplacé comme suit : *« **Art. 37.** La violation intentionnelle de l'article 8, alinéa 1er et de l'article 15 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125 000 euros ou d'une de ces peines seulement. La juridiction saisie prononce la cessation du traitement contraire aux dispositions de l'article 8, alinéa 1er et de l'article 15 sous peine d'astreinte dont le maximum est fixé par ladite juridiction. »*

Motivation

L'article 37, dans sa version initiale, prévoyait des sanctions pénales en cas de violation des articles 8, 15 et 36.

L'article 8 interdit le traitement de données PNR qui révèlent 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 et oblige l'UIP à effacer de telles données dès réception et de façon définitive. Le Conseil d'Etat a critiqué le fait que l'article 37 ne précise pas lequel des deux comportements visés à l'article 8 est sanctionné, le traitement illicite ou le défaut d'effacement ou les deux. Il a en outre exigé qu'il soit précisé s'il s'agit d'une infraction intentionnelle ou si le simple fait de procéder à un tel traitement est suffisant pour encourir la peine prévue par la loi, en donnant à considérer qu'un simple dysfonctionnement au sein de l'unité, dépourvu

de toute intention criminelle, qui serait éventuellement sanctionnable disciplinairement, ne serait pas de nature à entraîner la responsabilité pénale du responsable de l'UIP ou du fonctionnaire à l'origine du traitement.

Le Parquet général estime que la violation de l'article 8 relatif à l'interdiction de révéler 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 peut se concevoir en tant qu'infraction pénale, à condition cependant qu'il y ait intention délictuelle.

Les Parquets de Luxembourg et de Diekirch considèrent que la loi devrait fixer un délai maximal endéans lequel ces données devraient être effacées.

Compte tenu des avis du Conseil d'Etat et du Parquet général, l'article 37 a été reformulé de manière à préciser que constitue une infraction pénale la violation intentionnelle de l'interdiction de traiter des données sensibles prévue à l'article 8 de la présente loi. La demande des Parquets de Luxembourg et de Diekirch de fixer un délai maximal pour l'effacement des données n'a pas été retenue étant donné que les auteurs des amendements craignent qu'en fixant un délai pour ce faire, alors que la directive fait obligation d'effacer ces données immédiatement, il existe le risque que la Commission européenne considère que la législation luxembourgeoise ne serait sur ce point pas conforme à la directive.

Le Conseil d'Etat a suggéré d'inclure l'article 9 parmi les comportements pouvant entraîner une sanction pénale au motif que le défaut par l'UIP d'effacer les données autres que celles énumérées à l'annexe I viserait un comportement similaire au défaut d'effacement des données sensibles qui, pourtant, est sanctionné pénalement. Cette suggestion n'a pas été suivie étant donné que le défaut d'effacement des données sensibles a été retiré parmi les faits sanctionnables pénalement. Dès lors, au vu des arguments invoqués par le Conseil d'Etat pour assortir d'une sanction pénale une violation de l'article 9, l'ajout de l'article 9 parmi les faits constituant une infraction pénale ne ferait pas de sens.

Le fait de prendre une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR (art. 15) reste assorti d'une sanction pénale, mais suite aux questions soulevées par le Conseil d'Etat et le Parquet général, il a été précisé que la violation de cette disposition doit être intentionnelle. A également été érigé en infraction pénale le fait de prendre une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative qui serait fondée sur 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.

L'article 36 qui impose à l'UIP d'informer sans retard injustifié la personne concernée et la Commission nationale pour la protection des données lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, a été retirée de la liste des infractions pénales au vu des considérations émises par le Conseil d'Etat en relation avec les problèmes matériels auxquels l'UIP peut se voir confrontée pour toucher la personne concernée.

Par ailleurs, la seconde phrase de l'article 37, alinéa 1er qui fait référence aux dispositions du *« présent alinéa »* a été reformulée pour répondre aux critiques du Conseil d'Etat et des Parquets de Luxembourg et Diekirch que le traitement ne devrait pas être contraire aux dispositions de l'article 37, mais aux dispositions des articles auxquels l'article 37 fait référence.

Il a par ailleurs été tenu compte des avis du Conseil d'Etat et des Parquets de Luxembourg et de Diekirch d'après lesquels la cessation du traitement illégal ne devrait pas être une faculté, mais une obligation pour la juridiction de jugement.

Il importe finalement de remarquer que le paragraphe 2 de l'article 49 du projet de loi n°7168, qui prévoit des sanctions pénales en cas de violation des articles 10, 11 et 30 dudit projet de loi n'est pas applicable en matière de données PNR étant donné que l'article 37 du projet de loi PNR ne renvoit dans son alinéa 2 qu'aux paragraphes 1er, 3 et 5 du projet de loi n° 7168. Les auteurs des amendements ne partagent dès lors pas la crainte soulevée par le Conseil d'Etat par rapport à une éventuelle incohérence entre les dispositions pénales mises en place par les deux textes.

Amendement 26

L'article 38 est amendé comme suit :

1° Au paragraphe 1er, le point séparant les tranches de mille euros est supprimé et ces tranches sont séparées par une espace insécable et la partie de phrase *« renseignements y visés »* est remplacée par *« renseignements visés à l'article 3 »*.

2° Au paragraphe 2, alinéa 3, le mot « M*inistre* » est écrit avec une minuscule.

Motivation

La reformulation visée au point 1 est reprise de l'avis de la Chambre de commerce qui estime que la disposition telle que formulée ne permettait pas de déterminer avec précision quel comportement est susceptible de faire l'objet d'une amende.

Le Conseil d'Etat s'est interrogé sur les raisons pour lesquelles le présent loi prévoit une amende dont le maximum est le décuple des amendes prévues par l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration à l'encontre des entreprises de transport qui ne respectent pas les obligations leur imposées par l'article 106 de la même loi alors que les faits incriminés par les deux textes seraient identiques sur tous les points. Le Conseil d'Etat a réservé sa position quant à la dispense du second vote en attendant de recevoir des explications sur cette différence de traitement.

La sanction à laquelle fait référence le Conseil d'Etat a été introduite par la loi du 21 décembre 2006 portant transposition, entre autres, de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (« directive API »). S'il est partant vrai que la loi de transposition de la directive API et le projet de loi de transposition de la directive PNR prévoient tous les deux des sanctions administratives à l'encontre des transporteurs aériens qui ne transfèrent pas les données ou ne les transfèrent pas selon les conditions requises, la différence fondamentale entre les deux textes, et qui d'après les auteurs du projet de loi PNR justifie la différence au niveau des sanctions encourues, réside dans la finalité pour laquelle les données des passagers sont recueillies. Ainsi, l'objectif de la directive API consiste, tel qu'il ressort de son article 1er, à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine. Les données API sont des informations biographiques extraites de la partie du passeport lisible par machine et servent d'outils de vérification des identités et de gestion aux frontières. Ces données ne présentent pas d'intérêt pour l'évaluation des personnes ni pour le dépistage des délinquants ou terroristes «inconnus». En effet, *« une utilisation à la fois proactive et en temps réel des données PNR permet donc aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent, par rapport à ce que permet le traitement d'autres catégories de données à caractère personnel. Comme expliqué ci-dessous, le traitement de données à caractère personnel accessibles aux services répressifs dans le cadre d'instruments de l'UE actuels et futurs, tels que la directive relative aux informations préalables sur les passagers, le système d'information Schengen (SIS) et le système d'information Schengen de deuxième génération (SIS II), ne donne pas aux services répressifs la possibilité d'identifier des suspects «inconnus» comme le permet l'analyse de données PNR. Deuxièmement, après la commission d'une infraction, les données PNR aident les services répressifs à prévenir et à détecter d'autres infractions graves, dont des actes de terrorisme, et à enquêter sur celles-ci et à poursuivre leurs auteurs. À cet effet, les services répressifs doivent utiliser les données PNR en temps réel, pour les confronter à diverses bases de données de personnes «connues» et d'objets recherchés. Ils doivent également en faire un usage réactif, pour rassembler des preuves et, au besoin, trouver d'éventuels complices et démanteler des réseaux criminels. »*[2]

Les données PNR sont recueillies pour une finalité complètement différente, à savoir qu'ils constituent un moyen de prévention et de lutte contre le terrorisme et les formes graves de criminalité telles que la traite des êtres humains, l'exploitation sexuelle des enfants, le trafic d'armes, le vol organisé ou l'aide à l'entrée et le séjour irréguliers. Cette dernière infraction illustre d'ailleurs très bien la différence entre les finalités des traitements des données API et des données PNR. Ainsi, si la directive API vise à prévenir l'immigration illégale, qui ne constitue pas une infraction pénale, la directive PNR crée des moyens destinés à protéger la sécurité et la vie des personnes. Il n'y a aucun doute que les conséquences

2 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 (COM/2011/0032 final)

d'un défaut de transmission de données à des fins de contrôle des frontières ne sont pas les mêmes qu'un défaut de transmission de données qui peuvent permettre de prévenir une attaque terroriste ou un autre crime grave. La différence entre les sanctions encourues dans les deux cas de figure est dès lors justifiée.

Il importe par ailleurs de relever que l'article 14 de la directive PNR oblige les Etats membres à prévoir des sanctions effectives, proportionnées et dissuasives à l'encontre des transporteurs aériens qui ne transmettent pas les données comme le prévoit l'article 8 ou ne les transmettent pas dans le format requis. Comme il a été expliqué dans le commentaire de l'article 38, les auteurs du texte se sont alignés sur les montant des amendes fixées dans d'autres Etats membres, notamment la France, la Belgique et l'Allemagne. Il est à craindre que si le Luxembourg alignait la sanction encourue par le transporteur aérien qui omet de transférer les données PNR sur la sanction prévue par la loi précitée de 2008 sur l'immigration, la Commission européenne risquerait de considérer la sanction prévue dans le présent projet de loi comme ne remplissant pas les exigences posées par l'article 14 de la Directive.

Amendement 27

L'article 39 est amendé comme suit :

Au paragraphe 4, alinéa 1er, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, une virgule est insérée entre les termes *« y afférentes »* et *« ou »* et après les termes *« l'article 12 »* et la formulation *« dans la mesure où elle »* est remplacée par *« dans la mesure où celle-ci »*.

A l'alinéa 2, le chiffre *« six »* est supprimé, de sorte qu'il y a lieu de lire *« tous les mois »*.

Motivation

Le Conseil d'Etat s'est opposé formellement à la disposition du nouveau paragraphe 4 en ce qu'elle ne prévoit qu'un rapport semestriel, alors que le même article 5 prévoit dans son paragraphe 3 un rapport mensuel pour les observations et les inspections dans les lieux publics. Le Conseil d'Etat considère qu'un rapport tous les six mois était insuffisant et contrevenait à l'article 8 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales et à l'article 11, paragraphe 3 de la Constitution. Aussi, le texte a été amendé de manière à prévoir un rapport mensuel.

Amendement 28

A l'article 40, la partie de phrase *« le point a) est supprimé »* est remplacée par *« la lettre a) est supprimée »*.

Amendement 29

Il est ajouté un nouveau chapitre 13, intitulé *« Chapitre 13 – Disposition finale »* et un article 41 qui prend la teneur suivante : *« **Art. 41.** La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « Loi du jj/mm/aaaa relative au traitement des données des dossiers passagers»*.

Motivation

Cet amendement ne suscite pas de commentaire particulier.

*

TEXTE COORDONNE

PROJET DE LOI

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave, et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

Chapitre 1er – *Dispositions générales*

Art. 1er. La présente loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Art. 2. Pour l'application de la présente loi, on entend par :

1° «transporteur aérien» : toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes ;

2° «passager» : toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers ;

3° «dossier passager» : le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités ;

4° « système de réservation» : le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations ;

5° « système de contrôle des départs » : le système utilisé pour contrôler les passagers lors de l'embarquement ;

6° « données PNR» : les données contenues dans le dossier passager et énumérées à l'annexe I ;

7° «méthode push» : la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'informations passagers créée à l'article 3 de la présente loi;

8° «infractions terroristes» : les infractions visées au Livre II, Titre 1 Chapitre III-1 du Code pénal ;

9° «formes graves de criminalité» : les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans ;

10° «dépersonnaliser par le masquage d'éléments des données» : rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée ;

11° « services compétents » : les services visés à l'article 13 de la présente loi

Chapitre 2 – *Unité d'informations passagers*

Art. 3. Il est créé au sein de la Police grand-ducale une Unité d'informations passagers, ci-après désignée « UIP », qui est chargée :

1° de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données ;

2° du transfert de ces données et des résultats de leur traitement aux services compétents ;

3° de l'échange de ces données et des résultats de leur traitement avec les unités d'informations passagers des autres Etats membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4. (1) Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Il est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

(2) Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel de l'Administration des douanes et accises et du Service de renseignement de l'Etat. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Les membres du personnel de l'Administration des douanes et accises et du Service de renseignement de l'Etat sont désignés à l'UIP par une décision conjointe du ministre ayant la Police grand-ducale dans ses attributions et du ministre du ressort. Ils continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Art. 5. Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la méthode push, les données PNR de tous les passagers en provenance de, à destination de ou transitant par le Luxembourg pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien.

Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR incombe au transporteur aérien qui assure le vol.

Art. 6. (1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes:

1° 48 heures avant l'heure de départ programmée du vol ;

2° 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 qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point 2°, peut se limiter à une mise à jour du transfert visé à l'alinéa 1er, point 1°.

(2) Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP peut demander, au cas par cas, le transfert de données PNR en dehors des délais prévus au paragraphe 1er.

Art. 7. (1) Les données PNR sont transférées à l'UIP par voie électronique au moyen de protocoles communs et de formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la Directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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. Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg conformément à l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne.

Les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisés pour leurs transferts.

(2) En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union européenne en matière de protection des données soit pleinement respecté.

(3) Dans l'hypothèse où un transporteur aérien ne conserve pas les données API énumérées à l'annexe I, point 18, par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, il transfère également ces données par la méthode « push » à l'UIP. Dans le cas d'un tel transfert, toutes les dispositions de la présente loi s'appliquent à ces données API.

Chapitre 4 – *Traitement des données PNR*

Art. 8. Le traitement de données PNR qui révèlent 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 est interdit.

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive.

Art. 9. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données supplémentaires dès réception et de façon définitive.

Art. 10. (1) L'UIP traite les données PNR en vue de réaliser une évaluation des passagers avant leur arrivée prévue sur le territoire national ou leur départ prévu du territoire national afin d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis compte tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

(2) Pour réaliser cette évaluation l'UIP peut comparer les données PNR :

1° aux traitements de données à caractère personnel mis en oeuvre par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;

2° à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur 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.

(3) L'UIP réexamine individuellement, par des moyens non automatisés, toute concordance positive obtenue à la suite d'un traitement automatisé des données PNR effectué en vertu du présent article.

(4) L'UIP transmet aux services compétents, au cas par cas, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au présent article ou le résultat du traitement de ces données.

(5) Les conséquences de l'évaluation des passagers ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union européenne à la libre circulation sur le territoire du Grand-Duché de Luxembourg tel que prévu par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.

(6) Lorsque les évaluations sont réalisées pour des vols entre le Luxembourg et un autre Etat membre de l'Union européenne auquel s'applique le règlement 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), les conséquences de ces évaluations doivent respecter ledit règlement.

Art. 11. L'UIP traite les données PNR afin de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations visées à l'article 10.

Art. 12. L'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, dûment motivées et fondées sur des motifs suffisants visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques aux fins visées à l'article 1er, et visant à communiquer aux services compétents ou, le cas échéant, à Europol, le résultat de ce traitement.

Chapitre 5 – *Services compétents*

Art. 13. Sont habilités à demander à l'UIP ou à recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, en vue de procéder à un examen approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et poursuites en la matière:

a) 1° la Police grand-ducale ;

b) 2° le Service de renseignement de l'Etat conformément à l'article 5, paragraphe 4, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat ;

c) 3° l'Administration des douanes et accises.

En recherchant les crimes et délits visés à l'article 2, points 8° et 9°, le procureur d'Etat peut, par une décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 12.

Art. 14. Les services compétents ne peuvent traiter les données PNR et le résultat du traitement de ces données que pour les finalités de la présente loi telles que définies à l'article 1er.

L'alinéa 1er est sans préjudice des compétences de la Police grand-ducale et de l'Administration des douanes et accises lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement.

Art. 15. Les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Les décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peuvent pas être fondées sur 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.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Art. 16. Lorsqu'une personne est identifiée conformément à l'article 10, l'UIP communique toutes les données pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP des autres Etats membres de l'Union européenne concernés.

Lorsque l'UIP est destinataire d'informations telles que visées à l'alinéa 1er de la part d'une autre UIP, elle transmet ces informations aux services compétents.

Art. 17. (1) L'UIP transmet, dès que possible, à l'UIP d'un autre Etat membre de l'Union européenne qui en fait la demande, les données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par masquage conformément à l'article 26, et, si nécessaire, le résultat de tout traitement de ces données, s'il a déjà été réalisé conformément à l'article 10.

La demande, dûment motivée, peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière.

Si les données demandées ont été dépersonnalisées par masquage conformément à l'article 26, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que le transfert est nécessaire aux fins visées à l'article 12 et si elle y est autorisée par le procureur général d'Etat ou son délégué.

Les dispositions du présent paragraphe ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

(2) Dans des cas d'urgence, les autorités compétentes des autres Etats membres, désignées conformément à l'article 7, paragraphe 1er de la Directive (UE) 2016/661 du Parlement européen et du Conseil du 27 avril 2016 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 et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe 1er sont applicables.

(3) À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP

d'un État membre a le droit de demander à ce que l'UIP obtienne des données PNR conformément à l'article 6, paragraphe 2, et les communique à l'UIP requérante.

Art. 18. L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres Etats membres de l'Union européenne des données PNR ou les résultats du traitement de ces données. Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre Etat membre de l'Union européenne, il transmet copie de sa demande à l'UIP.

Art. 19. L'échange de données effectué en application du présent chapitre peut avoir lieu par l'intermédiaire de tous les canaux de coopération existant entre les services compétents des Etats membres de l'Union européenne.

La langue utilisée pour la demande et l'échange des données est celle applicable au canal utilisé.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Art. 20. (1) Dans les limites de ses compétences et pour l'accomplissement de ses missions, Europol peut présenter à l'UIP, au cas par cas, par l'intermédiaire de son unité nationale, une demande électronique dûment motivée visant à obtenir des données PNR spécifiques ou le résultat du traitement de ces données :

1° lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des Etats membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes dans la matière et ;

2° dans la mesure où ladite infraction relève de la compétence d'Europol.

(2) La demande énonce les motifs sur lesquels s'appuie Europol pour estimer que la transmission de données PNR ou du résultat de traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée ou à des enquêtes en la matière.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Art. 21. L'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si :

a) 1° l'une des conditions prévues à l'article 35, paragraphe 1er, point d) de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est remplie ;

2° l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité ;

3° le transfert est nécessaire aux fins telles que définies à l'article 1er;

4° le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er;

5° les conditions prévues à l'article 17, paragraphe 1er sont remplies.

Les dispositions du présent article ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

Art. 22. (1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre Etat membre de l'Union européenne à un pays non membre de l'Union européenne que si l'Etat membre auprès duquel les données ont été collectées a donné son accord au transfert.

(2) Dans des circonstances exceptionnelles, les données PNR peuvent être transférées à un pays non membre de l'Union européenne sans l'accord du pays membre de l'Union européenne auprès duquel les données ont été collectées si les conditions suivantes sont remplies :

1° 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 Etat membre de l'Union européenne ou un pays tiers ;

2° l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'Etat membre de l'Union européenne, qui n'a pas pu donner son accord en temps utile, est informée sans retard et le transfert est dûment enregistré et soumis à une vérification a posteriori.

Art. 23. L'UIP ne peut transférer des données PNR et les résultats du traitement de ces données aux autorités compétentes de pays non membres de l'Union européennequ'après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte les conditions et garanties de la présente loi.

Art. 24. Le délégué à la protection des données visé à l'article 29 est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Art. 25. L'UIP conserve les données PNR pendant une durée maximale de cinq ans à compter du transfert par le transporteur aérien.

A l'issue de cette période de cinq ans, elle efface les données PNR de manière définitive. Cette disposition ne s'applique pas si les données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière.

Art. 26. (1) À l'expiration d'une période de six mois à compter du transfert par le transporteur aérien, l'UIP dépersonnalise les données PNR par le masquage des éléments suivants :

1° le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR ;

2° l'adresse et les coordonnées ;

3° des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne ;

4° les informations «grands voyageurs» ;

5° les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte ;

6° toute donnée API qui a été recueillie.

(2) À l'expiration de la période de six mois visée au paragraphe (1), la communication de l'intégralité des données PNR n'est autorisée que sous les conditions suivantes :

1° elle est nécessaire aux fins visées à l'article 12 ;

2° elle a été approuvée par le procureur général d'Etat ou son délégué ou, si les données sont destinées à être communiquées au Service de renseignement de l'Etat, par la commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Art. 27. L'UIP ne conserve le résultat de l'évaluation réalisée en vertu de l'article 10 que le temps nécessaire pour informer les services compétents et, s'il y a lieu, les UIP des autres États membres de l'Union européenne de l'existence d'une concordance positive.

Lorsque, à la suite du réexamen individuel par des moyens non automatisés conformément à l'article 10, paragraphe 3, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées en vertu de l'article 25, de manière à éviter de futures fausses concordances positives.

Chapitre 10 – *Protection des données à caractère personnel*

Art. 28. L'autorité de contrôle visée à l'article 40 de la loi du jj/mm/aaaa jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est compétente pour contrôler et vérifier le respect des

dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 10 de la loi du *jj/mm/aaaa* portant création de la Commission nationale pour la protection des données et du régime général sur la protection des données et elle dispose, à cette fin, des pouvoirs prévus à l'article 16 de la même loi.

Art. 29. (1) Le responsable de l'UIP désigne un délégué à la protection des données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

(2) Le délégué à la protection des données contrôle le traitement des données PNR et met en oeuvre les garanties pertinentes au sein de l'UIP.

Il informe et conseille le responsable et le personnel de l'UIP sur les obligations qui leur incombent en matière de protection des données.

Il fait office de point de contact pour les personnes concernées pour toutes les questions relatives au traitement de leurs données PNR et pour la Commission nationale pour la protection des données.

(3) Le délégué à la protection des données effectue ses missions en toute indépendance.

Il fait directement rapport au responsable de l'UIP.

Par dérogation à l'alinéa 2, et sans préjudice du paragraphe (4), alinéa 2, en cas de problèmes relevant de la protection des données, le délégué à la protection des données rapporte directement au directeur général de la Police grand-ducale ou, s'il juge nécessaire, au ministre ayant la Police grand-ducale dans ses attributions.

(4) Le délégué à la protection des données a accès à toutes les données traitées par l'UIP.

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données conformément à la loi du jj/mm/aaaa relative à la création de la Commission nationale pour la protection des données et au régime général sur la protection des données.

Art. 30. L'UIP met à la disposition du public, par les moyens de communication appropriés, les informations suivantes :

1° ses coordonnées ;

2° les coordonnées du délégué à la protection des données ;

3° les finalités du traitement auquel sont destinées les données PNR ;

4° le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité ;

5° l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31. (1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 14 à 18 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 45 à 48 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 32. L'UIP conserve, traite et analyse les données PNR en un ou des endroits sécurisés situés sur le territoire du Grand-Duché de Luxembourg.

Art. 33. Le responsable de l'UIP met en oeuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et la nature des données PNR.

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en oeuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 29, paragraphe 2 de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 34. L'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

Cette documentation comprend :

1° le nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès ;

2° les demandes formulées par les services compétents et les UIP des autres Etats membres de l'Union européenne ;

3° toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Art. 35. L'UIP tient des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

Les registres des opérations de consultation et de communication indiquent la finalité, la date et l'heure de l'opération et l'identité de la personne qui a consulté ou communiqué les données PNR ainsi que l'identité des destinataires de ces données.

Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit.

L'UIP met les registres à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Les registres sont conservés pendant cinq ans.

Art. 36. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe sans retard injustifié la personne concernée et la Commission nationale pour la protection des données de cette atteinte.

Chapitre 11 – *Sanctions*

Art. 37. La violation intentionnelle de l'article 8, alinéa 1er et de l'article 15et est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125 000 euros ou d'une de ces peines seulement. La juridiction saisie prononce la cessation du traitement contraire aux dispositions de l'article 8, alinéa 1er et de l'article 15 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 49, paragraphe 1er et paragraphes 3 à 5 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38. (1) Est puni d'une amende d'un montant maximum de 50 000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements visés à l'article 3, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

(2) Le manquement est constaté par un procès-verbal établi par la Police grand-ducale. Copie en est transmise au transporteur aérien.

Le transporteur aérien a accès au dossier et est mis à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction.

L'amende est prononcée par le ministre ayant la Police grand-ducale dans ses attributions.

(3) La décision du ministre qui est motivée est susceptible d'un recours en réformation à introduire devant le Tribunal administratif dans un délai d'un mois à compter de la notification.

Chapitre 12 – *Dispositions modificatives*

Art. 39. Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

«(4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, ou de cyber-menace dans la mesure où celle-ci est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12, de la loi du jj.mm.aaaa relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Le directeur du SRE rapporte tous les mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en oeuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Art. 40. A l'article 8, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, I la lettre a) est supprimée.

Chapitre 13 – *Disposition finale*

Art. 41. La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : *« Loi du jj/mm/aaaa relative au traitement des données des dossiers passagers»*.

*

ANNEXE I

Liste des données PNR

1° Code repère du dossier passager ;
2° Date de réservation/d'émission du billet ;
3° Date(s) prévue(s) du voyage ;
4° Nom(s);
5° Adresse et coordonnées (numéro de téléphone, adresse électronique) ;
6° Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation ;
7° Itinéraire complet pour le PNR concerné ;
8° Informations «grands voyageurs» ;
9° Agence de voyages/agent de voyages ;
10° Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation ;
11° Indications concernant la scission/division du PNR ;
12° Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée);

13° Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix ;

14° Numéro du siège et autres informations concernant le siège ;

15° Informations sur le partage de code ;

16° Toutes les informations relatives aux bagages ;

17° Nombre et autres noms de voyageurs figurant dans le PNR ;

18° Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée) ;

19° Historique complet des modifications des données PNR énumérées aux points 1 à 18.

*

ANNEXE II

Liste des infractions visées à l'article 2, point (i)

1° Participation à une organisation criminelle ;

2° Traite des êtres humains ;

3° Exploitation sexuelle des enfants et pédopornographie ;

4° Trafic de stupéfiants et de substances psychotropes ;

5° Trafic d'armes, de munitions et d'explosifs ;

6° Corruption ;

7° Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union ;

8° Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro ;

9° Cybercriminalité ;

10° Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées ;

11° Aide à l'entrée et au séjour irréguliers ;

12° Meurtre, coups et blessures graves ;

13° Trafic d'organes et de tissus humains ;

14° Enlèvement, séquestration et prise d'otage ;

15° Vol organisé ou vol à main armée ;

16° Trafic de biens culturels, y compris d'antiquités et d'oeuvres d'art ;

17° Contrefaçon et piratage de produits ;

18° Falsification de documents administratifs et trafic de faux ;

19° Trafic de substances hormonales et d'autres facteurs de croissance ;

20° Trafic de matières nucléaires et radioactives ;

21° Viol ;

22° Infractions graves relevant de la Cour pénale internationale ;

23° Détournement d'avion/de navire ;

24° Sabotage ;

25° Trafic de véhicules volés ;

26° Espionnage industriel.

*

TEXTE COORDONNE AVEC SUIVI DES MODIFICATIONS

PROJET DE LOI

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Chapitre 1er – *Dispositions générales.*

Art. 1er. La présente loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Art. 2. Pour l'application de la présente loi, on entend par :

a) 1° «transporteur aérien» : toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes ;

b) 2° «passager» : toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers ;

c) 3° «dossier passager» : le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités ;

d) 4° « système de réservation» : le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations ;

e) 5° « système de contrôle des départs » : le système utilisé pour contrôler les passagers lors de l'embarquement ;

f) 6° « données PNR» les données contenues dans le dossier passager et énumérées à l'annexe I ;

g) 7° «méthode push» : la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'informations passagers créée à l'article 3 de la présente loi ;

h) 8° «infractions terroristes» : les infractions visées au Livre II, Titre Chapitre III-1 du Code pénal ;

i) 9° «formes graves de criminalité» : les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans ;

10° «dépersonnaliser par le masquage d'éléments des données» : rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée ;

j) 11° « services compétents » : les services visés à l'article 13 de la présente loi.

Chapitre 2 – *Unité d'informations passagers.*

Art. 3. Il est créé au sein de la Police grand-ducale une Unité d'informations passagers, ci-après désignée « UIP », qui est chargée :

a) 1° de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données ;

b) 2° du transfert de ces données et des résultats de leur traitement aux services compétents ;

c) 3° de l'échange de ces données et des résultats de leur traitement avec les unités d'informations passagers des autres Etats membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4. (1) Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Il est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

(2) Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel ~~détaché~~ de l'Administration des dDouanes et aAccises et du Service de rRenseignement de l'Etat. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Les membres du personnel de 1Administration des douanes et accises et du Service de renseignement de l'Etat sont désignés à l'UIP par une décision conjointe du ministre ayant la Police gland-ducale dans ses attributions et du ministre du ressort. Ils continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

Chapitre 3 – *Transfert des données par les transporteurs aériens*~~.~~

Art. 5. Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la méthode push, les données PNR de tous les passagers ~~de vols à destination ou~~ en provenance de, ~~u~~ à destination de ou transitant par le Luxembourg ~~dont ils disposent~~ pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien.

Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR incombe au transporteur aérien qui assure le vol.

Art. 6. (1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes:

1° ~~a)~~ 48 heures avant l'heure de départ programmée du vol ;

~~b) 24 heures avant l'heure de départ programmée du vol ;~~

2° ~~c)~~ 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 qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point ~~c)~~2° peut se limiter à une mise à jour dues transfert~~s~~ visé~~s~~ à l'alinéa 1er, point~~s a) et b)~~1°.

(2) Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP peut demander, au cas par cas, le transfert de données PNR en dehors des délais prévus au paragraphe 1er.

Art. 7. (1) Les données PNR sont transférées à l'UIP par voie électronique au moyen de~~s~~ protocoles communs et de~~s~~ formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la Directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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. Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg ~~dès leur publication au Journal officiel de l'Union européenne~~ conformément à l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne.

Les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisés pour leurs transferts.

(2) En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union européenne en matière de protection des données soit pleinement respecté.

(3) Dans l'hypothèse où un transporteur aérien ne conserve pas les données API énumérées à l'annexe I, point 18, par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR il transfère également ces données par la méthode « push » à l'UIP. Dans le cas d'un tel transfert, toutes les dispositions de la présente loi s'appliquent à ces données API.

Chapitre 4 – *Traitement des données PNR*~~.~~

Art. 8. Le traitement de données PNR qui révèlent 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 est interdit.

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive.

Art. 9. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données supplémentaires dès réception et de façon définitive.

Art. 10. (1) L'UIP traite les données PNR en vue de réaliser une évaluation des passagers avant leur arrivée prévue sur le territoire national ou leur départ prévu du territoire national afin d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis compte tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

(2) Pour réaliser cette évaluation l'UIP peut comparer les données PNR :

1° ~~a)~~ aux traitements de données à caractère personnel ~~banque des données gérées~~mis en oeuvre par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;

2° ~~b)~~ à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur 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.

(3) L'UIP réexamine individuellement, par des moyens non automatisés, toute concordance positive obtenue à la suite d'un traitement automatisé des données PNR effectué en vertu du présent article.

(4) L'UIP transmet aux services compétents, au cas par cas, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au présent article ou le résultat du traitement de ces données.

(5) Les conséquences de l'évaluation des passagers ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union européenne à la libre circulation sur le territoire du Grand-Duché de Luxembourg tel que prévu par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.

(6) Lorsque les évaluations sont réalisées pour des vols entre le Luxembourg et un autre Etat membre de l'Union européenne auquel s'applique le règlement ~~No~~ 2016/399~~562/2006~~ du Parlement européen et du Conseil du ~~15~~ 9 mars 201~~0~~6 ~~établissant~~ concernant un code ~~communautaire~~ de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), les conséquences de ces évaluations doivent respecter ledit règlement.

Art. 11. L'UIP traite les données PNR afin de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations visées à l'article 10.

Art. 12. L'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, dûment motivées et fondées sur des motifs suffisants visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques aux fins visées à l'article 1", et visant à communiquer aux services compétents ou, le cas échéant, à Europol, le résultat de ce traitement.

Chapitre 5 – *Services compétents*

Art. 13. Sans préjudice des attributions des autorités judiciaires telles que définies par le Code de procédure pénale,S sont habilités à demander à l'UIP ouet à recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, dans le cadre de leurs attributions légales et dans la limite de besoin d'en connaîtreen vue de procéder à un examen approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et poursuites en la matière :

a) 1° les services de la Police grand-ducale ;

b) 2° le Service de rRenseignement de l'Etat conformément à l'article 5, paragraphe 4, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat;

c) 3° les services de l'Administration des dDouanes et aAccises.

En recherchant les crimes et délits visés à l'article 2, points 8° et 9°, le procureur d'Etat peut, par une décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 12.

Art. 14. Les services compétents ne peuvent traiter les données PNR et le résultat du traitement de ces données que pour les finalités de la présente loi telles que définies à l'article 1er.

L'alinéa 1er est sans préjudice des compétences de la Police grand-ducale et de l'Administration des dDouanes et aAccises lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement.

Art. 15. Les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Les décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peuvent pas être fondées sur 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.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Art. 16. Lorsqu'une personne est identifiée conformément à l'article 10, l'UIP communique toutes les données pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP des autres Etats membres de l'Union européenne concernés.

Lorsque l'UIP est destinataire d'informations telles que visées à l'alinéa 1°' de la part d'une autre UIP, elle transmet ces informations aux services compétents.

Art. 17. (1) L'UIP transmet, dès que possible, à l'UIP d'un autre Etat membre de l'Union européenne qui en fait la demande, les données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par masquage conformément à l'article 26, et, si nécessaire, le résultat de tout traitement de ces données, s'il a déjà été réalisé conformément à l'article 10.

La demande, dûment motivée, peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière.

Si les données demandées ont été dépersonnalisées par masquage conformément à l'article 26, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que le transfert est nécessaire aux fins visées à l'article 12 et si elle y est autorisée par le procureur général d'Etat de Luxembourg ou son délégué.

Les dispositions du prescrit paragraphe ne sortent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

(2) Dans des cas d'urgence, les autorités compétentes des autres Etats membres, désignées conformément à l'article 7, paragraphe 1er, de la Directive (UE) 2016/661 du Parlement européen et du

Conseil du 27 avril 2016 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 et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe ~~(~~1~~)~~er sont applicables.

(3) À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un État membre a le droit de demander à ce que l'UIP obtienne des données PNR conformément à l'article 6, paragraphe ~~(~~2~~)~~, et les communique à l'UIP requérante.

Art. 18. L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres Etats membres de l'Union européenne des données PNR ou les résultats du traitement de ces données. ~~Les demandes sont introduites et traitées conformément au droit national de l'Etat membre requis.~~

Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre Etat membre de l'Union européenne, il transmet copie de sa demande à l'UIP.

Art. 19. L'échange de données effectué en application du présent chapitre peut avoir lieu par l'intermédiaire de tous les canaux de coopération ~~policière~~ existant entre les ~~autorités~~ services compétent~~e~~s des Etats membres de l'Union européenne.

La langue utilisée pour la demande et l'échange des données est celle applicable au canal utilisé.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*~~.~~

Art. 20. (1) Dans les limites de ses compétences et pour l'accomplissement de ses missions, Europol peut présenter à l'UIP, au cas par cas, par l'intermédiaire de son unité nationale, une demande électronique dûment motivée visant à obtenir des données PNR spécifiques ou le résultat du traitement de ces données :

~~a)~~ 1° lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des Etats membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes dans la matière et ;

~~b)~~ 2° dans la mesure où ladite infraction relève de la compétence d'Europol.

(2) La demande énonce les motifs sur lesquels s'appuie Europol pour estimer que la transmission de données PNR ou du résultat de traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée ou à des enquêtes en la matière.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne.*

Art. 21. ~~Sans préjudice des dispositions de l'article 35, paragraphe (1), point (d), et des articles 36 à 38 de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, L~~l'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si :

a) 1° l'une des conditions revues à l'article 35 paragraphe 1er, point d) de la loi du ji/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est remplie ;

~~a)~~ 2° l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité ;

~~b)~~ 3° le transfert est nécessaire aux fins telles que définies à l'article 1er ;

~~c)~~ 4° le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er ;

~~d)~~ 5° les conditions prévues à l'article 17, paragraphe ~~(~~1~~)~~er sont remplies.

Les dispositions du présent article ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

Art. 22. (1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre Etat membre de l'Union européenne à un pays non membre de l'Union européenne que si l'Etat membre auprès duquel les données ont été collectées a donné son accord au transfert.

(2) Dans des circonstances exceptionnelles, les données PNR peuvent être transférées à un pays non membre de l'Union européenne sans l'accord du pays membre de l'Union européenne auprès duquel les données ont été collectées si les conditions suivantes sont remplies :

~~a)~~ 1° 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 Etat membre de l'Union européenne ou un pays tiers ;

~~b)~~ 2° l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'Etat membre de l'Union européenne, qui n'a pas pu donner son accord en temps utile, est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ~~ex post~~ a posteriori.

Art. 23. L'UIP ne peut transférer des données PNR et les résultats du traitement de ces données aux autorités compétentes de pays non membres de l'Union européenne ~~que dans les conditions compatibles avec la présente loi et~~ qu'après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte l~~e~~es conditions et garanties de la présente loi.

Art. 24. Le délégué à la protection des données visé à l'article 29 est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*~~.~~

Art. 25. L'UIP conserve les données PNR pendant une durée maximale de cinq ans à compter du transfert par le transporteur aérien.

A l'issue de cette période de cinq ans, elle efface les données PNR de manière définitive. Cette disposition ne s'applique pas si les données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière.

Art. 26. (1) À l'expiration d'une période de six mois à compter du transfert par le transporteur aérien, l'UIP dépersonnalise les données PNR par le masquage des éléments suivants :

~~a)~~ 1° le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR ;

~~b)~~ 2° l'adresse et les coordonnées ;

~~c)~~ 3° des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne ;

~~d)~~ 4° les informations «grands voyageurs» ;

~~e)~~ 5° les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte ;

~~f)~~ 6° toute donnée API qui a été recueillie.

(2) À l'expiration de la période de six mois visée au paragraphe (1), la communication de l'intégralité des données PNR n'est autorisée que sous les conditions suivantes :

1° ~~a)~~ elle est nécessaire aux fins visées à l'article 12 ;

2° ~~b)~~ elle a été approuvée par le procureur général d'Etat ~~de Luxembourg~~ son délégué ou, si les données sont destinées à être communiquées au Service de r~~R~~enseignement de l'Etat, par la c~~C~~ommission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Art. 27. L'UIP ne conserve le résultat de l'évaluation réalisée en vertu de l'article 10 que le temps nécessaire pour informer les services compétents et, s'il y a lieu, les UIP des autres États membres de l'Union européenne de l'existence d'une concordance positive.

Lorsque, à la suite du réexamen individuel par des moyens non automatisés conformément à l'article 10, paragraphe ~~(~~33~~)~~, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées en vertu de l'article 25, de manière à éviter de futures «fausses» concordances positives.

Chapitre 10 – *Protection des données à caractère personnel~~.~~*

Art. 28. ~~Sans préjudice de l'article 41 de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale,~~ L~~l~~'autorité de contrôle visée à ~~instituée par~~ l'article ~~1~~1er 40 de la loi du jj/mm/aaaa ~~relative à la création de la Commission nationale pour la protection des données et au régime général sur la protection des données~~ jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 10 de la ~~même~~ loi du jj/mm/aaaa portant création de la Commission nationale pour la protection des données et du régime général sur la protection des données et elle dispose, à cette fin, des pouvoirs prévus à l'article 16 de la même loi.

Art. 29. (1) Le responsable de l'UIP désigne un délégué à la protection des données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et~~, en particulier,~~ de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

(2) Le délégué à la protection des données contrôle le traitement des données PNR et met en oeuvre les garanties pertinentes au sein de l'UIP.

Il informe et conseille le responsable et le personnel de l'UIP sur les obligations qui leur incombent en matière de protection des données.

Il fait office de point de contact pour les personnes concernées pour toutes les questions relatives au traitement de leurs données PNR et pour la Commission nationale pour la protection des données.

(3) Le délégué à la protection des données effectue ses missions en toute indépendance.

Il fait directement rapport au responsable de l'UIP.

Par dérogation à l'alinéa 2, et sans préjudice du paragraphe (4), alinéa 2, en cas de problèmes relevant de la protection des données, le délégué à la protection des données rapporte directement au d~~D~~irecteur général de la Police grand-ducale ou, s'il juge nécessaire, au m~~M~~inistre ayant la Police grand-ducale dans ses attributions.

(4) Le délégué à la protection des données a accès à toutes les données traitées par l'UIP.

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données conformément à la loi du ji/mm/aaaa relative à la création de la Commission nationale pour la protection des données et au régime général sur la protection des données.

Art. 30. L'UIP met à la disposition du public, par les moyens de communication appropriés, les informations suivantes :

~~a)~~ 1° ses coordonnées ;

~~b)~~ 2° les coordonnées du délégué à la protection des données ;

~~c)~~ 3° les finalités du traitement auquel sont destinées les données PNR ;

~~d)~~ 4° le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité ;

~~e)~~ 5° l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31. (1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 14 à 18 du projet de loi du *[jj/mm/aaaa]* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 45 à 48 du projet de loi du *[jj/mm/aaaa]* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 32. L'UIP conserve, traite et analyse les données PNR en un ou des endroits sécurisés situés sur le territoire du Grand-Duché de Luxembourg.

Art. 33. Le responsable de l'UIP met en oeuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et la nature des données PNR.

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en oeuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 29, paragraphe ~~(~~2~~)~~ de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 34. L'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

Cette documentation comprend :

~~a)~~ 1° l~~L~~e nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès ;

~~b)~~ 2° l~~L~~es demandes formulées par les services compétents et les UIP des autres Etats membres de l'Union européenne ;

~~c)~~ 3° t~~T~~outes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Art. 35. L'UIP tient des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

Les registres des opérations de consultation et de communication indiquent la finalité, la date et l'heure de l'opération et l'identité de la personne qui a consulté ou communiqué les données PNR ainsi que l'identité des destinataires de ces données.

Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit.

L'UIP met les registres à la disposition de l'autorité de contrôle, à la demande de celle-ci. Les registres sont conservés pendant cinq ans.

Art. 36. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe sans retard injustifié la personne concernée et la Commission nationale pour la protection des données ~~l'autorité de contrôle~~ de cette atteinte.

Chapitre 11 – *Sanctions*~~.~~

Art. 37. La violation intentionnelle de~~s~~ l'article~~s~~ 8, alinéa 1er et de l'article 15 et ~~36~~ est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125~~.~~ 000 euros ou d'une de ces peines seulement. La juridiction saisie ~~peut~~ prononce~~r~~ la cessation du traitement contraire aux dispositions

de ~~u présent article~~ l'article 8, alinéa 1er et de l'article 15 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 49, paragraphe 1er et paragraphes 3 à 5 du projet de loi du *[jj/mm/aaaa]* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38. (1) Est puni d'une amende d'un montant maximum de 50 000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements ~~y~~ visés à l'article 3, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

(2) Le manquement est constaté par un procès-verbal établi par la Police grand-ducale. Copie en est transmise au transporteur aérien.

Le transporteur aérien a accès au dossier et est mis à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction.

L'amende est prononcée par le m~~M~~inistre ayant la Police grand-ducale dans ses attributions.

(3) La décision du ministre qui est motivée est susceptible d'un recours en réformation à introduire devant le Tribunal administratif dans un délai d'un mois à compter de la notification.

Chapitre 12 – *Dispositions modificatives*

Art. 39. Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

«(4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, ou de cyber-menace dans la mesure où celle-cielle est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12, de la loi du jj/mm/aaaa relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Le directeur du SRE rapporte tous les ~~six~~ mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en oeuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Art. 40. A l'article 8, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, ~~le point~~ la lettre a) est supprimée.

Chapitre 13 – *Disposition finale*

Art. 41. La référence a la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : *« Loi du jj/mm/aaaa relative au traitement des données des dossiers passagers».*

*

ANNEXE I

Liste des données PNR

1° ~~a)~~ Code repère du dossier passager ;

2° ~~b)~~ Date de réservation/d'émission du billet ;

~~c)~~ 3° Date(s) prévue(s) du voyage ;

~~d)~~ 4° Nom(s) ;

~~e)~~ 5° Adresse et coordonnées (numéro de téléphone, adresse électronique) ;

~~f)~~ 6° Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation ;

7° ~~g)~~ Itinéraire complet pour le PNR concerné ;

~~h)~~ 8° Informations «grands voyageurs» ;

~~i)~~ 9° Agence de voyages/agent de voyages ;

~~j)~~ 10° Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation ;

~~k)~~ 11° Indications concernant la scission/division du PNR ;

~~l)~~ 12° Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée) ;

~~m)~~ 13° Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix ;

~~n)~~ 14° Numéro du siège et autres informations concernant le siège ;

~~o)~~ 15° Informations sur le partage de code ;

~~p)~~ 16° Toutes les informations relatives aux bagages ;

~~q)~~ 17° Nombre et autres noms de voyageurs figurant dans le PNR ;

~~r)~~ 18° Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée) ;

~~s)~~ 19° Historique complet des modifications des données PNR énumérées aux points 1 à 18.

*

ANNEXE II

Liste des infractions visées à l'article 2, point (i)

~~a)~~ 1° Participation à une organisation criminelle ;
~~b)~~ 2° Traite des êtres humains ;
~~c)~~ 3° Exploitation sexuelle des enfants et pédopornographie ;
~~d)~~ 4° Trafic de stupéfiants et de substances psychotropes ;
~~e)~~ 5° Trafic d'armes, de munitions et d'explosifs ;
~~f)~~ 6° Corruption ;
~~g)~~ 7° Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union ;
~~h)~~ 8° Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro ;
~~i)~~ 9° Cybercriminalité ;
~~j)~~ 10° Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées ;
~~k)~~ 11° Aide à l'entrée et au séjour irréguliers ;
~~l)~~ 12° Meurtre, coups et blessures graves ;
~~m)~~ 13° Trafic d'organes et de tissus humains ;
~~n)~~ 14° Enlèvement, séquestration et prise d'otage ;
~~o)~~ 15° Vol organisé ou vol à main armée ;
~~p)~~ 16° Trafic de biens culturels, y compris d'antiquités et d'oeuvres d'art ;
~~q)~~ 17° Contrefaçon et piratage de produits ;
~~r)~~ 18° Falsification de documents administratifs et trafic de faux ;
~~s)~~ 19° Trafic de substances hormonales et d'autres facteurs de croissance ;
~~t)~~ 20° Trafic de matières nucléaires et radioactives ;
~~u)~~ 21° Viol ;
~~v)~~ 22° Infractions graves relevant de la Cour pénale internationale ;
~~w)~~ 23° Détournement d'avion/de navire ;
~~x)~~ 24° Sabotage ;
~~y)~~ 25° Trafic de véhicules volés ;
~~z)~~ 26° Espionnage industriel.

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/08

N° 7151[8]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant organisation du Service de renseignement de l'Etat

* * *

AVIS COMPLEMENTAIRE DU CONSEIL D'ETAT

(26.6.2018)

Par dépêche du 27 avril 2018, le Premier ministre, ministre d'État, a soumis à l'avis du Conseil d'État une série de vingt-neuf amendements, élaborés par le ministre de la Sécurité intérieure.

Ces amendements étaient accompagnés d'un commentaire pour chacun des amendements ainsi que d'un texte coordonné du projet de loi sous avis intégrant les amendements gouvernementaux.

*

EXAMEN DES AMENDEMENTS

Amendements 1 à 3

Les amendements 1 à 3 ne soulèvent pas d'observation.

Amendements 4

L'amendements 4 répond à l'opposition formelle que le Conseil d'État avait émise dans son avis du 30 mars 2018 concernant l'article 4 du projet de loi. Le Conseil d'État est dès lors en mesure de lever cette opposition formelle.

Amendement 5

Cet amendement ne soulève pas d'observation.

Amendement 6

Cet amendement répond à l'opposition formelle qu'il avait formulée dans son avis du 30 mars 2018 concernant l'article 6. Le Conseil d'État peut dès lors lever l'opposition formelle qu'il avait formulée.

Amendement 7

L'amendement 7 remplace la référence, à l'article 7, paragraphe 1er, alinéa 1er, seconde phrase, à la publication des actes d'exécution adoptés par la Commission européenne au Journal officiel de l'Union européenne, par une référence à l'article 297, paragraphe 1er, alinéa 3[1], du Traité sur le fonctionnement de l'Union européenne qui prévoit cette publication.

---

1 Article 297, paragraphe 1er, alinéa 3, du Traité sur le fonctionnement de l'Union européenne : « Les actes législatifs sont publiés dans le Journal officiel de l'Union européenne. Ils entrent en vigueur à la date qu'ils fixent ou, à défaut, le vingtième jour suivant leur publication ».

Cet amendement n'est cependant pas de nature à répondre à l'opposition formelle figurant dans le prédit avis du Conseil d'État. Il n'appartient pas au législateur national de déterminer les modalités de l'applicabilité sur le territoire du Luxembourg des actes de l'Union.

Le Conseil d'État doit, par conséquent, maintenir son opposition formelle, mais rappelle qu'il suffira de supprimer la phrase en question pour assurer la conformité du dispositif luxembourgeois avec le dispositif européen.

Amendements 8 à 10

Ces amendements répondent aux observations et oppositions formelles que le Conseil d'État avait émises dans son avis du 30 mars 2018 et n'appellent pas de commentaire. Le Conseil d'État peut dès lors lever les différentes oppositions formelles qu'il avait formulées.

Amendement 11

L'amendement sous examen ajoute à l'article 17 la précision que les dispositions du paragraphe 3 de cet article « ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale ». Le Conseil d'État comprend cette disposition comme visant les dispositions de droit international et celles découlant de la loi formelle nationale. Le cas échéant, il y aurait lieu de préciser ce point. Le Conseil d'État pourrait dès à présent marquer son accord avec une formulation faisant référence « (…) aux dispositions tant internationales que nationales sur l'entraide judiciaire (…) »

Amendement 12

Cet amendement ne soulève pas d'observation.

Amendement 13

Cet amendement répond à l'opposition formelle que le Conseil d'État avait formulée dans son premier avis concernant l'article 19 du projet de loi.

Le Conseil d'État est dès lors en mesure de lever cette opposition formelle.

Amendements 14 à 19

Ces amendements ne soulèvent pas d'observation.

Amendement 20

Cet amendement répond à l'opposition formelle que le Conseil d'État avait formulée dans son premier avis concernant l'article 28 du projet de loi qu'il est dès lors en mesure de lever.

Le Conseil d'État constate qu'il est fait référence à la future loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale qui fait l'objet du projet de loi n° 7168 ainsi qu'à la loi en projet n° 7184 portant création de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Il relève qu'il faudra, d'une part, veiller à compléter les références à ces lois par leurs dates de promulgation, une fois que celles seront connues, et, d'autre part, éviter que la loi en projet entre en vigueur antérieurement aux lois auxquelles il est fait référence.

Amendements 21 à 24

Sans observation.

Amendement 25

L'amendement 25 porte sur l'article 37 du projet de loi sous avis, consacré aux sanctions pénales. Le Conseil d'État note que l'amendement sous examen précise que la violation intentionnelle de l'interdiction de traiter des données sensibles, telle que prévue à l'article 8 de la loi sous avis, sera sanctionnée pénalement, tandis que le fait de ne pas effacer des données sensibles qui auraient été traitées malgré l'interdiction de la loi ne le sera pas. Sera encore sanctionné de la même manière le fait de prendre intentionnellement une décision produisant des effets juridiques préjudiciables à une personne ou

l'affectant de manière significative sur la seule base d'un traitement automatisé de données PNR ou sur celle de l'évaluation de certains critères découlant d'un traitement de données particulièrement sensibles.

L'amendement apporte dès lors les clarifications demandées par le Conseil d'État dans son prédit avis. Le Conseil d'État est en mesure de lever l'opposition formelle qu'il avait formulée.

Amendement 26

L'amendement sous examen a trait à l'article 38 qui punit d'une peine d'amende d'un montant maximum de 50.000 euros le transporteur aérien à raison de chaque fois pour laquelle il n'a pas transmis les renseignements visés à la loi sous examen, ne les a pas transmis dans les délais ou selon les modalités prévues. Dans son avis du 30 mars 2018, le Conseil d'État s'était notamment interrogé sur le montant maximal de l'amende, qui correspond au décuple de l'amende prévue dans le cadre de l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes, et avait réservé sa position quant à la dispense du second vote constitutionnel dans l'attente des explications nécessaires.

Les auteurs de l'amendement 36 avancent un argumentaire tiré d'une comparaison entre la loi en projet et la loi du 21 décembre 2006[2] visée au commentaire de l'amendement et qui aboutit à la conclusion que, si la loi de 2006, relative aux données API, ne concerne que des données qui ne présentent « pas d'intérêt pour l'évaluation des personnes ni pour le dépistage des délinquants terroristes inconnus », la loi en projet, relative aux données PNR, aura comme finalité la prévention et la lutte contre le terrorisme et les formes graves de criminalité reprises au commentaire de l'amendement. Ainsi, la directive API (transposée par la loi de 2006) vise à prévenir l'immigration illégale « qui ne constitue pas d'infraction pénale », tandis que la directive PNR « crée des moyens destinés à protéger la sécurité et la vie des personnes », ce qui justifie la différence entre les sanctions encourues.

Le Conseil d'État prend acte des explications avancées et peut retirer sa réserve.

Amendements 27 à 29

Sans observation. Les différentes oppositions formelles figurant dans l'avis précité peuvent être levées.

*

OBSERVATIONS D'ORDRE LEGISTIQUE

Amendement 2

Les références aux dispositions figurant dans le dispositif et, le cas échéant, dans ses annexes se font en principe sans rappeler qu'il s'agit du « présent » acte. Partant, au point 1°, la formulation « créée à l'article 3 de la présente loi » est à remplacer par la formulation « telle que créée à l'article 3 » et au point 2°, les termes « de la présente loi » sont à supprimer.

Amendement 8

À l'article 10, paragraphe 6, de la loi en projet que le point 3° entend amender, les termes « (UE) » sont à insérer avant le numéro du règlement pour lire « règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) ».

---

2 Loi du 21 décembre 2006 portant 1. transposition – de la directive 2001/40/CE du Conseil du 28 mai 2001 relative à la reconnaissance mutuelle des décisions d'éloignement des ressortissants de pays tiers ; – de la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 ; – de la directive 2002/90/CE du Conseil du 28 novembre 2002 définissant l'aide à l'entrée, au transit et au séjour irréguliers ; – de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers ; 2. modification de la loi modifiée du 28 mars 1972 concernant 1. l'entrée et le séjour des étrangers ; 2. le contrôle médical des étrangers ; 3. l'emploi de la main-d'œuvre étrangère.

Amendement 9

À l'article 13, paragraphe 1er, point 2°, qu'il s'agit d'amender, il convient d'écrire « Service de renseignement de l'État » avec une lettre « s » majuscule à « service ».

Amendement 15

Suite à l'observation formulée dans son avis du 30 mars 2018, le Conseil d'État constate que les termes latins *« ex post »* ont été remplacés par la locution *« a posteriori »* également en latin. Le Conseil d'État propose d'employer la locution francisée « à posteriori » ou le terme « ultérieure ».

Amendement 20

À l'article 28 qu'il s'agit d'amender, le Conseil d'État observe que la référence à « la loi du jj/mm/aaaa ~~jj/mm/aaaa~~ relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale » comporte deux fois l'indication de la date non encore connue de la loi en question. Par ailleurs, le Conseil d'État constate qu'il est introduit une référence à « la loi du jj/mm/aaaa portant création de la Commission nationale pour la protection des données et du régime général sur la protection des données » et que la date de la loi en question fait défaut. Une fois connues, ces dates devront être insérées aux endroits pertinents.

Texte coordonné

Il convient de remplacer le terme « Luxembourg » par « Grand-Duché de Luxembourg » à l'article 7, paragraphe 1er, et à l'article 10, paragraphe 6.

À l'article 7, paragraphe 1er, de la loi en projet, le terme « directive » s'écrit avec une lettre « d » minuscule et les termes « (UE) » sont à ajouter avant le numéro de la directive à laquelle il est renvoyé, pour lire « directive (UE) 2016/681 […] ».

À l'article 29, paragraphe 4, alinéa 2, conformément à l'observation formulée relative à l'amendement 20, la date de la loi dont il s'agit sera à ajouter une fois connue.

Ainsi délibéré en séance plénière et adopté à l'unanimité des 20 votants, le 26 juin 2018.

Le Secrétaire général,
Marc BESCH

Le Président,
Georges WIVENES

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151/09

N° 7151[9]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

* * *

RAPPORT DE LA COMMISSION DE LA FORCE PUBLIQUE

(19.7.2018)

La Commission se compose de : Mme Claudia DALL'AGNOL, Présidente-Rapportrice ; Mme Diane ADEHM, M. Marc ANGEL, Mme Nancy ARENDT, MM. Alex BODRY, Felix EISCHEN, Léon GLODEN, Gusty GRAAS, Max HAHN, Jean-Marie HALSDORF, Fernand KARTHEISER, Henri KOX, Alexander KRIEPS, Membres.

*

I. PROCEDURE LEGISLATIVE

Le projet de loi sous rubrique a été déposé à la Chambre des Députés le 19 juin 2017 par Monsieur le Ministre de la Sécurité intérieure. Le texte du projet, comprenant deux annexes, était accompagné d'un exposé des motifs, d'un commentaire des articles, d'un tableau de correspondance, d'une fiche financière, d'une fiche d'évaluation d'impact et du texte de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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, ainsi que de ses deux annexes.

Le projet de loi a fait l'objet des avis :

- du Parquet général en date du 24 août 2017 ;
- des Parquets de Luxembourg et de Diekirch en date du 15 octobre 2017 ;
- du Tribunal d'arrondissement de et à Luxembourg en date du 18 septembre 2017 ;
- de la Commission nationale pour la protection des données en date du 23 novembre 2017 ;
- de la Cour supérieure de Justice en date du 20 novembre 2017 ;
- de la Chambre de Commerce en date du 13 décembre 2017.

Une première série d'amendements gouvernementaux a été soumise au Conseil d'État le 27 février 2018.

Le Conseil d'État a émis son avis sur ces amendements et le projet de loi le 30 mars 2018.

Le 27 avril 2018, le texte a été amendé une seconde fois par les auteurs.

Dans sa réunion du 4 mai 2018, la commission a désigné Mme Claudia Dall'Agnol comme rapportrice et a procédé à l'examen du projet de loi à la lumière de l'avis du Conseil d'État.

L'avis complémentaire du Conseil d'État a été rendu le 26 juin 2018.

La réunion de la commission du 5 juillet 2018 était consacrée à l'examen de l'avis complémentaire du Conseil d'État.

La commission a adopté le présent rapport le 19 juillet 2018.

II. CONSIDERATIONS GENERALES

Les données des dossiers passagers (Passenger Name Records, « 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 usage commercial. Elles comprennent des informations telles que les coordonnées du passager, la date du voyage et d'émission du billet, le mode de paiement utilisé et le poids des bagages.

Outre leur usage commercial, les données PNR présentent un intérêt avéré pour les autorités chargées de la prévention et de la répression de la criminalité et sont utilisées depuis des années par les services policiers et douaniers de certains pays. Les activités liées à la criminalité organisée et au terrorisme impliquent souvent des déplacements internationaux. Ces données permettent de contrer la menace que représentent en particulier le terrorisme et certaines autres formes graves de criminalité sous un angle différent que d'autres catégories de données à caractère personnel traitées par les services répressifs.

Les données PNR peuvent être utilisées de différentes manières et à différentes fins. En temps réel, elles aident à trouver des personnes recherchées par la confrontation à des bases de données nationales et internationales ainsi qu'à identifier des personnes pour lesquelles l'analyse de profil indique qu'elles peuvent être impliquées dans une activité criminelle. Les données peuvent également être utilisées de manière réactive pour rassembler des preuves dans le cadre d'enquêtes et, finalement, de manière proactive pour analyser et définir des critères d'évaluation qui peuvent ensuite être appliqués afin d'évaluer le risque que représentent les passagers avant leur arrivée et avant leur départ.

a) Le cadre européen

L'idée de créer un cadre légal européen pour l'utilisation des données passagers à des fins répressives remonte à une proposition de la Commission européenne du 6 novembre 2007. La proposition de décision-cadre n'ayant toutefois pas été adoptée par le Conseil de l'Union européenne (UE) au moment de l'entrée en vigueur du traité sur le fonctionnement de l'Union européenne le 1er décembre 2009, elle a dû être remplacée par un nouveau texte. Dans sa communication du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers aux pays tiers, la Commission a décrit un certain nombre d'éléments essentiels d'une politique européenne dans ce domaine. Finalement, le 2 février 2011, la Commission a présenté une proposition de directive sur laquelle le Conseil Justice et Affaires intérieures (JAI) a dégagé une orientation générale le 26 avril 2012. Un vote de rejet de la Commission Libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen du 24 avril 2013 a toutefois bloqué la proposition de directive.

La montée en puissance du phénomène des combattants étrangers a relancé les discussions autour de la mise en place d'un système PNR européen. Après les attenants qui ont frappé Paris en janvier 2015, les chefs d'État et de Gouvernement de l'Union européenne ont appelé à adopter d'urgence une directive robuste et efficace relative à un système PNR européen, dotée de garanties en matière de protection des données.

Le Luxembourg avait également inscrit la lutte contre le terrorisme et la criminalité organisée parmi les priorités de sa présidence du Conseil de l'UE au deuxième semestre de l'année 2015 et s'était, entre autres, fixé comme objectif de parvenir à un accord politique sur la création d'un système PNR européen.

Au mois de février 2015, le Parlement européen s'est engagé à travailler sur la finalisation d'une directive jusqu'à la fin de l'année 2015, tout en encourageant le Conseil à faire des progrès sur le « paquet sur la protection des données » afin de permettre des trilogues en parallèle sur la proposition de directive PNR et la proposition de directive relative à la protection des données à caractère personnel en matière pénale. Le 15 juillet 2015, le Parlement européen a adopté un rapport révisé sur la proposition de directive PNR et un mandat de négociation avec le Conseil.

La présidence luxembourgeoise du Conseil a réussi à négocier un texte de compromis qui respecte à la fois les principes fondamentaux en matière de protection des données et réponde aux besoins opérationnels des services compétents. Le texte de compromis a été approuvé par le Conseil JAI le 4 décembre 2015 et par le Parlement européen le 14 avril 2016.

En date du 27 avril 2016, le Parlement européen et le Conseil ont par ailleurs adopté parallèlement le paquet sur la protection des données. Les deux instruments européens qui constituent le paquet sur

la protection des données s'ajoutent à la directive PNR, réformant en profondeur le droit de la protection des données au niveau de l'Union européenne.

b) Les points de discussion principaux sur la directive

Les principaux éléments de discussion entre la Commission européenne, le Conseil de l'UE et le Parlement européen étaient l'inclusion des vols intra-communautaires, l'application de la directive aux opérateurs économiques non transporteurs et la durée de conservation des données sous une forme active.

L'inclusion des vols intra-communautaires opposait les États membres qui plaidaient pour l'inclusion obligatoire de tous les vols intra-UE aux États membres qui étaient opposés à l'inclusion de ces vols. Le compromis trouvé dans l'orientation générale adoptée en avril 2012 avait laissé le choix aux États membres de collecter ou non les données PNR sur tous ou sur certains vols intra-UE. En raison de la menace sécuritaire constituée par les combattants étrangers et des stratégies de contournement entretemps développées, l'inclusion des vols intra-UE n'a plus été un sujet controversé au sein du Conseil en 2015. L'expérience acquise par les services répressifs montre en effet que les combattants étrangers empruntent des trajets de plus en plus compliqués à travers l'Union européenne pour dissimuler leur point de départ initial et leur destination finale. Le même phénomène est observé à propos des membres d'organisations criminelles. Le Parlement européen souhaitait cependant voir limiter l'application de la directive aux vols en provenance ou à destination d'États non membres de l'Union européenne. Le texte de la directive tel qu'adopté le 27 avril 2016 retient finalement que les États membres sont libres de collecter les données PNR sur tous ou sur certains vols intra-UE. Dans une déclaration commune du 4 décembre 2015, les ministres JAI se sont engagés à faire pleinement usage de la faculté de recueillir des données PNR pour les vols intra-UE dès la mise en application de la directive. Ce choix est entériné dans le texte du projet de loi.

Un autre sujet de négociation était la collecte obligatoire de données PNR auprès d'opérateurs économiques non transporteurs, tels que des agences ou des organisateurs de voyages. Il a été retenu que la Commission procède, au plus tard deux ans après le délai de transposition, à un réexamen de tous les éléments de la directive, et notamment la nécessité d'inclure ces opérateurs économiques. Par ailleurs, un considérant de la directive précise que les États membres peuvent prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs ou auprès de transporteurs autres que les transporteurs aériens. Dans la déclaration commune précitée du 4 décembre 2015, les ministres se sont engagés, dans la mesure du possible, à élargir la collecte des données PNR auprès d'opérateurs économiques autres que les transporteurs. Cette inclusion pose cependant des difficultés pratiques dans la mesure où les opérateurs économiques utilisent des systèmes de réservation différents et qu'il n'existe pas de standards en ce qui concerne leurs systèmes informatiques. Le Luxembourg engagera des réflexions sur la mise en pratique de l'inclusion des opérateurs économiques, mais attendra les résultats de l'évaluation au sujet de la nécessité de les inclure dans le champ d'application. C'est pourquoi le texte du présent projet de loi limite la collecte des données PNR aux transporteurs aériens.

Un troisième élément de discussion était la durée de conservation des données PNR. La proposition de la Commission prévoyait une période initiale de conservation de trente jours, suivie d'une période supplémentaire de cinq ans au cours de laquelle les données seraient masquées. Les négociations entre États membres ont toutefois fait apparaître qu'une période initiale de trente jours était trop courte d'un point de vue opérationnel et le Conseil a retenu une période de conservation globale de cinq ans, subdivisée en deux périodes, une première période de deux ans au cours de laquelle les données seraient pleinement accessibles, et une seconde période de trois ans où les données servant à identifier le passager seraient masquées et leur divulgation complète serait subordonnée à des conditions strictes. Selon l'avis et les expériences des services répressifs, le système PNR ne permet en effet de lutter de manière efficace contre le terrorisme et la criminalité organisée que si les données restent actives pendant une certaine période. Comme les actes de terrorisme se préparent généralement sur une période plus longue, le système PNR doit être conçu de manière à ce qu'il permette de reconstituer l'activité d'un ou de plusieurs individus en remontant sur une période suffisamment longue. Le suivi des groupes terroristes exige d'établir des profils de mouvements, procédure qui s'inscrit dans le long terme. La probabilité qu'une information intéressante se trouve dans les données PNR recueillies depuis moins de trente jours est minimale. Par ailleurs, concernant le cas particulier des individus se rendant dans des camps d'entraînement en Syrie ou en Irak, selon les renseignements des services spécialisés, ces séjours

dépassent généralement trente jours. Un délai de trente jours est également trop court pour lutter contre d'autres formes de criminalité telles que le trafic de drogue. Les critères d'évaluation sont en effet établis sur base de l'analyse répétée des données de voyage d'un individu en particulier ou de personnes qui apparaissent régulièrement dans le même dossier de voyage. Or, les trafiquants de drogues sont déployés tous les quatre à six mois. Une période de temps suffisamment longue avant le masquage est nécessaire pour découvrir de telles routes et pour comprendre comment les criminels adaptent leurs habitudes. Le Parlement européen a soutenu la proposition initiale de la Commission. La Présidence luxembourgeoise a toutefois réussi à démontrer, sur base d'exemples concrets fournis par les services compétents des États membres et décrits ci-dessus, qu'une période active de trente jours n'est pas suffisante. Le texte de compromis retient que les éléments des données qui peuvent servir à identifier directement le passager auquel se rapportent les données doivent être masqués à l'expiration d'une période de six mois à compter de leur transfert par les transporteurs aériens.

En général, l'adoption de la directive PNR et la mise en place du système de traitement des données PNR a été subordonnée à l'insertion dans le dispositif de garanties de protection strictes. Ces garanties consistent notamment à imposer des conditions limitatives d'accès et de transfert des données PNR aux différentes autorités nationales, européennes ou extra-européennes, à limiter la conservation des données PNR comme exposé ci-dessus, ou encore à désigner un délégué à la protection des données chargé de contrôler le traitement des données PNR.

*

III. OBJET DU PROJET DE LOI

Le projet de loi a pour objet de transposer en droit national la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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.

L'enjeu de la directive est de mettre en place entre les États membres de l'UE un système harmonisé de collecte, d'utilisation et de conservation des données PNR, tout en garantissant le respect des droits fondamentaux, et surtout de la protection des données à caractère personnel. Ce système repose sur la création dans chaque État membre d'une unité centrale nationale appelée « Unité d'informations Passagers » (« UIP ») chargée d'analyser les données PNR transférées par les transporteurs aériens et d'assurer la coordination des procédures et le transfert des informations entre les UIP des différents États membres, certaines autorités nationales bien définies, Europol, ainsi qu'à destination de pays non-membres de l'UE dans les cas où le traitement des données PNR s'avérerait positif.

Le premier chapitre du projet de loi contient les dispositions générales du texte, dont le champ d'application et les définitions clés de la loi en projet. Il est précisé que la loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Le deuxième chapitre crée au sein de la Police grand-ducale une Unité d'informations passagers et en règle les missions et la composition. L'UIP peut comprendre du personnel de l'Administration des douanes et accises et du personnel du Service de renseignement de l'État qui continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

Le troisième chapitre précise les modalités du transfert des données PNR par les transporteurs aériens.

Le quatrième chapitre concerne le traitement des données PNR par l'UIP, dont l'obligation d'effacer des données transférées autres que celles énumérées à l'annexe I du texte ou la manière dont les données peuvent être traitées.

Le cinquième chapitre traite des services compétents qui peuvent demander à l'UIP ou recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, à savoir la Police grand-ducale, le Service de renseignement de l'État et l'Administration des douanes et accises.

Les chapitres six, sept et huit décrivent les procédures pour échanger des données PNR ou le résultat du traitement de ces données, respectivement entre les États membres de l'Union européenne, avec Europol et avec des pays non membres de l'Union européenne.

Le neuvième chapitre concerne la durée de conservation des données PNR et la dépersonnalisation de ces données.

Le chapitre dix est consacré à la protection des données. La directive du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données est transposée en droit national parallèlement à la directive PNR. Le texte fait référence aux dispositions pertinentes du projet de loi de transposition de la directive du 27 avril 2016, notamment en ce qui concerne les droits des personnes et l'autorité de contrôle en matière de données PNR. En dehors de ces références, le présent chapitre comporte toute une série de dispositions spéciales qui sont destinées à garantir la protection des données PNR en particulier.

Le chapitre onze prévoit l'application de sanctions pénales lors de la violation intentionnelle de l'interdiction de traiter des données PNR qui révèlent 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. En outre, une sanction administrative est prévue pour sanctionner le transporteur aérien qui n'a pas rempli ses obligations en vertu de cette loi.

Finalement, les chapitres douze et treize contiennent les dispositions modificatives et finale.

*

IV. LES AVIS RELATIFS AU PROJET DE LOI

1. Les avis du Conseil d'Etat

Dans son avis du 30 mars 2018, le Conseil d'État précise qu'il n'entend pas faire une appréciation de la directive elle-même au regard des critères établis dans l'avis 1/15 rendu par la Cour de justice de l'Union européenne en date du 26 juillet 2017 relative à la compatibilité du projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers avec l'article 16 du TFUE et les articles 7, 8 et l'article 52, paragraphe 1er, de la Charte des droits fondamentaux de l'Union européenne.

Dans son analyse article par article, le Conseil d'État émet une série d'oppositions formelles qui sont basées sur le fait que les auteurs du projet de loi n'ont pas repris correctement ou dans leur totalité les articles de la directive. Le détail de ces observations peut être retracé dans le commentaire des articles.

La Haute Corporation s'interroge en outre sur la composition de l'UIP. Le choix de la Police grand-ducale en tant qu'administration de rattachement de l'UIP est, en soi, conforme à la directive. L'unité nouvellement créée sera composée non seulement de personnel provenant de la Police, mais encore de personnel pouvant être détaché de l'Administration des douanes et accises ainsi que du SRE. Le Conseil d'État s'interroge sur le statut de ce personnel « détaché » et sur ses compétences. Il relève que le projet de loi est en contradiction avec le statut général des fonctionnaires de l'État, puisqu'il prévoit que les personnes concernées continueront à agir « dans les limites des attributions légales de l'administration dont (elles) relève(nt) ». Bien que le Conseil d'État comprenne l'utilité d'une disposition qui prévoit que les différents services compétents disposent d'un représentant en tant qu'« agent de liaison » au sein de l'UIP ainsi que l'utilité d'une solution qui assure que ces agents gardent un accès aux traitements de données propres aux différents services d'origine, il se doit d'émettre une opposition formelle pour insécurité juridique.

Concernant les sanctions en cas de violation des différents prescrits de la loi en projet, le Conseil d'État attire l'attention sur le fait que les trois projets composant le « Paquet protection des données » contiennent des approches différentes dans la mesure où les méconnaissances des règles imposées sont sanctionnées tantôt par des dispositions pénales classiques, tantôt par des sanctions administratives imposées par la CNPD. Concernant plus précisément l'interdiction du traitement de données révélant des données sensibles et l'obligation d'effacement définitif si de telles données étaient néanmoins collectées, la Haute Corporation estime qu'afin d'assurer le respect du principe constitutionnel de la légalité de la peine, il y a lieu de préciser lequel des deux comportements est sanctionné : le traitement illicite ou bien le défaut d'effacement ? Il y a également lieu de préciser s'il s'agit d'une infraction intentionnelle, nécessitant la volonté déterminée de contrevenir à la disposition légale, ou bien si le

simple fait de procéder à un tel traitement (ou non-effacement) est suffisant pour encourir la peine prévue par la loi, sans que la preuve d'un dol spécial doive être rapportée. Le Conseil d'État considère en effet qu'un simple dysfonctionnement au sein de l'unité, dépourvu de toute intention criminelle, qui serait éventuellement sanctionnable du point de vue disciplinaire, n'est pas de nature à entraîner la responsabilité pénale.

Finalement, le Conseil d'État réserve sa position quant à la dispense du second vote constitutionnel en attendant des explications sur la différence de traitement introduite en ce qui concerne l'amende qu'un transporteur aérien encourt en cas de manquement de transmettre les données PNR par rapport aux données relatives aux passagers dit « données API ». Le Conseil d'État compare en effet les amendes prévues aux amendes déjà prévues par l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration à l'encontre des entreprises de transport qui ne respectent pas les obligations leur imposées par l'article 106 de la même loi, et concernant les données API.

Après l'examen d'une série d'amendements gouvernementaux, le Conseil d'État a levé la plupart des oppositions formelles et a fait des propositions pour les deux autres dans son avis complémentaire du 26 juin 2018. La Haute Corporation rappelle encore qu'il est fait référence à la future loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale qui fait l'objet du projet de loi n° 7168 ainsi qu'à la loi en projet n° 7184 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. Il relève qu'il faudra, d'une part, veiller à compléter les références à ces lois par leurs dates de promulgation, une fois que celles-ci seront connues, et, d'autre part, éviter que la loi en projet entre en vigueur antérieurement aux lois auxquelles il est fait référence.

2. L'avis des autorités judiciaires

L'avis des autorités judiciaires se compose de l'avis du Parquet général du 24 août 2017, de l'avis des Parquets de Luxembourg et de Diekirch du 15 octobre 2017 et de l'avis du Tribunal d'arrondissement de et à Luxembourg du 18 septembre 2017 et a été soumis à la Chambre des Députés en date du 10 novembre 2017.

Dans son avis du 24 août 2017, le Parquet général rappelle tout d'abord la finalité et la nécessité de collecter les données PNR. Effectivement, selon le Parquet général, les données PNR se révèlent essentielles pour les évaluations des risques présentés par certaines personnes et l'établissement des liens entre les personnes déjà connues et des personnes inconnues. La finalité du traitement des données des passagers s'inscrit ainsi clairement dans le cadre de la prévention et de la recherche d'infractions terroristes, des formes graves de criminalité, des atteintes à l'ordre public dans le cadre de la radicalisation violente et des activités pouvant menacer les intérêts fondamentaux des États membres de l'Union européenne.

Le Parquet général déplore que le gouvernement ait opté à ne pas imposer l'obligation de transmettre les données PNR à d'autres opérateurs économiques autres que les transporteurs aériens, étant donné que les organisations terroristes et criminelles ne se limitent pas à l'utilisation du transport aérien pour organiser leurs activités.

Finalement, le Parquet général s'inquiète concernant le rôle et les droits des autorités judiciaires en la matière. Ainsi, concernant l'Unité d'informations passagers à créer au sein de la Police grand-ducale, le Parquet général pose la question s'il n'était pas opportun qu'un représentant des autorités judiciaires de poursuite en fasse partie, puisque la recherche, la constatation et la poursuite des infractions relèvent de la compétence des autorités judiciaires de poursuite, et si ce représentant ne devrait pas même être le responsable de l'UIP. Le Parquet propose également de procéder à une adaptation du Code de procédure pénale, à l'instar de ce qui a été fait en Belgique, pour que le Parquet général puisse charger un officier de police judiciaire de requérir l'UIP afin de communiquer des données PNR et que cette mesure peut même porter sur un ensemble de données relatives à une enquête pénale spécifique.

L'avis des Parquets de Luxembourg et de Diekirch du 15 octobre 2017 concerne principalement les dispositions qui impliquent l'intervention des parquets ou qui, selon l'avis, devraient les impliquer. Ils se rallient à l'avis du Parquet général en ce qui concerne la composition de l'UIP en posant la question s'il ne serait pas recommandable de faire présider l'UIP par un magistrat afin de veiller au mieux à la protection des données à caractère personnel dans le cadre de la recherche, de la constatation et de la

poursuite des infractions de terrorisme et de criminalité grave qui se déroulent sous la direction des autorités judiciaires. Il est en outre proposé, en vue d'une transposition correcte et intégrale de la directive, de faire figurer les autorités judiciaires dans l'énumération des autorités habilitées à demander et à recevoir de la part de l'UIP des données PNR ou le résultat du traitement de ces données.

Le Tribunal d'arrondissement de et à Luxembourg discute dans son avis du 18 septembre 2017 surtout la question du juste équilibre entre les nécessités de la politique sécuritaire et la protection des données personnelles. Selon cet avis, il est entendu que le but de la législation projetée n'est pas discutable, la connaissance des données en relation avec les déplacements effectués par les personnes constitue, à l'évidence, un élément très important dans la lutte, tant contre le terrorisme, que la criminalité grave. Il faudra néanmoins veiller à entourer la collecte de ces données essentiellement liées notamment à la liberté d'aller et de venir d'une protection adéquate. Après une révision des chapitres du projet de loi, le Tribunal d'arrondissement de et à Luxembourg conclut : « Dans l'ensemble le projet de loi reflète dès lors à suffisance un juste équilibre entre l'utilité et la nécessité indiscutable de la collecte des données PNR et le souci de protection des données personnelles qui ne devraient en aucun cas être accessibles et utilisables en dehors du champ légal dans le cadre duquel elles ont été collectées. »

3. L'avis de la Commission nationale pour la protection des données

L'avis de la Commission nationale pour la protection des données (CNPD) du 23 novembre 2017 est entré à la Chambre des Députés le 18 décembre 2017. En guise d'introduction, la CNPD se déclare bien consciente que le législateur a l'obligation de transposer la directive européenne en droit national au plus tard pour le 25 mai 2018, faute de risquer un recours en manquement de la part de la Commission européenne. Ainsi, elle n'a pas l'intention de remettre en cause en lui-même le système PNR, bien que la CNPD soit plutôt critique du système en tant que tel. La CNPD a limité ses remarques aux dispositions où les auteurs du projet de loi ont usé la marge de manœuvre laissée aux États membres lors de la transposition.

Quant au champ d'application, la CNPD prend note que les auteurs du projet de loi ont opté, à l'instar de leurs homologues belges, français ou allemands, d'inclure les vols intra-UE dans le champ d'application du projet de loi afin de maximiser l'efficacité du système PNR. Par ailleurs, la CNPD approuve la décision des auteurs du projet de loi de ne pas avoir étendu le système PNR aux agences ou organisateurs de voyages, ainsi qu'aux opérateurs économiques autres que les transporteurs ou auprès de transporteurs autres que les transporteurs aériens. Comme un tel élargissement du champ d'application du système PNR menacerait de manière encore plus importante les droits fondamentaux des personnes concernées, il paraît raisonnable d'attendre l'évaluation de la Commission européenne de tous les éléments de la directive PNR. Finalement, la CNPD se demande si l'obligation de transmettre à l'UIP les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg s'impose aussi aux taxis aériens privés.

S'agissant des bases de données et critères d'évaluation auxquels les données PNR peuvent être comparées, la CNPD est d'avis que le projet de loi dans sa première version ne définit pas avec exactitude les banques de données en cause, ni une liste exhaustive énumérant les critères d'évaluation. Dans l'optique de la CNPD, le projet de loi devrait identifier et énumérer expressément dans le corps du texte les différentes banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions. Un règlement grand-ducal pourra alors prévoir une liste exhaustive des critères d'évaluation prédéterminés qui pourrait au besoin être complétée ou modifiée si nécessaire.

Quant aux différentes catégories de données PNR, qui ont été critiquées pour ne pas être suffisamment claires et précises par le Contrôleur européen de la protection des données (CEPD), la CNPD recommande de décrire de manière plus précise et concise les catégories de données PNR « grands-voyageurs » et « remarques générales ».

Pour ce qui est de la conservation des données, la CNPD recommande d'inclure dans le corps du texte législatif une durée de conservation maximale à respecter par les services compétents en cas de transfert de données par l'UIP.

Finalement, quant au droit à l'information des personnes concernées, la CNPD suggère d'inclure dans le projet de loi les indications sur la durée de conservation et, le cas échéant, des catégories de destinataires des données PNR, dans les informations que l'UIP doit transmettre au public. La CNPD

recommande en outre de prévoir dans le projet de loi une disposition selon laquelle l'UIP est obligée d'informer les personnes concernées dont les données PNR ont été utilisées ou transférées, tout en y incluant la possibilité d'un retard ou d'une limitation du droit à l'information des personnes concernées conformément à l'article 13, paragraphe 3 du projet de loi transposant la directive 2016/680.

4. L'avis de la Cour supérieure de Justice

L'avis de la Cour supérieure de Justice du 20 novembre 2017 est intervenu à la Chambre des Députés en date du 18 décembre 2017.

La Cour supérieure de Justice souligne que le projet de loi doit être considéré avec les projets de loi ayant pour objet la mise en œuvre et la transposition en droit national du règlement (UE) 2016/679 et la directive européenne (UE) 2016/680 visant à l'harmonisation des dispositions nationales des États membres en matière de protection de données personnelles, puisque les trois projets forment un paquet de dispositions sur cette protection de données. Ils instaurent une réforme du cadre existant, visant à renforcer la protection des données à caractère personnel et à adapter les règles aux nouveaux défis réglementaires, dans un souci de pérennité et de neutralité technologique, en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

La Cour supérieure de Justice rappelle, à titre d'introduction, que la Cour de justice de l'Union européenne (CJUE) a dans son avis n° 1/15 du 26 juillet 2017 relatif à un projet d'accord entre le Canada et l'Union européenne sur le transfert de données des dossiers passagers aériens depuis l'Union européenne vers le Canada estimé que cet accord, qui reprend des dispositions identiques à celles de la directive PNR, était incompatible avec les articles 7, 8 et 21 ainsi qu'avec l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne.

Cet avis de la CJUE a amené la Cour supérieure de Justice à s'interroger sur la compatibilité de la directive PNR avec les susdits articles de la Charte. La Cour supérieure de Justice en a tiré la conclusion que « la CJUE a conclu la très longue polémique suscitée par les accords PNR et la directive (UE) 2016/681 et elle a validé le système PNR dans son principe tout en émettant des réserves ». La Cour continue à analyser les réserves en détail comme suit :

> « Parmi les points listés, la CJUE estime tout d'abord que les 19 catégories de données qui figurent dans l'accord (les mêmes dans tous les accords PNR ainsi que dans la directive européenne) devraient être définies de manière claire et précise et des termes comme *« toutes les coordonnées disponibles »* ou *« remarques générales »* sont à exclure dès lors qu'ils ne fixent aucune limitation quant à l'étendue et à la nature des informations susceptibles d'y figurer. La CJUE exclut par ailleurs le transfert de données sensibles (celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou concernant l'état de santé ou la vie sexuelle d'une personne), comme étant contraire à la Charte des droits fondamentaux.
>
> La CJUE relève encore que les autorités devront produire des « *modèles et critères préétablis (…) spécifiques et fiables* » de sorte à aboutir à des « *résultats ciblant les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou de criminalité transnationale grave* ». Les avancées technologiques devront être un outil au service de la société et non un prétexte à instituer des politiques ultra-sécuritaires violant les droits fondamentaux.
>
> S'agissant de la conservation des données, la CJUE relève que la conservation dans le pays destinataire doit être limité au strict nécessaire après le départ du passager, mais la durée de cinq ans prévue par la directive (UE) 2016/681 et reprise par le projet de loi sous avis ne semble pas « *excéder les limites de ce qui est strictement nécessaire à des fins de lutte contre le terrorisme et la criminalité transnationale grave* ».
>
> Quant au possible transfert de données PNR vers un pays tiers, la CJUE ne l'admet que si la Commission a constaté l'existence d'un « *niveau adéquat* » de protection dans le pays destinataire (art. 25, paragraphe 6 de la directive 95/46), ou « *substantiellement équivalent* » à celui assuré au sein de l'UE.
>
> Quant au contrôle du respect des exigences de la protection des données par le biais d'une autorité indépendante, exigence figurant tant dans la Charte (art. 8, paragraphe 3) que dans le Traité (Article 16, paragraphe 2 TFUE), seule une « *autorité publique indépendante* » présente les qualités requises et la CJUE n'admet pas d'autres termes pour définir l'autorité visée. »

La Cour fournit en outre quelques remarques et observations dans une analyse chapitre par chapitre du projet de loi. Dans ses remarques, la Cour se rallie aux avis des autres autorités judiciaires qu'il serait opportun de prévoir la possibilité d'un détachement d'un membre des Parquets ou du Parquet général vers l'UIP afin d'assurer une meilleure liaison à ce niveau. Concernant la méthode de transmission des données PNR, la Cour explique que la méthode à employer dite « push » est la méthode plus protectrice des données personnelles, mais qu'il serait opportun de la préciser davantage dans le texte du projet de loi.

En outre, la Cour qualifie le texte de l'article 13 comme étant pas très clair en ce qu'il semble limiter la transmission des données PNR aux autorités judiciaires seulement selon les règles du Code de procédure pénale et non en vertu du projet de loi. Si le fait de limiter la demande et la réception des données au seul cadre de prévention et de détection des infractions visées par la loi s'inscrit dans les principes prévalant en matière de protection des données à caractère personnel, il y a lieu d'observer que les termes de « dans la limite du besoin d'en connaître » sont imprécis et risquent de donner lieu à des interprétations diverses.

La Cour fait encore observer que c'est l'autorité de contrôle judiciaire qui reçoit compétence pour toiser les réclamations tombant sous l'application des articles 1er et 2 de la loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, tandis que la CNPD reste compétente pour toiser les réclamations tombant sous le champ d'application du règlement (UE) 2016/679. Or, la Cour estime que cette dualité de compétences peut comporter un risque de conflits.

5. L'avis de la Chambre de Commerce

L'avis de la Chambre de Commerce du 13 décembre 2017 a été soumis à la Chambre des Députés en date du 20 décembre 2017. Dans ses considérations générales, la Chambre de Commerce attire l'attention du législateur sur la nécessité de coordonner l'entrée en vigueur du projet de loi avec les deux autres projets de loi auxquels il fait référence (projets de loi n° 7168 et n°7184).

Quant aux implications financières de l'adoption du projet de loi, la Chambre de Commerce regrette que la mise en place du système de transfert des données PNR entraîne des coûts supplémentaires à charge des opérateurs du secteur. En ce qui concerne l'impact du projet de loi sur les finances de l'État, la Chambre de Commerce regrette que la fiche financière ne contienne aucune donnée précise concernant la mise en place effective du système de traitement des données PNR.

Le transfert des données PNR par les transporteurs aériens est à la base du système de traitement des données PNR mis en place par le projet de loi. Soucieuse que cette obligation n'engendre pas d'incertitude juridique pour les transporteurs aériens, la Chambre de Commerce souhaite mettre en évidence plusieurs points sur lesquels il lui semble particulièrement important de faire évoluer le projet de loi. Tout d'abord, la Chambre de Commerce regrette que l'article 5 du projet de loi ne reflète pas de manière suffisamment explicite le principe fondamental du système mis en place en vertu duquel les données PNR visées par l'obligation de transfert sont exclusivement les données recueillies par les transporteurs dans le cours normal de leurs activités de transport aérien au jour du transfert. Elle constate ensuite que l'obligation systématique de transfert des données d'un vol par le transporteur aérien devrait être destinée aux UIP de chaque État membre sur le territoire duquel le vol décollera ou atterrira, et non pas uniquement à l'UIP luxembourgeoise. De manière plus générale, la Chambre de Commerce s'interroge quant aux limites du système envisagé au sein duquel le traitement des données PNR sera, selon sa compréhension, limité à un contrôle national, transmis aux autres autorités compétentes uniquement en cas de correspondance positive. La Chambre de Commerce suggère également de limiter les échéances du transfert de données PNR à deux par vol.

Quant à la communication de données entre UIP en cas d'identification, la Chambre de Commerce suggère que l'article 16 du projet de loi soit modifié afin que, en cas d'identification d'une personne sur base du traitement des données PNR, la communication de données soit adressée aux UIP de tous les États membres de l'UE, et non pas seulement aux UIP des États membres concernés.

Quant au régime de sanctions, la Chambre de Commerce s'interroge sur l'opportunité d'adopter un texte de nature à porter atteinte à un régime de protection unifié et cohérent tel qu'il a vocation à être régi par le projet de loi n°7168. La Chambre de Commerce s'interroge également quant à la légalité de certaines peines visées par le projet de loi. La Chambre de Commerce dénonce enfin le caractère

manifestement disproportionné de l'amende pouvant aller jusqu'à 50 000 € par vol pour lequel un transporteur aérien ne remplirait pas son obligation de transfert de données PNR.

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi sous rubrique sous réserve de la prise en compte des commentaires formulés dans son avis.

*

V. COMMENTAIRE DES ARTICLES

Chapitre 1er – *Dispositions générales*

Articles 1er et 2

L'article 1er transpose l'article 1er de la directive PNR et détermine l'objet de la loi et précise et limite les finalités pour lesquelles les données PNR peuvent être traitées : sont visés les transporteurs aériens, lesquels doivent transférer les données des dossiers passagers pour le traitement de celles-ci à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

L'article 2 définit les différentes notions. Par amendement gouvernemental du 27 avril 2018, le point 7, en l'absence d'une définition de l'Unité d'informations passagers (UIP), a été complété par la référence à l'article 3 créant l'UIP, tel que suggéré par le Conseil d'État dans son avis du 30 mars 2018. Par ailleurs, un point 11 nouveau a été ajouté pour la notion de « services compétents », demande formulée par le Conseil d'État notamment à l'endroit de l'article 10, paragraphe 1er.

Chapitre 2 – *Unité d'informations passagers*

Articles 3 et 4

L'article 3 met en place au sein de la Police grand-ducale l'UIP chargée de la collecte, du transfert et de l'échange des données et des résultats de leur traitement, tel que prévu par la future loi.

L'UIP sera intégrée dans la direction « relations internationales » rattachée au comité de direction de la Police grand-ducale.

Dans son avis, le Conseil d'État approuve le choix de la Police grand-ducale en tant qu'administration de rattachement de l'UIP. Ce choix est conforme à l'article 4, paragraphe 1er de la directive, selon lequel « Chaque État membre met en place ou désigne une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité (…). ». Ce choix se justifie d'autant plus que « la Police grand-ducale est déjà à l'heure actuelle destinataire des données transférées en vertu de la loi précitée du 21 décembre 2006[1] ».

L'article 4 prévoit que l'UIP peut comprendre, outre le personnel policier, du personnel de l'Administration des douanes et accises (ADA) et du Service de renseignement de l'État (SRE).

Le Conseil d'État pose la question du statut et des compétences du personnel détaché en rappelant que, suivant l'article 7 du Statut général des fonctionnaires de l'État, le détachement consiste en « l'assignation au fonctionnaire d'un autre emploi correspondant à sa catégorie et à son grade dans une autre administration, dans un établissement public ou auprès d'un organisme international », qui a comme conséquence que « le fonctionnaire relève de l'autorité hiérarchique de l'administration, respectivement de l'établissement ou de l'organisme auquel il est détaché ». Par conséquent, les fonctionnaires détachés de l'ADA et du SRE « relèveront entièrement de la Police grand-ducale. Dès lors, en précisant que les personnes concernées continueront à agir « dans les limites des attributions légales de l'administration dont (elles) relève(nt) » le projet de loi sous examen est en contradiction avec la

1 Loi du 21 décembre 2006 portant 1. transposition – de la directive 2001/40/CE du Conseil du 28 mai 2001 relative à la reconnaissance mutuelle des décisions d'éloignement des ressortissants de pays tiers ; – de la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 ; – de la directive 2002/90/CE du Conseil du 28 novembre 2002 définissant l'aide à l'entrée, au transit et au séjour irréguliers ; – de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers ; 2. modification de la loi modifiée du 28 mars 1972 concernant 1. l'entrée et le séjour des étrangers ; 2. le contrôle médical des étrangers ; 3. l'emploi de la main-d'œuvre étrangère

disposition précitée du Statut général ». En conséquence, le Conseil d'État a exprimé une opposition formelle pour incohérence et insécurité juridique. En outre, il s'interroge sur la définition des « services compétents ».

Dans la lettre d'amendements gouvernementaux du 27 avril 2018, les auteurs confirment que « le projet de loi limite le traitement des données à une finalité de prévention et de répression du terrorisme et de la criminalité grave. Conformément à l'article 3, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du SRE, « *le SRE a pour mission de rechercher, d'analyser et de traiter, dans une perspective d'anticipation et de prévention, […] les renseignements relatifs à toute activité qui menace ou pourrait menacer la sécurité nationale […]* ». Le paragraphe 2 de l'article 3 de la loi précitée du 5 juillet 2016 précise qu'on « *entend par toute activité qui menace ou pourrait menacer la sécurité nationale […], toute activité […] qui peut avoir un rapport avec l'espionnage, l'ingérence, le terrorisme, l'extrémisme à propension violente, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, le crime organisé ou la cyber-menace dans la mesure où ces deux derniers sont liés aux activités précitées* ». Il est donc permis de conclure que les missions du SRE, et notamment ses missions de prévention en matière de lutte contre le terrorisme, l'espionnage, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes ou la cyber-menace dans la mesure où elle est liée aux activités précitées, correspondent parfaitement à la finalité définie par le projet de loi sous examen. Le SRE est partant justifié à traiter des données PNR. Le traitement de données PNR par un service de renseignement correspond d'ailleurs aux législations en place des pays européens dans la matière. Par exemple, l'article 14 de la loi belge du 25 décembre 2016 relative au traitement des données des passagers prévoit une UIP composée de la Sûreté de l'Etat visée par la loi organique du 30 novembre 1998 des services de renseignement et de sécurité et du Service général de Renseignement et de Sécurité visé par la loi organique du 30 novembre 1998 organique des services de renseignement et de sécurité. ».

Le Conseil d'État souligne aussi que les personnes détachées « ne sont plus en droit d'accéder aux données et informations traitées dans leur service d'origine sur base de leur première affectation, étant donné qu'en vertu de leur détachement ils n'en font plus partie », sauf à ajouter des dispositions spécifiques au texte de loi. Comprenant « l'utilité d'une disposition qui prévoit que les différents services compétents disposent d'un représentant en tant qu'« agent de liaison » au sein de l'UIP », le Conseil d'État propose notamment comme solution, s'inspirant de la loi belge de transposition de la directive PNR, de mettre en place une unité indépendante de la Police grand-ducale, à l'instar de la Cellule de renseignement financier auprès du parquet de Luxembourg.

La solution retenue par les auteurs des amendements se distingue du détachement en mentionnant que « si la version française de la Directive parle d'agents détachés, la version allemande utilise les termes « *abgeordnet werden* » et la version anglaise prévoit que « *staff members of a PIU may be seconded from competent authorities* » ». Les auteurs s'inspirent de l'article 9, paragraphe 3, de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat qui dispose que « *Les agents du centre peuvent être placés auprès d'un département ministériel ou d'une administration de l'Etat par une décision conjointe du ministre et du ministre du ressort. Dans ce cas, et pendant toute la durée de leur placement, ils continuent de relever de l'autorité hiérarchique du directeur du centre.* » Il ressort du commentaire des articles du projet de loi ayant abouti à la loi précitée du 20 avril 2009 que « *En ce qui concerne le personnel, la seule particularité pour le CTIE est la possibilité de placer certains de ses agents auprès des départements ministériels, administrations ou services de l'Etat sur base d'une décision conjointe des membres du Gouvernement respectifs. Cette mesure est destinée à permettre au CTIE d'envoyer des informaticiens auprès d'autres entités administratives afin de mettre en place et de gérer les systèmes informatiques d'une administration en particulier. Contrairement aux agents détachés, les agents placés par le CTIE continuent de relever de leur autorité hiérarchique d'origine. Ceci est nécessaire en raison du fait qu'ils doivent effectuer leur travail d'après les directives et les critères que le CTIE fixe pour l'ensemble du réseau informatique de l'Etat. (…) Le mécanisme du placement des agents est inspiré de la situation des contrôleurs financiers qui relèvent de l'autorité du Ministre ayant le budget dans ses attributions, mais qui exercent leurs missions auprès des différents départements ministériels*.[2]

Ainsi, le personnel de l'ADA et le personnel du SRE seront désignés à l'UIP comme membres de leurs administrations respectives et agiront comme tels. Cette solution ne remet pas en cause le principe

2 Projet de loi 5912

selon lequel l'UIP fonctionne sous forme de « closed box » et que les services désignés comme services compétents n'ont pas un accès direct aux données PNR. Le personnel de l'ADA et du SRE resteront placés sous l'autorité hiérarchique de leur administration d'origine. Pour permettre au responsable de l'UIP d'exercer les responsabilités qui lui incombent en vertu de la présente loi, il aura autorité fonctionnelle sur ce personnel. ».

Par ailleurs, quant à la critique du Conseil d'État que le texte ne donne aucune indication sur le grade ou la fonction du responsable de l'UIP, ni ne précise s'il doit s'agir d'un membre du personnel du cadre policier ou si un membre du cadre civil de la Police peut également remplir cette tâche de direction, le paragraphe 1er a été complété par un alinéa 2 précisant que le responsable de l'UIP est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

Le Conseil d'État relève que, « Dans leurs avis respectifs, tant la Cour supérieure de justice que les deux parquets d'arrondissement ont estimé que l'UIP devrait également comprendre, parmi son personnel, un magistrat détaché à cette fin ; les parquets se sont même demandés « s'il ne serait pas recommandable de faire présider cette unité » par un tel magistrat. Le Conseil d'État soulève que le détachement de magistrats au sein de cette unité y compris à sa direction, équivaudrait à un changement de statut de l'UIP, sans que ce changement contienne une plus-value évidente. Une telle possibilité ne serait par ailleurs envisageable que si l'UIP était mise en place en tant qu'unité indépendante des structures de la Police grand-ducale (…). ».

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Articles 5 à 7

L'article 5, transposant l'article 8, paragraphe 1er de la directive, prévoit que les transporteurs aériens transfèrent à l'UIP les données PNR de tous les passagers en provenance ou à destination du Luxembourg ou transitant par le Luxembourg.

Le transfert des données se fait sans préjudice des obligations imposées par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, à savoir la transmission des informations préalables recueillies sur les passagers (Advanced Passenger Information (API) au Service de contrôle à l'aéroport. Dans son avis, le Conseil d'État rappelle que ces informations sont déjà actuellement recueillies pour les passagers provenant d'un État non membre de l'Union européenne. Il rend attentif à l'obligation, prévue par l'article 8, paragraphe 2 de la directive, pour les États « d'adopter les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent également ces données, par la « méthode push », à l'UIP ». Il réserve sa position quant à la dispense du second vote constitutionnel dans l'attente des renseignements « de nature à établir que ce transfert est effectué dans les conditions requises par le législateur européen ».

Par amendement gouvernemental du 27 avril 2018, l'article 7 a été complété par un paragraphe 3 tenant compte de la réserve exprimée par le Conseil d'État.

L'article 6 concerne les moments du transfert des données à l'UIP, prévues par l'article 8, paragraphe 3 de la directive.

Le texte initial a fait l'objet d'une opposition formelle en raison de l'ajout d'une « obligation supplémentaire à celles prévues par la directive, risquant ainsi en outre de créer une charge administrative supplémentaire pour les transporteurs qui utilisent l'aéroport de Luxembourg par rapport à ceux qui ont recours à des aéroports situés dans des pays n'imposant pas un même niveau d'obligations ».

Par amendement gouvernemental du 27 avril 2018, l'obligation supplémentaire a été supprimée.

L'article 7 précise les procédés techniques de transfert des données et transpose l'article 16 de la directive.

Dans son avis du 30 mars 2018, le Conseil d'État demande, sous peine d'opposition formelle, la suppression de la seconde phrase du paragraphe 1er, alinéa 1er au regard de l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne (TFUE), selon lequel « Les actes législatifs sont publiés dans le Journal officiel de l'Union européenne. Ils entrent en vigueur à la date qu'ils fixent ou, à défaut, le vingtième jour suivant leur publication. ». Le libellé de ladite phrase figurant à l'article 7 dans sa version initiale est le suivant : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg dès leur publication au Journal officiel de l'Union européenne. ».

Par amendement gouvernemental du 27 avril 2018, cette phrase est modifiée comme suit : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg ~~dès leur publication au Journal officiel de l'Union européenne~~conformément à l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne. ».

Dans son avis complémentaire, le Conseil d'État maintient son opposition formelle, constatant que l'amendement ne répond pas à l'opposition formelle, puisqu'« il n'appartient pas au législateur national de déterminer les modalités de l'applicabilité sur le territoire du Luxembourg des actes de l'Union ». Il indique que la suppression de la phrase concernée assurera la conformité du dispositif luxembourgeois avec le dispositif européen.

La commission a par conséquent suivi le Conseil d'État et supprimé la phrase.

Chapitre 4 – *Traitement des données PNR*

Articles 8 à 12

L'article 8 transpose l'article 13, paragraphe 4 de la directive qui interdit le traitement de données PNR qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance à un syndicat, l'état de santé, la vie sexuelle ou l'orientation sexuelle. Ces données doivent être effacées dès réception et de façon définitive.

L'article 9 impose à l'UIP d'effacer celles des données transférées qui ne sont pas énumérées à l'annexe I.

Le Conseil d'État note dans son avis « que, contrairement à l'article 8, l'article 9 ne figure pas à l'article 37 du projet de loi sous examen parmi les articles dont la violation peut entraîner une sanction pénale. Étant donné cependant que le défaut d'effacement visé à l'article 9 vise un comportement similaire au défaut d'effacement visé à l'article 8, alinéa 2, le Conseil d'État suggère d'inclure cette disposition également à l'article 37 même si le Conseil d'État admet qu'un défaut d'effacement de données légalement collectées et transférées, mais ne figurant pas à l'annexe I du projet, est un comportement qui n'atteint pas le même seuil de gravité qu'une violation de l'article 8, de telle sorte que la sanction devrait être adaptée à cette gravité moindre. En effet, s'il est vrai que l'article 14, paragraphe 1er, de la directive n'oblige pas expressément les États à incriminer le comportement en question, une disposition prévoyant une sanction n'y est cependant pas contraire et sera indiquée pour assurer une meilleure protection des données personnelles. ».

Les auteurs n'ont pas suivi le Conseil d'État, « étant donné que le défaut d'effacement des données sensibles a été retiré parmi les faits sanctionnables pénalement ».

Les articles 10 à 12 transposent l'article 6, paragraphes 1er à 6 et 9 de la directive. Ils définissent les différentes manières dont les données PNR peuvent être utilisées dans le cadre de la prévention et la lutte contre le terrorisme et les formes graves de criminalité.

L'article 10 a trait à l'utilisation des données PNR pour réaliser une évaluation des passagers avant leur arrivée ou leur départ dans le but « d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis ». Cette évaluation se fait par comparaison des données PNR avec les données à caractère personnel traitées par les services compétents ou auxquelles ils ont accès dans l'exercice de leurs missions ou avec des critères préétablis. Le paragraphe 2, alinéa 2 édicte des règles strictes pour ces critères. En vertu du paragraphe 3, « toute concordance positive obtenue » engendre un réexamen individuel. Le paragraphe 4 prévoit la transmission des données « au cas par cas, en vue d'un examen plus approfondi ».

Suivant l'article 11, les données PNR peuvent aussi être traitées pour mettre à jour les critères d'évaluation ou pour définir de nouveaux critères.

L'article 12 prévoit comme autre finalité de traitement des données PNR celle de répondre aux demandes des services compétents, « dûment motivées et fondées sur des motifs suffisants ». Le commentaire du document tel que déposé explique que ces données peuvent servir comme éléments de preuve dans le cadre d'enquêtes judiciaires ; ainsi, elles peuvent aider à orienter les enquêteurs sur le lieu de séjour d'une personne suspecte au moment où les faits ont été commis.

Chapitre 5 – *Services compétents*

Articles 13 à 15

L'article 13 énumère les services habilités à demander et à recevoir des données PNR ou le résultat du traitement de ces données et détermine la finalité de la transmission des données aux services concernés. Il reprend l'article 7, paragraphe 1er de la directive, tenant ainsi compte d'une opposition formelle du Conseil d'État et des critiques du Parquet général et de la Cour supérieure de Justice pour transposition incorrecte de la directive et manque de précision en ce qui concerne la finalité de la transmission des données aux services concernés.

Par ailleurs, l'alinéa 1er, point 2 a été complété suite à une opposition formelle du Conseil d'État exprimée à l'égard de l'article 39 ajouté au projet de loi par amendement gouvernemental du 27 février 2018 (cf. sous article 39).

Le second alinéa résulte des propositions du Conseil d'État et du Parquet général d'introduire dans le cadre juridique national, à l'instar de la loi belge ayant transposé la directive PNR, un accès simplifié des procureurs d'État « aux données PNR détenues par l'UIP en leur évitant d'avoir à saisir le juge d'instruction ne fût-ce que par le biais d'une procédure dite « mini-instruction », tout en sachant qu'en tant qu'acte d'enquête, la réquisition serait susceptible du recours inscrit à l'article 48-2 du Code de procédure pénale ».

L'article 14 limite le traitement des données PNR et du résultat du traitement aux finalités déterminées par l'article 1er, sans préjudice des compétences de la Police grand-ducale et de l'ADA, « lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement ». Il transpose l'article 7, paragraphes 4 et 5 de la directive.

L'article 15, transposant l'article 7, paragraphe 6 de la directive, prévoit que les services compétents ne peuvent prendre aucune décision ayant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR. Même si l'article 8 du projet de loi interdit le traitement des données sensibles y visées, l'interdiction de prendre des décisions qui seraient basées sur de telles données, si celles-ci avaient néanmoins été collectées, a été ajoutée suite à l'opposition formelle du Conseil d'État.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Articles 16 à 19

Les articles 16 et 17 transposent l'article 9, paragraphes 1 à 4 de la directive. Le commentaire du texte déposé souligne que ces deux articles représentent des éléments-clés du système PNR européen, comme une grande importance avait été attachée lors des négociations en trilogues à l'échange d'informations entre États membres. Alors que l'article 16 règle la transmission d'office d'informations aux UIP d'autres États membres, l'article 17 règle la transmission d'informations sur demande de l'UIP d'un autre État membre.

L'article 16 vise à préciser que, lorsque l'UIP luxembourgeoise reçoit des informations d'une UIP étrangère, elle les continue aux services nationaux compétents.

L'article 17 définit les conditions de la demande adressée à l'UIP luxembourgeoise. Le paragraphe 1er distingue entre les données qui n'ont pas encore été dépersonnalisées par masquage tel que prévu par l'article 26 et les données masquées. Suivant le paragraphe 2, sauf en cas d'urgence, les demandes et les échanges de données ont lieu par l'intermédiaire des UIP. Le paragraphe 3 permet, en cas de menace précise et réelle, de demander des données auprès d'un transporteur aérien en dehors des délais prévus à l'article 6, paragraphe 1er.

Par amendement gouvernemental du 27 avril 2018, l'article 17, paragraphe 1er a été complété par un alinéa 4. Suivant le commentaire de l'amendement, celui-ci « est à voir en relation avec la question, soulevée par le Parquet général à propos de l'article 21 réglant le transfert de données PNR à des États non membres de l'Union européenne, de savoir si cet échange échapperait aux dispositions traditionnelles de l'entraide judiciaire. Afin de dissiper toute incertitude à cet égard, une précision afférente a été apportée non seulement en ce qui concerne les échanges de données PNR avec des pays tiers, mais également l'échange de telles données avec d'autres États membres. ». Dans son avis complémentaire, le Conseil d'État a proposé une formulation plus précise qui a été reprise par la commission.

L'article 18 est relatif aux cas où les autorités luxembourgeoises adressent des demandes de données à l'UIP d'un autre État membre.

L'article 19 transpose l'article 9, paragraphe 5 de la directive qui concerne les modalités techniques d'échange des informations entre États membres.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Article 20

Cet article transpose l'article 10 de la directive, définissant les conditions d'accès aux données PNR par Europol.

Le Conseil d'État reconnaît à cette disposition une pure valeur déclaratoire, « étant donné que les compétences d'Europol ainsi que ses droits et obligations dans le cadre desdites compétences, font l'objet d'instruments européens et ne nécessitent pas de mesures de transposition particulières en droit national ».

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Articles 21 à 24

L'article 21 transpose l'article 11, paragraphe 1er de la directive qui détermine les conditions du transfert de données PNR à un pays non membre de l'Union européenne.

Suite aux observations du Conseil d'État faites dans son avis, l'article 21 a été restructuré par amendement gouvernemental pour « clarifier le texte en ce qu'il énonce, parmi les conditions à respecter, celles prévues à l'article 35 [devenu l'article 34], paragraphe 1er, point d) de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, à savoir que la Commission européenne doit avoir adopté une décision d'adéquation ou, en l'absence d'une telle décision, que des garanties appropriées ont été prévues ou existent ou, en l'absence de décision d'adéquation et de garanties appropriées, que des dérogations pour des situations particulières s'appliquent. Afin de ne pas surcharger la présente loi avec des dispositions figurant déjà dans une autre loi, les auteurs des amendements ont préféré faire un renvoi à la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ».

L'article 22 transpose l'article 11, paragraphe 2 de la directive qui a trait au transfert de données PNR, obtenues d'un autre État membre, à un pays non membre de l'Union européenne.

L'article 23 transpose l'article 11, paragraphe 3 de la directive. Il prévoit une condition supplémentaire aux transferts de données vers des pays tiers. Suite aux interrogations du Conseil d'État, le texte a été amendé « de manière à n'ajouter comme condition supplémentaire par rapport aux conditions fixées aux articles 21 et 22 que celle d'avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données respecte les conditions et garanties de la présente loi ».

L'article 24 transpose l'article 11, paragraphe 4 de la directive, en vertu duquel « Chaque fois qu'un État membre transfère des données PNR en vertu du présent article, le délégué à la protection des données de l'UIP de cet État membre en est informé. ».

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Articles 25 à 27

L'article 25 transpose l'article 12, paragraphes 1er et 4 de la directive et dispose que la durée maximale de conservation des données PNR est de cinq ans. Les données sont ensuite effacées de manière définitive, sauf celles qui ont été transférées à un service compétent et qui sont utilisées dans le cadre d'une enquête ou poursuite.

L'article 26 transpose l'article 12, paragraphe 2 de la directive qui impose l'obligation de dépersonnaliser par le masquage des éléments des données qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR. Le commentaire du texte déposé explique que « Le masquage est une technique qui consiste à rendre ces éléments de données invisibles, sans toutefois les altérer. Des recherches automatisées restent ainsi possibles parmi les données masquées et des hits

peuvent être générés. Toutefois les informations permettant d'identifier la personne à laquelle les données se rapportent ne sont pas affichées sur l'écran. Pour pouvoir visualiser ces informations, l'UIP doit obtenir l'accord du procureur [général] d'Etat ou de son délégué ou, si la requête émane du Service de Renseignement de l'Etat, l'accord de la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de Renseignement de l'Etat.

Le système technique devra été conçu de manière à ce que les données masquées ne puissent être consultées qu'après que l'accord de l'autorité compétente désignée en vertu du présent article aura été obtenu et qu'il soit possible de retracer les opérations de démasquage effectuées.

Des prescriptions de service interne à l'UIP devront établir une procédure à suivre par l'opérateur lorsqu'un *hit* est généré parmi des données PNR masquées. ».

L'article 27 transpose l'article 12, paragraphe 5 de la directive et concerne la durée de conservation du résultat de l'évaluation réalisée sur base de l'article 10. Cette durée correspond au temps nécessaire pour informer les services compétents et, le cas échéant, les UIP, de l'existence d'une concordance positive. Au cas où le réexamen individuel manuel révèle un résultat du traitement automatisé négatif, celui-ci peut être archivé par l'UIP aussi longtemps que les données de base n'ont pas été effacées, ceci pour éviter de futures fausses concordances positives.

Chapitre 10 – *Protection des données à caractère personnel*

Articles 28 à 36

L'article 28 transpose l'article 13 de la directive.

Dans son avis, le Conseil d'État constate « que le projet sous avis, contrairement à l'article 13 de la directive, retient le principe de la compétence de la CNPD[3] ainsi que l'application du régime général sur la protection des données[4] aux données PNR collectées, pour ne mentionner la loi de transposition de la directive (UE) 2016/680 qu'en début de la disposition pour réserver les droits des autorités judiciaires. Il est dès lors en porte-à-faux avec le texte à transposer qui vise expressément la décision-cadre 2008/977/JAI, remplacée par la directive (UE) 2016/680, et ne retient l'application du régime de droit commun de la protection des données que pour le traitement des données à caractère personnel effectué par les transporteurs aériens[5], de telle sorte que le Conseil d'État doit s'opposer formellement au texte actuel, qui constitue une transposition incorrecte de la directive. ».

Par amendement gouvernemental du 27 avril 2018, le texte a été reformulé et se réfère à l'article 40 [devenu l'article 39] de la future loi portant transposition de la directive sur la protection des données en matière pénale. Le commentaire précise que « Dans la mesure où cette loi désigne la CNPD comme autorité compétente pour contrôler les traitements des données en matière pénale autres que ceux effectués par les juridictions de jugement, ce sera également la CNPD qui sera compétente pour contrôler le traitement des données PNR. Etant donné que les missions et les pouvoirs de cette commission sont définis par la loi portant sur le régime général, il est renvoyé à cette loi pour ce qui est des missions et des pouvoirs de la CNPD. ».

L'article 29 est relatif au délégué à la protection des données désigné par le responsable de l'UIP. Il transpose l'article 5 et l'article 6, paragraphe 6 de la directive. Sur demande du Conseil d'État, le paragraphe 4, alinéa 2 a été complété pour préciser la base légale permettant la saisine de la CNPD.

L'article 30 détermine les informations que l'UIP met à la disposition du public.

L'article 31 transpose l'article 13, paragraphe 1er de la directive. Il est consacré aux droits des personnes dont les données sont traitées, ces droits étant définis par référence aux articles pertinents du projet de loi 7168 portant transposition de la directive sur la protection des données pénales.

L'article 32 transpose l'article 6, paragraphe 8 de la directive qui oblige les UIP à stocker, traiter et analyser les données PNR exclusivement dans un ou des endroits sécurisés situés sur le territoire de l'État membre.

---

3 Commission nationale pour la protection des données

4 Projet de loi 7184

5 Directive (UE) 2016/681, article 13, paragraphe 3

Transposant l'article 13, paragraphes 2 et 7 de la directive, l'article 33 oblige le responsable de l'UIP de mettre en œuvre des mesures et des procédures techniques pour garantir un niveau élevé de sécurité des données.

En vertu de l'article 34 qui transpose l'article 13, paragraphe 5 de la directive, l'UIP doit conserver une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

L'article 35, transposant l'article 13, paragraphe 6 de la directive, a pour objet l'obligation pour l'UIP de tenir des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

L'article 36 transpose l'article 13, paragraphe 8 de la directive et prévoit l'information obligatoire, sans retard injustifié, de la personne concernée et de la CNPD, lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection de ces données ou d'affecter négativement la vie de la personne concernée.

Chapitre 11 – *Sanctions*

Articles 37 et 38

Ces articles transposent l'article 14 de la directive.

L'article 37, alinéa 1er punit, dans sa version initiale, la violation des articles 8, 15 et 36 de sanctions pénales. S'agissant de l'article 8, le Conseil d'État demande, afin d'assurer le respect du principe constitutionnel de la légalité de la peine, de préciser lequel des deux comportements visés à l'article 8 est sanctionné : le traitement illicite ou le défaut d'effacement des données concernées ou les deux. Il exige en outre de préciser s'il s'agit d'une infraction intentionnelle ou non, considérant « qu'un simple dysfonctionnement au sein de l'unité, dépourvu de toute intention criminelle, qui serait éventuellement sanctionnable du point de vue disciplinaire, n'est pas de nature à entraîner la responsabilité pénale, que ce soit du responsable de l'unité ou du fonctionnaire à l'origine du traitement en question ».

La question de l'intention de l'auteur du fait incriminé se pose également pour l'article 15.

Pour ce qui est de l'article 36, lequel oblige l'UIP à informer sans retard injustifié la personne concernée et l'autorité de contrôle d'une atteinte aux données à caractère personnel, le Conseil d'État met en doute « la faisabilité matérielle de l'information de la personne concernée qui, dans la grande majorité des cas, risque de ne pas résider sur le territoire national ».

Par conséquent, l'article 37 a fait l'objet d'un amendement gouvernemental tenant compte des avis du Conseil d'État et des autorités judiciaires. Le nouveau libellé précise que l'infraction consiste en une violation intentionnelle de l'interdiction de traiter des données sensibles, telle que prévue à l'article 8, alinéa 1er. Les auteurs de l'amendement indiquent ne pas avoir retenu la demande des Parquets de Luxembourg et de Diekirch de fixer un délai maximal pour l'effacement des données ; en effet, en fixant un délai pour ce faire, alors que la directive fait obligation d'effacer ces données immédiatement, il existe le risque que la Commission européenne considère que la législation luxembourgeoise ne serait sur ce point pas conforme à la directive.

Concernant l'article 15, l'article 37 amendé précise que la violation de la disposition, selon laquelle une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peut être prise sur la seule base du traitement automatisé de données PNR, doit être intentionnelle. Par ailleurs, a également été érigé en infraction pénale le fait de prendre une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative qui serait fondée sur 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.

L'article 36 a été retiré de la liste des infractions pénales suite aux doutes du Conseil d'État au sujet de la faisabilité matérielle de l'information de la personne concernée.

Le Conseil d'État et les Parquets ont été suivis en faisant de la cessation du traitement illégal une obligation pour la juridiction de jugement.

Au sujet de l'article 49 [devenu l'article 47], paragraphe 2 [devenu le paragraphe 3] du projet de loi 7168, les auteurs de l'amendement font remarquer que cette disposition n'est pas applicable en matière de données PNR, puisque l'article 37 du projet de loi PNR ne renvoie dans son alinéa 2 qu'aux

paragraphes 1er, 3 à 5 [devenus les paragraphes 2 et 4 à 6] du projet de loi n° 7168. Les auteurs « ne partagent dès lors pas la crainte soulevée par le Conseil d'État par rapport à une éventuelle incohérence entre les dispositions pénales mises en place par les deux textes ».

L'article 38 punit d'une amende maximale de 50 000 € le transporteur aérien pour chaque vol pour lequel il n'a pas transmis les renseignements visés à l'article 3, ne les a pas transmis dans le délai prévu ou selon les modalités ou dans les formes prescrites.

Dans son avis du 30 mars 2018, le Conseil d'État « constate que le droit positif connaît déjà à l'heure actuelle une disposition qui règle une situation tout à fait analogue.

En effet, l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration punit d'une amende d'un montant maximum de 5 000 euros les entreprises de transport aérien visées à l'article 108 de la même loi « à raison de chaque voyage pour lequel l'entreprise, par faute, n'a pas transmis les renseignements y visés ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis des renseignements incomplets ou erronés », amende qui est prononcée par le ministre ayant l'Immigration dans ses attributions. L'article 108, quant à lui, dispose en son paragraphe 1er qu'encourt les sanctions prévues aux articles 147 et 148 toute « entreprise de transport aérien qui (…) n'a pas transmis les renseignements visés à l'article 106 ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis les renseignements incomplets ou erronés ». L'article 106, de son côté, prévoit en son paragraphe 1er qu'« afin de prévenir un refus d'entrée sur le territoire, les entreprises de transport aérien ont l'obligation de transmettre à la Police grand-ducale les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire du Grand-duché de Luxembourg en provenance d'un pays non-membre de l'Union européenne ».

S'il est vrai que la disposition sous examen vise la transmission de données relatives à des vols en provenance non pas d'États non membres de l'Union européenne, mais provenant d'États membres, que la communication doit se faire non pas à la Police grand-ducale mais à l'UIP, qui fait cependant partie de cette même police, et que le ministre sanctionnateur est un autre, les faits incriminés sont identiques sur tous les autres points, de telle sorte que le Conseil d'État s'interroge sur les raisons qui ont fait que le projet sous avis prévoit une amende dont le maximum est le décuple des sanctions prévues dans la disposition déjà existante, créant ainsi une inégalité de traitement selon l'origine du passager transporté, toutes autres choses étant égales par ailleurs.

Dans l'attente de recevoir des explications sur cette différence de traitement, le Conseil d'État est obligé de réserver sa position quant à la dispense du second vote. »

Les auteurs du projet de loi ont donné les explications demandées dans le contexte de l'amendement gouvernemental 26 du 27 avril 2018. Dans son avis complémentaire, le Conseil en prend acte et retire sa réserve.

Les auteurs rappellent que « La sanction à laquelle fait référence le Conseil d'État a été introduite par la loi du 21 décembre 2006 portant transposition, entre autres, de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (« directive API »). S'il est partant vrai que la loi de transposition de la directive API et le projet de loi de transposition de la directive PNR prévoient tous les deux des sanctions administratives à l'encontre des transporteurs aériens qui ne transfèrent pas les données ou ne les transfèrent pas selon les conditions requises, la différence fondamentale entre les deux textes, et qui d'après les auteurs du projet de loi PNR justifie la différence au niveau des sanctions encourues, réside dans la finalité pour laquelle les données des passagers sont recueillies. Ainsi, l'objectif de la directive API consiste, tel qu'il ressort de son article 1er, à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine. Les données API sont des informations biographiques extraites de la partie du passeport lisible par machine et servent d'outils de vérification des identités et de gestion aux frontières. Ces données ne présentent pas d'intérêt pour l'évaluation des personnes ni pour le dépistage des délinquants ou terroristes « inconnus ». En effet, « *une utilisation à la fois proactive et en temps réel des données PNR permet donc aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent, par rapport à ce que permet le traitement d'autres catégories de données à caractère personnel. Comme expliqué ci-dessous, le traitement de données à caractère personnel accessibles aux services répressifs dans le cadre d'instruments de l'UE actuels et futurs, tels que la directive relative aux informations préalables sur les passagers, le système d'information Schengen (SIS) et le système d'information Schengen de deuxième génération (SIS II), ne donne pas aux services répressifs la possibilité d'identifier des suspects « inconnus » comme le permet l'analyse*

de données PNR. Deuxièmement, après la commission d'une infraction, les données PNR aident les services répressifs à prévenir et à détecter d'autres infractions graves, dont des actes de terrorisme, et à enquêter sur celles-ci et à poursuivre leurs auteurs. À cet effet, les services répressifs doivent utiliser les données PNR en temps réel, pour les confronter à diverses bases de données de personnes « connues » et d'objets recherchés. Ils doivent également en faire un usage réactif, pour rassembler des preuves et, au besoin, trouver d'éventuels complices et démanteler des réseaux criminels. »[6]

Les données PNR sont recueillies pour une finalité complètement différente, à savoir qu'ils constituent un moyen de prévention et de lutte contre le terrorisme et les formes graves de criminalité telles que la traite des êtres humains, l'exploitation sexuelle des enfants, le trafic d'armes, le vol organisé ou l'aide à l'entrée et le séjour irréguliers. Cette dernière infraction illustre d'ailleurs très bien la différence entre les finalités des traitements des données API et des données PNR. Ainsi, si la directive API vise à prévenir l'immigration illégale, qui ne constitue pas une infraction pénale, la directive PNR crée des moyens destinés à protéger la sécurité et la vie des personnes. Il n'y a aucun doute que les conséquences d'un défaut de transmission de données à des fins de contrôle des frontières ne sont pas les mêmes qu'un défaut de transmission de données qui peuvent permettre de prévenir une attaque terroriste ou un autre crime grave. La différence entre les sanctions encourues dans les deux cas de figure est dès lors justifiée.

Il importe par ailleurs de relever que l'article 14 de la directive PNR oblige les États membres à prévoir des sanctions effectives, proportionnées et dissuasives à l'encontre des transporteurs aériens qui ne transmettent pas les données comme le prévoit l'article 8 ou ne les transmettent pas dans le format requis. Comme il a été expliqué dans le commentaire de l'article 38, les auteurs du texte se sont alignés sur les montant[s] des amendes fixées dans d'autres États membres, notamment la France, la Belgique et l'Allemagne. Il est à craindre que si le Luxembourg alignait la sanction encourue par le transporteur aérien qui omet de transférer les données PNR sur la sanction prévue par la loi précitée de 2008 sur l'immigration, la Commission européenne risquerait de considérer la sanction prévue dans le présent projet de loi comme ne remplissant pas les exigences posées par l'article 14 de la Directive. ».

Chapitre 12 – *Dispositions modificatives*

Articles 39 et 40

Ce chapitre a été ajouté par amendement gouvernemental du 27 février 2018.

L'article 39 a fait l'objet de deux oppositions formelles du Conseil d'État. La première concerne l'ajout d'un paragraphe 4 à l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État. Le Conseil d'État rappelle que l'article 5 de cette loi « énumère les moyens et mesures de recherche dont dispose le SRE et qui, pour leur mise en œuvre, nécessitent une autorisation écrite du directeur du service, suite à une demande motivée et écrite de l'agent du SRE chargé du dossier. La nouvelle disposition ajoute à ces moyens et mesures de recherche la possibilité pour le SRE de demander à l'UIP la communication des données PNR dans le cadre de ses activités.

L'amendement 2 est à lire avec l'amendement 3, qui tend à supprimer le point a) de l'article 8 de la loi précitée du 5 juillet 2016, prévoyant que le SRE peut être autorisé par le Comité ministériel du renseignement, instauré par le paragraphe 2 de l'article 2 de ladite loi, de « solliciter (…) les données des dossiers passagers relatives à une ou plusieurs personnes identifiées ou identifiables au sujet desquels le SRE dispose d'un ou de plusieurs indices concordants relatifs à une menace actuelle ou potentielle visant la sécurité nationale ou les intérêts visés à l'article 3. Le transporteur de personnes par voie aérienne visé par la demande doit fournir sa réponse sans délai. ». Cette mesure ne peut cependant être autorisée par ledit comité, au vœu du paragraphe 1er de l'article 8, que « si les moyens et les mesures de recherche dont dispose le SRE en vertu des articles 5, 6, et 7 (de la loi précitée) s'avèrent inopérants en raison de la nature des faits et des circonstances spécifiques de l'espèce ».

Il résulte de la combinaison de ces deux amendements que la mesure de l'article 8, permettant au SRE de contacter directement les opérateurs de transports aériens, sera remplacée par la possibilité pour ledit service de demander des renseignements à l'UIP et ne pourra plus être utilisée en conséquence.

---

6 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 (COM/2011/0032 final)

Cet amendement pose cependant problème en ce que, en limitant les finalités de l'accès du SRE aux données de l'UIP, il reste en deçà de l'article 13 du projet de loi sous examen et en réduit par conséquent la portée, entraînant ainsi une transposition incorrecte de la directive, à laquelle le Conseil d'État doit s'opposer formellement. ».

Les auteurs de l'amendement ont par conséquent suivi le Conseil d'État en complétant l'article 13 par une référence à l'article 5, paragraphe 4, de la loi précitée du 5 juillet 2016.

La seconde opposition formelle se rapporte à l'alinéa 2 du paragraphe 4 nouveau ajouté par l'amendement 2 ci-dessus à l'article 5 de la loi précitée du 5 juillet 2016. Pour le Conseil d'État, le fait de prévoir « que le directeur du SRE « rapporte tous les six mois par écrit » au prédit comité « la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquelles l'exercice des missions a exigé la demande de communication » n'est pas de nature à garantir suffisamment les droits des personnes concernées, cela d'autant plus que la procédure invoquée par les auteurs de l'amendement et prévue à l'article 5, paragraphe 3, de la loi précitée du 5 juillet 2016, qui a trait aux observations dans les lieux publics ainsi qu'aux inspections de lieux publics, prévoit un rapport par écrit au comité une fois par mois, et non pas une fois chaque semestre.

Il s'oppose par conséquent formellement à l'amendement sous avis pour contravention à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 11, paragraphe 3, de la Constitution pour autant qu'il réduit la fréquence du prédit rapport à un rapport semestriel, ce qui est totalement insuffisant pour garantir les droits des personnes concernées. ».

En conséquence, l'alinéa 2 du paragraphe 4 nouveau ajouté à l'article 5 de la loi précitée du 5 juillet 2016 a été amendé de manière à prévoir un rapport mensuel.

Chapitre 13 – *Disposition finale*

Article 41

Sans observation.

Annexes I et II

Sans observation.

*

Compte tenu des observations qui précèdent, la Commission de la Force publique propose en sa majorité à la Chambre des Députés d'adopter le projet de loi dans la teneur suivante :

*

7151

PROJET DE LOI

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

Chapitre 1er – *Dispositions générales*

Art. 1er. La présente loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Art. 2. Pour l'application de la présente loi, on entend par :

1° « transporteur aérien » : toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes ;

2° « passager » : toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers ;

3° « dossier passager » : le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités ;

4° « système de réservation » : le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations ;

5° « système de contrôle des départs » : le système utilisé pour contrôler les passagers lors de l'embarquement ;

6° « données PNR » : les données contenues dans le dossier passager et énumérées à l'annexe I ;

7° « méthode push » : la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'informations passagers telle que créée à l'article 3 ;

8° « infractions terroristes » : les infractions visées au Livre II, Titre 1ier, Chapitre III-1 du Code pénal ;

9° « formes graves de criminalité » : les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans ;

10° « dépersonnaliser par le masquage d'éléments des données » : rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée ;

11° « services compétents » : les services visés à l'article 13.

Chapitre 2 – *Unité d'informations passagers*

Art. 3. Il est créé au sein de la Police grand-ducale une Unité d'informations passagers, ci-après désignée « UIP », qui est chargée :

1° de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données ;

2° du transfert de ces données et des résultats de leur traitement aux services compétents ;

3° de l'échange de ces données et des résultats de leur traitement avec les unités d'informations passagers des autres Etats membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4. (1) Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Il est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

(2) Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel de l'Administration des douanes et accises et du Service de renseignement de l'Etat. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Les membres du personnel de l'Administration des douanes et accises et du Service de renseignement de l'Etat sont désignés à l'UIP par une décision conjointe du ministre ayant la Police grand-ducale dans ses attributions et du ministre du ressort. Ils continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Art. 5. Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la méthode push, les données PNR de tous les passagers en provenance de, à destination de ou transitant par le Luxembourg pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien.

Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR incombe au transporteur aérien qui assure le vol.

Art. 6. (1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes :

1° 48 heures avant l'heure de départ programmée du vol ;

2° 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 qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point 2°, peut se limiter à une mise à jour du transfert visé à l'alinéa 1er, point 1°.

(2) Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP peut demander, au cas par cas, le transfert de données PNR en dehors des délais prévus au paragraphe 1er.

Art. 7. (1) Les données PNR sont transférées à l'UIP par voie électronique au moyen de protocoles communs et de formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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.

Les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisés pour leurs transferts.

(2) En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union européenne en matière de protection des données soit pleinement respecté.

(3) Dans l'hypothèse où un transporteur aérien ne conserve pas les données API énumérées à l'annexe I, point 18, par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, il transfère également ces données par la méthode « push » à l'UIP. Dans le cas d'un tel transfert, toutes les dispositions de la présente loi s'appliquent à ces données API.

Chapitre 4 – *Traitement des données PNR*

Art. 8. Le traitement de données PNR qui révèlent 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 est interdit.

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive.

Art. 9. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données supplémentaires dès réception et de façon définitive.

Art. 10. (1) L'UIP traite les données PNR en vue de réaliser une évaluation des passagers avant leur arrivée prévue sur le territoire national ou leur départ prévu du territoire national afin d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis compte tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

(2) Pour réaliser cette évaluation l'UIP peut comparer les données PNR :

1° aux traitements de données à caractère personnel mis en œuvre par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;

2° à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur 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.

(3) L'UIP réexamine individuellement, par des moyens non automatisés, toute concordance positive obtenue à la suite d'un traitement automatisé des données PNR effectué en vertu du présent article.

(4) L'UIP transmet aux services compétents, au cas par cas, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au présent article ou le résultat du traitement de ces données.

(5) Les conséquences de l'évaluation des passagers ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union européenne à la libre circulation sur le territoire du Grand-Duché de Luxembourg tel que prévu par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.

(6) Lorsque les évaluations sont réalisées pour des vols entre le Grand-Duché de Luxembourg et un autre Etat membre de l'Union européenne auquel s'applique le règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), les conséquences de ces évaluations doivent respecter ledit règlement.

Art. 11. L'UIP traite les données PNR afin de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations visées à l'article 10.

Art. 12. L'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, dûment motivées et fondées sur des motifs suffisants visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques aux fins visées à l'article 1er, et visant à communiquer aux services compétents ou, le cas échéant, à Europol, le résultat de ce traitement.

Chapitre 5 – *Services compétents*

Art. 13. Sont habilités à demander à l'UIP ou à recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, en vue de procéder à un examen approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et poursuites en la matière :

1° la Police grand-ducale ;

2° le Service de renseignement de l'Etat conformément à l'article 5, paragraphe 4, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat ;

3° l'Administration des douanes et accises.

En recherchant les crimes et délits visés à l'article 2, points 8° et 9°, le procureur d'Etat peut, par une décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 12.

Art. 14. Les services compétents ne peuvent traiter les données PNR et le résultat du traitement de ces données que pour les finalités de la présente loi telles que définies à l'article 1er.

L'alinéa 1er est sans préjudice des compétences de la Police grand-ducale et de l'Administration des douanes et accises lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement.

Art. 15. Les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Les décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peuvent pas être fondées sur 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.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Art. 16. Lorsqu'une personne est identifiée conformément à l'article 10, l'UIP communique toutes les données pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP des autres Etats membres de l'Union européenne concernés.

Lorsque l'UIP est destinataire d'informations telles que visées à l'alinéa 1er de la part d'une autre UIP, elle transmet ces informations aux services compétents.

Art. 17. (1) L'UIP transmet, dès que possible, à l'UIP d'un autre Etat membre de l'Union européenne qui en fait la demande, les données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par masquage conformément à l'article 26, et, si nécessaire, le résultat de tout traitement de ces données, s'il a déjà été réalisé conformément à l'article 10.

La demande, dûment motivée, peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière.

Si les données demandées ont été dépersonnalisées par masquage conformément à l'article 26, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que le transfert est nécessaire aux fins visées à l'article 12 et si elle y est autorisée par le procureur général d'Etat ou son délégué.

Les dispositions du présent paragraphe ne portent pas atteinte aux dispositions tant internationales que nationales sur l'entraide judiciaire internationale en matière pénale.

(2) Dans des cas d'urgence, les autorités compétentes des autres Etats membres, désignées conformément à l'article 7, paragraphe 1er , de la directive (UE) 2016/661 du Parlement européen et du Conseil du 27 avril 2016 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 et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe 1er sont applicables.

(3) À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un État membre a le droit de demander à ce que l'UIP obtienne des données PNR conformément à l'article 6, paragraphe 2, et les communique à l'UIP requérante.

Art. 18. L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres Etats membres de l'Union européenne des données PNR ou les résultats du traitement de ces données.

Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre Etat membre de l'Union européenne, il transmet copie de sa demande à l'UIP.

Art. 19. L'échange de données effectué en application du présent chapitre peut avoir lieu par l'intermédiaire de tous les canaux de coopération existant entre les services compétents des Etats membres de l'Union européenne.

La langue utilisée pour la demande et l'échange des données est celle applicable au canal utilisé.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Art. 20. (1) Dans les limites de ses compétences et pour l'accomplissement de ses missions, Europol peut présenter à l'UIP, au cas par cas, par l'intermédiaire de son unité nationale, une demande électronique dûment motivée visant à obtenir des données PNR spécifiques ou le résultat du traitement de ces données :

1° lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des Etats membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes dans la matière et ;

2° dans la mesure où ladite infraction relève de la compétence d'Europol.

(2) La demande énonce les motifs sur lesquels s'appuie Europol pour estimer que la transmission de données PNR ou du résultat de traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée ou à des enquêtes en la matière.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Art. 21. L'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si :

1° l'une des conditions prévues à l'article 34, paragraphe 1er, point d) de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est remplie ;

2° l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité ;

3° le transfert est nécessaire aux fins telles que définies à l'article 1er ;

4° le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er ;

5° les conditions prévues à l'article 17, paragraphe 1er sont remplies.

Les dispositions du présent article ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

Art. 22. (1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre Etat membre de l'Union européenne à un pays non membre de l'Union européenne que si l'Etat membre auprès duquel les données ont été collectées a donné son accord au transfert.

(2) Dans des circonstances exceptionnelles, les données PNR peuvent être transférées à un pays non membre de l'Union européenne sans l'accord du pays membre de l'Union européenne auprès duquel les données ont été collectées si les conditions suivantes sont remplies :

1° 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 Etat membre de l'Union européenne ou un pays tiers ;

2° l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'Etat membre de l'Union européenne, qui n'a pas pu donner son accord en temps utile, est informée sans retard et le transfert est dûment enregistré et soumis à une vérification à posteriori.

Art. 23. L'UIP ne peut transférer des données PNR et les résultats du traitement de ces données aux autorités compétentes de pays non membres de l'Union européenne qu'après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte les conditions et garanties de la présente loi.

Art. 24. Le délégué à la protection des données visé à l'article 29 est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Art. 25. L'UIP conserve les données PNR pendant une durée maximale de cinq ans à compter du transfert par le transporteur aérien.

A l'issue de cette période de cinq ans, elle efface les données PNR de manière définitive. Cette disposition ne s'applique pas si les données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière.

Art. 26. (1) À l'expiration d'une période de six mois à compter du transfert par le transporteur aérien, l'UIP dépersonnalise les données PNR par le masquage des éléments suivants :

1° le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR ;

2° l'adresse et les coordonnées ;

3° des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne ;

4° les informations « grands voyageurs » ;

5° les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte ;

6° toute donnée API qui a été recueillie.

(2) À l'expiration de la période de six mois visée au paragraphe 1er, la communication de l'intégralité des données PNR n'est autorisée que sous les conditions suivantes :

1° elle est nécessaire aux fins visées à l'article 12 ;

2° elle a été approuvée par le procureur général d'Etat ou son délégué ou, si les données sont destinées à être communiquées au Service de renseignement de l'Etat, par la commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Art. 27. L'UIP ne conserve le résultat de l'évaluation réalisée en vertu de l'article 10 que le temps nécessaire pour informer les services compétents et, s'il y a lieu, les UIP des autres États membres de l'Union européenne de l'existence d'une concordance positive.

Lorsque, à la suite du réexamen individuel par des moyens non automatisés conformément à l'article 10, paragraphe 3, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées en vertu de l'article 25, de manière à éviter de futures fausses concordances positives.

Chapitre 10 – *Protection des données à caractère personnel*

Art. 28. L'autorité de contrôle visée à l'article 39 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 8 de la loi du jj/mm/aaaa portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et elle dispose, à cette fin, des pouvoirs prévus à l'article 14 de la même loi.

Art. 29. (1) Le responsable de l'UIP désigne un délégué à la protection des données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

(2) Le délégué à la protection des données contrôle le traitement des données PNR et met en œuvre les garanties pertinentes au sein de l'UIP.

Il informe et conseille le responsable et le personnel de l'UIP sur les obligations qui leur incombent en matière de protection des données.

Il fait office de point de contact pour les personnes concernées pour toutes les questions relatives au traitement de leurs données PNR et pour la Commission nationale pour la protection des données.

(3) Le délégué à la protection des données effectue ses missions en toute indépendance.

Il fait directement rapport au responsable de l'UIP.

Par dérogation à l'alinéa 2, et sans préjudice du paragraphe 4, alinéa 2, en cas de problèmes relevant de la protection des données, le délégué à la protection des données rapporte directement au directeur général de la Police grand-ducale ou, s'il juge nécessaire, au ministre ayant la Police grand-ducale dans ses attributions.

(4) Le délégué à la protection des données a accès à toutes les données traitées par l'UIP.

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données conformément à la loi du jj/mm/aaaa portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Art. 30. L'UIP met à la disposition du public, par les moyens de communication appropriés, les informations suivantes :

1° ses coordonnées ;

2° les coordonnées du délégué à la protection des données ;

3° les finalités du traitement auquel sont destinées les données PNR ;

4° le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité ;

5° l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31. (1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 13 à 17 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 44 à 46 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 32. L'UIP conserve, traite et analyse les données PNR en un ou des endroits sécurisés situés sur le territoire du Grand-Duché de Luxembourg.

Art. 33. Le responsable de l'UIP met en œuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et la nature des données PNR.

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en œuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 28, paragraphe 2 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 34. L'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

Cette documentation comprend :

1° le nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès ;

2° les demandes formulées par les services compétents et les UIP des autres Etats membres de l'Union européenne ;

3° toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Art. 35. L'UIP tient des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

Les registres des opérations de consultation et de communication indiquent la finalité, la date et l'heure de l'opération et l'identité de la personne qui a consulté ou communiqué les données PNR ainsi que l'identité des destinataires de ces données.

Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit.

L'UIP met les registres à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Les registres sont conservés pendant cinq ans.

Art. 36. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe sans retard injustifié la personne concernée et la Commission nationale pour la protection des données de cette atteinte.

Chapitre 11 – *Sanctions*

Art. 37. La violation intentionnelle de l'article 8, alinéa 1er et de l'article 15 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125 000 euros ou d'une de ces peines seulement. La juridiction saisie prononce la cessation du traitement contraire aux dispositions de l'article 8, alinéa 1er et de l'article 15 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 47, paragraphes 1er, 2, 4, 5 et 6 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38. (1) Est puni d'une amende d'un montant maximum de 50 000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements visés à l'article 3, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

(2) Le manquement est constaté par un procès-verbal établi par la Police grand-ducale. Copie en est transmise au transporteur aérien.

Le transporteur aérien a accès au dossier et est mis à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction.

L'amende est prononcée par le ministre ayant la Police grand-ducale dans ses attributions.

(3) La décision du ministre qui est motivée est susceptible d'un recours en réformation à introduire devant le Tribunal administratif dans un délai d'un mois à compter de la notification.

Chapitre 12 – *Dispositions modificatives*

Art. 39. Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

« (4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, ou de cyber-menace dans la mesure où celle-ci est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12, de la loi du jj/mm/aaaa relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Le directeur du SRE rapporte tous les mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en œuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Art. 40. À l'article 8, paragraphe 1er de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, la lettre a) est supprimée.

Chapitre 13 – *Disposition finale*

Art. 41. La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « Loi du jj/mm/aaaa relative au traitement des données des dossiers passagers ».

*

ANNEXE I

Liste des données PNR

1° Code repère du dossier passager ;

2° Date de réservation/d'émission du billet ;

3° Date(s) prévue(s) du voyage ;

4° Nom(s) ;

5° Adresse et coordonnées (numéro de téléphone, adresse électronique) ;

6° Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation ;

7° Itinéraire complet pour le PNR concerné ;

8° Informations « grands voyageurs » ;

9° Agence de voyages/agent de voyages ;

10° Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation ;

11° Indications concernant la scission/division du PNR ;

12° Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée) ;

13° Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix ;

14° Numéro du siège et autres informations concernant le siège ;

15° Informations sur le partage de code ;

16° Toutes les informations relatives aux bagages ;

17° Nombre et autres noms de voyageurs figurant dans le PNR ;

18° Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée) ;

19° Historique complet des modifications des données PNR énumérées aux points 1 à 18.

*

ANNEXE II

Liste des infractions visées à l'article 2, point 9

1° Participation à une organisation criminelle ;
2° Traite des êtres humains ;
3° Exploitation sexuelle des enfants et pédopornographie ;
4° Trafic de stupéfiants et de substances psychotropes ;
5° Trafic d'armes, de munitions et d'explosifs ;
6° Corruption ;
7° Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union ;
8° Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro ;
9° Cybercriminalité ;
10° Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées ;
11° Aide à l'entrée et au séjour irréguliers ;
12° Meurtre, coups et blessures graves ;
13° Trafic d'organes et de tissus humains ;
14° Enlèvement, séquestration et prise d'otage ;
15° Vol organisé ou vol à main armée ;
16° Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art ;
17° Contrefaçon et piratage de produits ;
18° Falsification de documents administratifs et trafic de faux ;
19° Trafic de substances hormonales et d'autres facteurs de croissance ;
20° Trafic de matières nucléaires et radioactives ;
21° Viol ;
22° Infractions graves relevant de la Cour pénale internationale ;
23° Détournement d'avion/de navire ;
24° Sabotage ;
25° Trafic de véhicules volés ;
26° Espionnage industriel.

Luxembourg, le 19 juillet 2018

La Présidente-Rapportrice,
Claudia DALL'AGNOL

Impression: CTIE – Division Imprimés et Fournitures de bureau

7151

J-2017-0-1593 (PL 7151)

Bulletin de Vote (Vote Public)

Date:	26/07/2018 17:59:58		
Scrutin:	9	Président:	M. Di Bartolomeo Mars
Vote:	PL 7151 Trait. des données passagers	Secrétaire A:	M. Frieseisen Claude
Description:	Projet de loi 7151	Secrétaire B:	Mme Barra Isabelle

	Oui	Abst	Non	Total
Présents:	47	3	2	52
Procuration:	8	0	0	8
Total:	55	3	2	60

Nom du député	Vote	(Procuration)	Nom du député	Vote	(Procuration)
CSV					
Mme Adehm Diane	Oui		Mme Andrich-Duval Sylvie	Oui	
Mme Arendt Nancy	Oui		M. Eicher Emile	Oui	
M. Eischen Félix	Oui		M. Gloden Léon	Oui	
M. Halsdorf Jean-Marie	Oui		Mme Hansen Martine	Oui	
Mme Hetto-Gaasch Françoise	Oui		M. Kaes Aly	Oui	
Mme Konsbruck Claudine	Oui		M. Lies Marc	Oui	
Mme Mergen Martine	Oui		M. Meyers Paul-Henri	Oui	
Mme Modert Octavie	Oui		M. Mosar Laurent	Oui	(Mme Mergen Martine)
M. Roth Gilles	Oui		M. Schank Marco	Oui	(Mme Arendt Nancy)
M. Spautz Marc	Oui		M. Wilmes Serge	Oui	(Mme Modert Octavie)
M. Wiseler Claude	Oui		M. Wolter Michel	Oui	
M. Zeimet Laurent	Oui	(Mme Hansen Martine)			
LSAP					
M. Angel Marc	Oui		M. Arndt Fränk	Oui	
Mme Asselborn-Bintz Simone	Oui		M. Bodry Alex	Oui	
Mme Bofferding Taina	Oui	(Mme Dall'Agnol Claudia)	Mme Burton Tess	Oui	
M. Cruchten Yves	Oui		Mme Dall'Agnol Claudia	Oui	
M. Di Bartolomeo Mars	Oui		M. Engel Georges	Oui	
M. Fayot Franz	Oui		M. Haagen Claude	Oui	
Mme Hemmen Cécile	Oui				
déi gréng					
M. Anzia Gérard	Oui		M. Kox Henri	Oui	
Mme Lorsché Josée	Oui		Mme Loschetter Viviane	Oui	
Mme Tanson Sam	Oui		M. Traversini Roberto	Oui	(Mme Loschetter Viviane)
DP					
M. Bauler André	Oui		M. Baum Gilles	Oui	
Mme Beissel Simone	Oui		M. Berger Eugène	Oui	
M. Colabianchi Frank	Oui		M. Delles Lex	Oui	(M. Graas Gusty)
Mme Elvinger Joëlle	Oui		M. Graas Gusty	Oui	
M. Hahn Max	Oui		M. Krieps Alexander	Oui	
M. Lamberty Claude	Oui		M. Mertens Edy	Oui	
Mme Polfer Lydie	Oui	(M. Bauler André)			
déi Lénk					
M. Baum Marc	Non		M. Wagner David	Non	
ADR					
M. Gibéryen Gast	Abst.		M. Kartheiser Fernand	Abst.	
M. Reding Roy	Abst.				

Le Président:

Le Secrétaire général:

7151 - Dossier consolidé : 197

7151/10

N° 7151[10]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant organisation du Service de renseignement de l'Etat

* * *

DISPENSE DU SECOND VOTE CONSTITUTIONNEL PAR LE CONSEIL D'ETAT

(27.7.2018)

Le Conseil d'État,

appelé par dépêche du Président de la Chambre des députés, du 26 juillet 2018 à délibérer sur la question de dispense du second vote constitutionnel du

PROJET DE LOI

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant organisation du Service de renseignement de l'Etat

qui a été adopté par la Chambre des députés dans sa séance du 26 juillet 2018 et dispensé du second vote constitutionnel ;

Vu ledit projet de loi et les avis émis par le Conseil d'État en ses séances des 30 mars et 26 juin 2018 ;

se déclare d'accord

avec la Chambre des députés pour dispenser le projet de loi en question du second vote prévu par l'article 59 de la Constitution.

Ainsi décidé en séance publique à l'unanimité des 14 votants, le 27 juillet 2018.

Le Secrétaire général,
Marc BESCH

Le Président du Conseil d'État,
Georges WIVENES

Impression: CTIE – Division Imprimés et Fournitures de bureau

11

Session ordinaire 2017-2018

MW/PR P.V. FRP 11

Commission de la Force publique

Procès-verbal de la réunion du 19 juillet 2018

Ordre du jour :

1. Approbation des projets de procès-verbal des réunions du 25 juin 2018 et du 5 juillet 2018

2. 7151 Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant organisation du Service de renseignement de l'État
- Rapporteur : Madame Claudia Dall'Agnol

- Présentation et adoption d'un projet de rapport

*

Présents : M. Marc Angel, M. Eugène Berger (en rempl. de M. Gusty Graas), M. Alex Bodry, Mme Claudia Dall'Agnol, M. Léon Gloden, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Henri Kox

M. Fränk Reimen, Direction, Mme Martine Schmit, du Ministère de la Sécurité intérieure

Mme Marianne Weycker, de l'Administration parlementaire

*

Présidence : Mme Claudia Dall'Agnol, Présidente de la Commission

*

1. Approbation de projets de procès-verbal

Les projets de procès-verbal sont approuvés.

2. Projet de loi 7151

Madame la Présidente-Rapportrice rend attentif à la nécessité d'adapter quelques références dans le texte du projet de loi à certaines dispositions des projets de loi 7168 et

7184 suite aux amendements apportés à ceux-ci. Le Conseil d'État en sera informé par courrier.

Un membre de la commission souhaiterait savoir, en premier lieu, si l'UIP fonctionnera 24/24 et, en second lieu, si le personnel de cette unité peut aussi compter des civils parmi ses membres.

Un représentant ministériel estime que les délais applicables dans ce domaine sont tels qu'un fonctionnement vingt-quatre heures sur vingt-quatre n'est pas nécessaire. Concernant le personnel, il semble improbable que des civils puissent en faire partie, alors que l'UIP traite des données sensibles. Les réponses précises à ces questions seront fournies plus tard.

Le projet de rapport est adopté à la majorité (abstention ADR). La commission propose comme temps de parole le modèle de base avec un temps de parole supplémentaire pour la rapportrice.

*

Au sujet du projet de loi 7044 sur l'Inspection générale de la Police, la commission prend acte du deuxième avis complémentaire du Conseil d'État du 17 juillet 2018 relatif au projet de loi 7168 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. Le Conseil d'État note que « L'amendement sous revue[1] vise à apporter des modifications au projet de loi n° 7044 sur l'Inspection générale de la Police, qui s'inspirent largement des modifications opérées par les amendements 8 et 9 sous avis au projet de loi n° 7045 précité.

Le paragraphe 3 soulève toutefois des questions en ce qu'il permettrait, tel que formulé à l'amendement sous avis, au personnel de l'Inspection générale de la Police, ci-après l'« IGP », d'accéder directement aux données traitées dans les divers traitements des données à caractère personnel dont le responsable du traitement est le directeur général de la Police. Le Conseil d'État estime cependant qu'un tel accès va au-delà des finalités découlant de la mission première de l'IGP, définie à l'article 4, alinéa 2, du prédit projet de loi n° 7044 comme l'exercice « d'un droit d'inspection général et permanent au sein de la Police ». Seul l'exercice par l'IGP de missions d'instruction judiciaire qui lui sont confiées par l'autorité judiciaire compétente dans le cadre de l'article 8 du prédit projet de loi justifierait un tel accès, qui est toutefois d'ores et déjà possible en vertu des dispositions du Code de procédure pénale expressément visées au même article et qui, tantôt prévoient un accès direct à certains traitements, tantôt permettent un accès aux traitements par le biais d'une procédure judiciaire, telle une perquisition offrant toutes les garanties judiciaires requises.

Le Conseil d'État doit, par conséquent, s'opposer formellement à l'amendement sous examen pour transposition incorrecte de la directive, le texte proposé débouchant sur des conséquences incompatibles avec les dispositions de celle-ci, notamment celles ayant trait à la finalité des traitements de données à caractère personnel.

Le Conseil d'État comprend cependant que, dans le cadre de l'exercice des missions de contrôle pré-rappelées, l'IGP doit pouvoir accéder aux fichiers d'accès (« log files ») des différents traitements de données à caractère personnel effectués par la Police grand-ducale, de telle sorte qu'il peut d'ores et déjà se déclarer d'accord avec la formulation suivante :

[1] Doc. parl. 7168[12] - amendement 10 concernant l'article 62 nouveau, modifiant l'article 15 du projet de loi 7044

« (3) Dans le cadre des missions énoncées aux articles 4, 7 et 9, l'IGP a accès aux données retraçant les accès aux traitements des données à caractère personnel dont le directeur général de la Police est le responsable du traitement. » ».

Luxembourg, le 24 juillet 2018

Le Secrétaire-administrateur,
Marianne Weycker

La Présidente de la Commission de la Force publique,
Claudia Dall'Agnol

09

Session ordinaire 2017-2018

MW/PR P.V. FRP 09

Commission de la Force publique

Procès-verbal de la réunion du 5 juillet 2018

Ordre du jour :

7151 Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant organisation du Service de renseignement de l'État
- Rapporteur : Madame Claudia Dall'Agnol

- Examen de l'avis complémentaire du Conseil d'État

*

Présents : M. Marc Angel, M. Eugène Berger (en rempl. de M. Gusty Graas), Mme Claudia Dall'Agnol, M. Claude Haagen (en rempl. de M. Alex Bodry), M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Alexander Krieps

M. Fränk Reimen, Direction, Mme Martine Schmit, du Ministère de la Sécurité intérieure

Mme Marianne Weycker, de l'Administration parlementaire

Excusés : M. Max Hahn

M. Etienne Schneider, Ministre de la Sécurité intérieure

*

Présidence : Mme Claudia Dall'Agnol, Présidente de la Commission

*

Dans son avis complémentaire du 26 juin 2018, le Conseil d'État maintient son opposition formelle à l'égard de l'article 7, paragraphe 1er, alinéa 1er, seconde phrase.

L'article 7 est relatif aux procédés techniques de transfert des données PNR (Passenger Name Records) à l'UIP (Unité d'informations passagers) et transpose l'article 16 de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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.

Le libellé initial de ladite phrase est le suivant : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg dès leur publication au Journal officiel de l'Union européenne. ».

Dans son avis du 30 mars 2018, le Conseil d'État demande, sous peine d'opposition formelle, la suppression de cette phrase au regard de l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne (TFUE), selon lequel « Les actes législatifs sont publiés dans le Journal officiel de l'Union européenne. Ils entrent en vigueur à la date qu'ils fixent ou, à défaut, le vingtième jour suivant leur publication. ».

Par amendement gouvernemental du 27 avril 2018, cette phrase est modifiée comme suit : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg ~~dès leur publication au Journal officiel de l'Union européenne~~conformément à l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne. ».

Dans son avis complémentaire, le Conseil d'État constate que cet amendement ne répond pas à l'opposition formelle, comme « il n'appartient pas au législateur national de déterminer les modalités de l'applicabilité sur le territoire du Luxembourg des actes de l'Union ». La suppression de la phrase concernée assurera la conformité du dispositif luxembourgeois avec le dispositif européen.

La commission suit par conséquent le Conseil d'État et supprime la phrase.

Par ailleurs, le projet de loi fait l'objet de quelques modifications tenant à la forme.

Le présent projet de loi sera soumis au vote de la Chambre des Députés au cours de la semaine du 23 juillet 2018 avec les projets de loi 7168 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale[1] et 7184 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données[2].

Un député s'étonne de la hauteur de l'amende prévue à l'article 38, paragraphe 1er. Ce texte dispose que le transporteur aérien est puni d'une amende maximale de 50 000 € par vol

[1] Projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification : 1° de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 2° de la loi modifiée du 29 mai 1998 portant approbation de la Convention sur la base de l'article K.3 du Traité sur l'Union européenne portant création d'un Office européen de police (Convention Europol), signée à Bruxelles, le 26 juillet 1995 ; 3° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police ; 4° de la loi du 20 décembre 2002 portant approbation - de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995; - de l'Accord relatif à l'application provisoire entre certains États membres de l'Union européenne de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995 ; 5° de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 6° de la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État ; 7° de la loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle ; 8° de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement ; 9° de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire ; 10° de la loi modifiée du 19 décembre 2014 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière ; 11° de la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés ; 12° de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 13° de la loi du 23 juillet 2016 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de renseignement de l'État, et 14° de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière

[2] Projet de loi portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat

pour lequel il n'a pas transmis les données requises ou ne les a pas transmises dans le format requis.

Dans son avis du 30 mars 2018, le Conseil d'État se pose la même question. Il « constate que le droit positif connaît déjà à l'heure actuelle une disposition qui règle une situation tout à fait analogue.

En effet, l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration punit d'une amende d'un montant maximum de 5 000 euros les entreprises de transport aérien visées à l'article 108 de la même loi « à raison de chaque voyage pour lequel l'entreprise, par faute, n'a pas transmis les renseignements y visés ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis des renseignements incomplets ou erronés », amende qui est prononcée par le ministre ayant l'Immigration dans ses attributions. L'article 108, quant à lui, dispose en son paragraphe 1er qu'encourt les sanctions prévues aux articles 147 et 148 toute « entreprise de transport aérien qui (…) n'a pas transmis les renseignements visés à l'article 106 ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis les renseignements incomplets ou erronés ». L'article 106, de son côté, prévoit en son paragraphe 1er qu'« afin de prévenir un refus d'entrée sur le territoire, les entreprises de transport aérien ont l'obligation de transmettre à la Police grand-ducale les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire du Grand-duché de Luxembourg en provenance d'un pays non-membre de l'Union européenne ».

S'il est vrai que la disposition sous examen vise la transmission de données relatives à des vols en provenance non pas d'États non membres de l'Union européenne, mais provenant d'États membres, que la communication doit se faire non pas à la Police grand-ducale mais à l'UIP, qui fait cependant partie de cette même police, et que le ministre sanctionnateur est un autre, les faits incriminés sont identiques sur tous les autres points, de telle sorte que le Conseil d'État s'interroge sur les raisons qui ont fait que le projet sous avis prévoit une amende dont le maximum est le décuple des sanctions prévues dans la disposition déjà existante, créant ainsi une inégalité de traitement selon l'origine du passager transporté, toutes autres choses étant égales par ailleurs.

Dans l'attente de recevoir des explications sur cette différence de traitement, le Conseil d'État est obligé de réserver sa position quant à la dispense du second vote. »

Les auteurs du projet de loi ont donné les explications demandées dans le contexte de l'amendement gouvernemental 26 du 27 avril 2018. Dans son avis complémentaire, le Conseil en prend acte et retire sa réserve.

Les auteurs rappellent que « La sanction à laquelle fait référence le Conseil d'Etat a été introduite par la loi du 21 décembre 2006 portant transposition, entre autres, de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (« directive API »). S'il est partant vrai que la loi de transposition de la directive API et le projet de loi de transposition de la directive PNR prévoient tous les deux des sanctions administratives à l'encontre des transporteurs aériens qui ne transfèrent pas les données ou ne les transfèrent pas selon les conditions requises, la différence fondamentale entre les deux textes, et qui d'après les auteurs du projet de loi PNR justifie la différence au niveau des sanctions encourues, réside dans la finalité pour laquelle les données des passagers sont recueillies. Ainsi, l'objectif de la directive API consiste, tel qu'il ressort de son article 1er, à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine. Les données API sont des informations biographiques extraites de la partie du passeport lisible par machine et servent d'outils de vérification des identités et de gestion aux frontières. Ces données ne présentent pas d'intérêt pour l'évaluation des personnes ni pour le dépistage des délinquants ou terroristes «

inconnus ». En effet, *« une utilisation à la fois proactive et en temps réel des données PNR permet donc aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent, par rapport à ce que permet le traitement d'autres catégories de données à caractère personnel. Comme expliqué ci-dessous, le traitement de données à caractère personnel accessibles aux services répressifs dans le cadre d'instruments de l'UE actuels et futurs, tels que la directive relative aux informations préalables sur les passagers, le système d'information Schengen (SIS) et le système d'information Schengen de deuxième génération (SIS II), ne donne pas aux services répressifs la possibilité d'identifier des suspects « inconnus » comme le permet l'analyse de données PNR. Deuxièmement, après la commission d'une infraction, les données PNR aident les services répressifs à prévenir et à détecter d'autres infractions graves, dont des actes de terrorisme, et à enquêter sur celles-ci et à poursuivre leurs auteurs. À cet effet, les services répressifs doivent utiliser les données PNR en temps réel, pour les confronter à diverses bases de données de personnes « connues » et d'objets recherchés. Ils doivent également en faire un usage réactif, pour rassembler des preuves et, au besoin, trouver d'éventuels complices et démanteler des réseaux criminels. »*[3]

Les données PNR sont recueillies pour une finalité complètement différente, à savoir qu'ils constituent un moyen de prévention et de lutte contre le terrorisme et les formes graves de criminalité telles que la traite des êtres humains, l'exploitation sexuelle des enfants, le trafic d'armes, le vol organisé ou l'aide à l'entrée et le séjour irréguliers. Cette dernière infraction illustre d'ailleurs très bien la différence entre les finalités des traitements des données API et des données PNR. Ainsi, si la directive API vise à prévenir l'immigration illégale, qui ne constitue pas une infraction pénale, la directive PNR crée des moyens destinés à protéger la sécurité et la vie des personnes. Il n'y a aucun doute que les conséquences d'un défaut de transmission de données à des fins de contrôle des frontières ne sont pas les mêmes qu'un défaut de transmission de données qui peuvent permettre de prévenir une attaque terroriste ou un autre crime grave. La différence entre les sanctions encourues dans les deux cas de figure est dès lors justifiée.

Il importe par ailleurs de relever que l'article 14 de la directive PNR oblige les Etats membres à prévoir des sanctions effectives, proportionnées et dissuasives à l'encontre des transporteurs aériens qui ne transmettent pas les données comme le prévoit l'article 8 ou ne les transmettent pas dans le format requis. Comme il a été expliqué dans le commentaire de l'article 38, les auteurs du texte se sont alignés sur les montant[s] des amendes fixées dans d'autres Etats membres, notamment la France, la Belgique et l'Allemagne. Il est à craindre que si le Luxembourg alignait la sanction encourue par le transporteur aérien qui omet de transférer les données PNR sur la sanction prévue par la loi précitée de 2008 sur l'immigration, la Commission européenne risquerait de considérer la sanction prévue dans le présent projet de loi comme ne remplissant pas les exigences posées par l'article 14 de la Directive. ».

Le projet de rapport sera présenté à la commission le 17 juillet 2018.

Luxembourg, le 9 juillet 2018

Le Secrétaire-administrateur,
Marianne Weycker

La Présidente de la Commission de la Force publique,
Claudia Dall'Agnol

[3] 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 (COM/2011/0032 final)

05

Session ordinaire 2017-2018

MW/PR P.V. FRP 05

Commission de la Force publique

Procès-verbal de la réunion du 4 mai 2018

Ordre du jour :

1. Approbation du projet de procès-verbal de la réunion du 22 février 2018

2. 7151 Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

   - Désignation d'un rapporteur
   - Présentation du projet de loi
   - Examen de l'avis du Conseil d'État
   - Présentation des amendements gouvernementaux

*

Présents : M. Marc Angel, M. Alex Bodry, Mme Claudia Dall'Agnol, M. Gusty Graas, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Henri Kox, M. Alexander Krieps, M. Claude Lamberty (en rempl. de M. Max Hahn)

M. Etienne Schneider, Ministre de la Sécurité intérieure

M. Fränk Reimen, Direction, Mme Martine Schmit, du Ministère de la Sécurité intérieure

Police grand-ducale :

M. Alain Engelhardt, Premier Commissaire divisionnaire, M. Florent Goniva, Chef du Service des relations internationales

M. Bob Gengler, du Ministère de la Fonction publique et de la Réforme administrative

Mme Doris Woltz, Directrice du Service de renseignement de l'État du Luxembourg (SREL)

M. Jean-Paul Bever, de l'Administration parlementaire

*

Présidence : Mme Claudia Dall'Agnol, Présidente de la Commission

*

1. Approbation d'un projet de procès-verbal

Le projet de procès-verbal ne donne pas lieu à observation et est approuvé.

2. Projet de loi 7151

La commission désigne sa présidente, Mme Claudia Dall'Agnol, comme rapportrice du projet de loi.

En guise d'introduction, Monsieur le Ministre rappelle le rôle du Luxembourg dans la finalisation de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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. En effet, la présidence luxembourgeoise du Conseil de l'Union européenne a réussi, malgré le contexte difficile des attaques terroristes en Europe, à négocier un texte de compromis approuvé par le Conseil JAI[1] le 4 décembre 2015 et par le Parlement européen le 14 avril 2016.

Le délai de transposition de la directive est le 25 mai 2018. Le projet de loi ayant pour objet la transposition de la directive a été déposé le 19 juin 2017 et a fait l'objet d'un avis du Conseil d'État le 30 mars 2018. Une série d'amendements gouvernementaux a été adoptée par le gouvernement en conseil en date du 27 avril 2018.

Les auteurs font une présentation succincte du projet de loi, dont la structure est la suivante :

- Le chapitre 1er contient des dispositions générales, dont l'objet de la loi défini à l'article 1er : sont visés les transporteurs aériens, lesquels doivent transférer les données des dossiers passagers pour le traitement de celles-ci à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité, ces dernières étant énumérées à l'annexe II.
L'article 2 définit les différentes notions. Par amendement gouvernemental du 27 avril 2018, le point 7, en l'absence d'une définition de l'Unité d'informations passagers (UIP), a été complété par la référence à l'article 3 créant l'UIP, tel que suggéré par le Conseil d'État dans son avis du 30 mars 2018. Par ailleurs, un point 11 nouveau a été ajouté pour la notion de « services compétents », demande formulée par le Conseil d'État notamment à l'endroit de l'article 10, paragraphe 1er.

- Le chapitre 2 a trait à l'Unité d'informations passagers. L'article 3 met en place au sein de la Police grand-ducale l'UIP chargée de la collecte, du transfert et de l'échange des données et des résultats de leur traitement, tel que prévu par la future loi. L'UIP sera intégrée dans la direction « relations internationales » rattachée au comité de direction de la Police grand-ducale.

L'article 4 prévoit que l'UIP peut comprendre, outre le personnel policier, du personnel de l'Administration des douanes et accises (ADA) et du Service de renseignement de l'État (SRE).

Le Conseil d'État pose la question du statut et des compétences du personnel détaché en rappelant que, suivant l'article 7 du Statut général des fonctionnaires de l'État, le détachement consiste en « l'assignation au fonctionnaire d'un autre emploi correspondant à sa catégorie et à son grade dans une autre administration, dans un établissement public ou

[1] Justice et Affaires intérieures

auprès d'un organisme international », qui a comme conséquence que « le fonctionnaire relève de l'autorité hiérarchique de l'administration, respectivement de l'établissement ou de l'organisme auquel il est détaché ». Par conséquent, les fonctionnaires détachés de l'ADA et du SRE « relèveront entièrement de la Police grand-ducale. Dès lors, en précisant que les personnes concernées continueront à agir « dans les limites des attributions légales de l'administration dont (elles) relève(nt) » le projet de loi sous examen est en contradiction avec la disposition précitée du Statut général ». En conséquence, le Conseil d'État a exprimé une opposition formelle pour incohérence et insécurité juridique. En outre, il s'interroge sur la définition des « services compétents ».

Dans la lettre d'amendements gouvernementaux du 27 avril 2018, les auteurs confirment que « le projet de loi limite le traitement des données à une finalité de prévention et de répression du terrorisme et de la criminalité grave. Conformément à l'article 3, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du SRE, *« le SRE a pour mission de rechercher, d'analyser et de traiter, dans une perspective d'anticipation et de prévention, […] les renseignements relatifs à toute activité qui menace ou pourrait menacer la sécurité nationale […] »*. Le paragraphe 2 de l'article 3 de la loi précitée du 5 juillet 2016 précise qu'on *« entend par toute activité qui menace ou pourrait menacer la sécurité nationale […], toute activité […] qui peut avoir un rapport avec l'espionnage, l'ingérence, le terrorisme, l'extrémisme à propension violente, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, le crime organisé ou la cyber-menace dans la mesure où ces deux derniers sont liés aux activités précitées »*. Il est donc permis de conclure que les missions du SRE, et notamment ses missions de prévention en matière de lutte contre le terrorisme, l'espionnage, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes ou la cyber-menace dans la mesure où elle est liée aux activités précitées, correspondent parfaitement à la finalité définie par le projet de loi sous examen. Le SRE est partant justifié à traiter des données PNR. Le traitement de données PNR par un service de renseignement correspond d'ailleurs aux législations en place des pays européens dans la matière. Par exemple, l'article 14 de la loi belge du 25 décembre 2016 relative au traitement des données des passagers prévoit une UIP composée de la Sûreté de l'Etat visée par la loi organique du 30 novembre 1998 des services de renseignement et de sécurité et du Service général de Renseignement et de Sécurité visé par la loi organique du 30 novembre 1998 organique des services de renseignement et de sécurité. ».

Le Conseil d'État souligne aussi que les personnes détachées « ne sont plus en droit d'accéder aux données et informations traitées dans leur service d'origine sur base de leur première affectation, étant donné qu'en vertu de leur détachement ils n'en font plus partie », sauf à ajouter des dispositions spécifiques au texte de loi. Comprenant « l'utilité d'une disposition qui prévoit que les différents services compétents disposent d'un représentant en tant qu'« agent de liaison » au sein de l'UIP », le Conseil d'État propose notamment comme solution, s'inspirant de la loi belge de transposition de la directive PNR, de mettre en place une unité indépendante de la Police grand-ducale, à l'instar de la Cellule de renseignement financier auprès du parquet de Luxembourg.

La solution retenue par les auteurs des amendements se distingue du détachement en mentionnant que « si la version française de la Directive parle d'agents détachés, la version allemande utilise les termes *« abgeordnet werden »* et la version anglaise prévoit que *« staff members of a PIU may be seconded from competent authorities » »*. Les auteurs s'inspirent de l'article 9, paragraphe 3, de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat qui dispose que *« Les agents du centre peuvent être placés auprès d'un département ministériel ou d'une administration de l'Etat par une décision conjointe du ministre et du ministre du ressort. Dans ce cas, et pendant toute la durée de leur placement, ils continuent de relever de l'autorité hiérarchique du directeur du centre. »* Il ressort du commentaire des articles du projet de loi ayant abouti à la loi précitée du 20 avril

2009 que « *En ce qui concerne le personnel, la seule particularité pour le CTIE est la possibilité de placer certains de ses agents auprès des départements ministériels, administrations ou services de l'Etat sur base d'une décision conjointe des membres du Gouvernement respectifs. Cette mesure est destinée à permettre au CTIE d'envoyer des informaticiens auprès d'autres entités administratives afin de mettre en place et de gérer les systèmes informatiques d'une administration en particulier. Contrairement aux agents détachés, les agents placés par le CTIE continuent de relever de leur autorité hiérarchique d'origine. Ceci est nécessaire en raison du fait qu'ils doivent effectuer leur travail d'après les directives et les critères que le CTIE fixe pour l'ensemble du réseau informatique de l'Etat. (…) Le mécanisme du placement des agents est inspiré de la situation des contrôleurs financiers qui relèvent de l'autorité du Ministre ayant le budget dans ses attributions, mais qui exercent leurs missions auprès des différents départements ministériels.*[2]

Ainsi, le personnel de l'ADA et le personnel du SRE seront désignés à l'UIP comme membres de leurs administrations respectives et agiront comme tels. Cette solution ne remet pas en cause le principe selon lequel l'UIP fonctionne sous forme de « closed box » et que les services désignés comme services compétents n'ont pas un accès direct aux données PNR. Le personnel de l'ADA et du SRE resteront placés sous l'autorité hiérarchique de leur administration d'origine. Pour permettre au responsable de l'UIP d'exercer les responsabilités qui lui incombent en vertu de la présente loi, il aura autorité fonctionnelle sur ce personnel. ».

Quant à la critique du Conseil d'État que le texte ne donne aucune indication sur le grade ou la fonction du responsable de l'UIP, ni ne précise s'il doit s'agir d'un membre du personnel du cadre policier ou si un membre du cadre civil de la Police peut également remplir cette tâche de direction, le paragraphe 1er a été complété par un alinéa 2 précisant que le responsable de l'UIP est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

- Le chapitre 3 est relatif au transfert des données par les transporteurs aériens.

Le transfert des données se fait sans préjudice des obligations imposées par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, à savoir la transmission des informations préalables recueillies sur les passagers (Advanced Passenger Information (API) au Service de contrôle à l'aéroport. Dans son avis, le Conseil d'État rappelle que ces informations sont déjà actuellement recueillies pour les passagers provenant d'un État non membre de l'Union européenne. Il rend attentif à l'obligation, prévue par l'article 8, paragraphe 2 de la directive, pour les États « d'adopter les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent également ces données, par la « méthode push », à l'UIP ». Il réserve sa position quant à la dispense du second vote constitutionnel dans l'attente des renseignements « de nature à établir que ce transfert est effectué dans les conditions requises par le législateur européen ».

Par amendement gouvernemental du 27 avril 2018, l'article 7 est complété par un paragraphe 3 tenant compte de la réserve exprimée par le Conseil d'État.

L'article 6 concerne les moments du transfert des données à l'UIP, prévues par l'article 8, paragraphe 3 de la directive.

Le texte initial a fait l'objet d'une opposition formelle en raison de l'ajout d'une « obligation supplémentaire à celles prévues par la directive, risquant ainsi en outre de créer une charge administrative supplémentaire pour les transporteurs qui utilisent l'aéroport de Luxembourg

[2] Projet de loi 5912

par rapport à ceux qui ont recours à des aéroports situés dans des pays n'imposant pas un même niveau d'obligations ».

Par amendement gouvernemental du 27 avril 2018, l'obligation supplémentaire est supprimée.

L'article 7 précise les procédés techniques de transfert des données et transpose l'article 16 de la directive.

Dans son avis du 30 mars 2018, le Conseil d'État demande, sous peine d'opposition formelle, la suppression de la seconde phrase du paragraphe 1er, alinéa 1er au regard de l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne (TFUE), selon lequel « Les actes législatifs sont publiés dans le Journal officiel de l'Union européenne. Ils entrent en vigueur à la date qu'ils fixent ou, à défaut, le vingtième jour suivant leur publication. ». Le libellé de ladite phrase figurant à l'article 7 dans sa version initiale est le suivant : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg dès leur publication au Journal officiel de l'Union européenne. ».

Par amendement gouvernemental du 27 avril 2018, cette phrase est modifiée comme suit : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg ~~dès leur publication au Journal officiel de l'Union européenne~~conformément à l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne. ».

- Le chapitre 4 concerne le traitement des données PNR.

L'article 8 transpose l'article 13, paragraphe 4 de la directive qui interdit le traitement de données PNR qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance à un syndicat, l'état de santé, la vie sexuelle ou l'orientation sexuelle. Ces données doivent être effacées dès réception et de façon définitive.

L'article 9 impose à l'UIP d'effacer celles des données transférées qui ne sont pas énumérées à l'annexe I.

L'article 10 a trait à l'utilisation des données PNR pour réaliser une évaluation des passagers avant leur arrivée ou leur départ dans le but « d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis ». Cette évaluation se fait par comparaison des données PNR avec les données à caractère personnel traitées par les services compétents ou auxquelles ils ont accès dans l'exercice de leurs missions ou avec des critères préétablis. Le paragraphe 2, alinéa 2 édicte des règles strictes pour ces critères. En vertu du paragraphe 3, « toute concordance positive obtenue » engendre un réexamen individuel. Le paragraphe 4 prévoit la transmission des données « au cas par cas, en vue d'un examen plus approfondi ».

Suivant l'article 11, les données PNR peuvent aussi être traitées pour mettre à jour les critères d'évaluation ou pour définir de nouveaux critères.

L'article 12 prévoit comme autre finalité de traitement des données PNR celle de répondre aux demandes des services compétents, « dûment motivées et fondées sur des motifs suffisants ». Le commentaire du document tel que déposé explique que ces données peuvent servir comme éléments de preuve dans le cadre d'enquêtes judiciaires ; ainsi, elles peuvent aider à orienter les enquêteurs sur le lieu de séjour d'une personne suspecte au moment où les faits ont été commis.

- Le chapitre 5 est consacré aux services compétents.

L'article 13 énumère les services habilités à demander et à recevoir des données PNR ou le résultat du traitement de ces données et détermine la finalité de la transmission des données aux services concernés. Il reprend l'article 7, paragraphe 1er de la directive, tenant ainsi compte d'une opposition formelle du Conseil d'État et des critiques du Parquet général et de la Cour supérieure de justice pour transposition incorrecte de la directive et manque de précision en ce qui concerne la finalité de la transmission des données aux services concernés.

Le second alinéa résulte des propositions du Conseil d'État et du Parquet général d'introduire dans le cadre juridique national, à l'instar de la loi belge ayant transposé la directive PNR, un accès simplifié des procureurs d'État « aux données PNR détenues par l'UIP en leur évitant d'avoir à saisir le juge d'instruction ne fût-ce que par le biais d'une procédure dite « mini-instruction », tout en sachant qu'en tant qu'acte d'enquête, la réquisition serait susceptible du recours inscrit à l'article 48-2 du Code de procédure pénale ».

L'article 14 limite le traitement des données PNR et du résultat du traitement aux finalités déterminées par l'article 1er, sans préjudice des compétences de la Police grand-ducale et de l'ADA, « lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement ». Il transpose l'article 7, paragraphes 4 et 5 de la directive.

L'article 15, transposant l'article 7, paragraphe 6 de la directive, prévoit que les services compétents ne peuvent prendre aucune décision ayant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR. Même si l'article 8 du projet de loi interdit le traitement des données sensibles y visées, l'interdiction de prendre des décisions qui seraient basées sur de telles données, si celles-ci avaient néanmoins été collectées, a été ajoutée suite à l'opposition formelle du Conseil d'État.

- Le chapitre 6 traite de l'échange d'informations entre les États membres de l'Union européenne.

L'article 16 règle la transmission d'office d'informations aux UIP d'autres États membres.

L'article 17 règle la transmission d'informations sur demande de l'UIP d'un autre État membre. Il définit les conditions de la demande adressée à l'UIP luxembourgeoise. Le paragraphe 1er distingue entre les données qui n'ont pas encore été dépersonnalisées par masquage tel que prévu par l'article 26 et les données masquées. Par amendement gouvernemental du 27 avril 2018, le paragraphe 1er a été complété par un alinéa 4. Suivant le commentaire de l'amendement, celui-ci « est à voir en relation avec la question, soulevée par le Parquet général à propos de l'article 21 réglant le transfert de données PNR à des États non membres de l'Union européenne, de savoir si cet échange échapperait aux dispositions traditionnelles de l'entraide judiciaire. Afin de dissiper toute incertitude à cet égard, une précision afférente a été apportée non seulement en ce qui concerne les échanges de données PNR avec des pays tiers, mais également l'échange de telles données avec d'autres États membres. ».[3]

Suivant le paragraphe 2, sauf en cas d'urgence, les demandes et les échanges de données ont lieu par l'intermédiaire des UIP. Le paragraphe 3 permet, en cas de menace précise et

[3] Dans son avis complémentaire du 26 juin 2018, le Conseil d'État a proposé une formulation plus précise qui a été reprise par la commission.

réelle, de demander des données auprès d'un transporteur aérien en dehors des délais prévus à l'article 6, paragraphe 1er.

L'article 18 est relatif aux cas où les autorités luxembourgeoises adressent des demandes de données à l'UIP d'un autre État membre.

L'article 19 transpose l'article 9, paragraphe 5 de la directive qui concerne les modalités techniques d'échange des informations entre États membres.

- Le chapitre 7 est relatif aux conditions d'accès aux données PNR par Europol.

L'article 20 transpose l'article 10 de la directive, définissant les conditions d'accès aux données PNR par Europol.

Le Conseil d'État reconnaît à cette disposition une pure valeur déclaratoire, « étant donné que les compétences d'Europol ainsi que ses droits et obligations dans le cadre desdites compétences, font l'objet d'instruments européens et ne nécessitent pas de mesures de transposition particulières en droit national ».

- Le chapitre 8 règle le transfert de données vers des pays non membres de l'Union européenne.

L'article 21 transpose l'article 11, paragraphe 1er de la directive qui détermine les conditions du transfert de données PNR à un pays non membre de l'Union européenne.

L'article 22 transpose l'article 11, paragraphe 2 de la directive qui a trait au transfert de données PNR, obtenues d'un autre État membre, à un pays non membre de l'Union européenne.

L'article 23 transpose l'article 11, paragraphe 3 de la directive. Il prévoit une condition supplémentaire aux transferts de données vers des pays tiers. Suite aux interrogations du Conseil d'État, le texte a été amendé « de manière à n'ajouter comme condition supplémentaire par rapport aux conditions fixées aux articles 21 et 22 que celle d'avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données respecte les conditions et garanties de la présente loi ».

L'article 24 transpose l'article 11, paragraphe 4 de la directive, en vertu duquel « Chaque fois qu'un État membre transfère des données PNR en vertu du présent article, le délégué à la protection des données de l'UIP de cet État membre en est informé. ».

- Le chapitre 9 a pour objet la durée de conservation et la dépersonnalisation des données.

L'article 25 transpose l'article 12, paragraphes 1er et 4 de la directive et dispose que la durée maximale de conservation des données PNR est de cinq ans. Les données sont ensuite effacées de manière définitive, sauf celles qui ont été transférées à un service compétent et qui sont utilisées dans le cadre d'une enquête ou poursuite.

L'article 26 transpose l'article 12, paragraphe 2 de la directive qui impose l'obligation de dépersonnaliser par le masquage des éléments des données qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR. Le commentaire du texte déposé explique que « Le masquage est une technique qui consiste à rendre ces éléments de données invisibles, sans toutefois les altérer. Des recherches automatisées restent ainsi possibles parmi les données masquées et des hits peuvent être générés. Toutefois les informations permettant d'identifier la personne à laquelle les données se rapportent ne sont pas affichées sur l'écran. Pour pouvoir visualiser ces informations, l'UIP doit obtenir l'accord

du procureur [général] d'Etat ou de son délégué ou, si la requête émane du Service de Renseignement de l'Etat, l'accord de la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de Renseignement de l'Etat. ».

L'article 27 transpose l'article 12, paragraphe 5 de la directive et concerne la durée de conservation du résultat de l'évaluation réalisée sur base de l'article 10. Cette durée correspond au temps nécessaire pour informer les services compétents et, le cas échéant, les UIP, de l'existence d'une concordance positive. Au cas où le réexamen individuel manuel révèle un résultat du traitement automatisé négatif, celui-ci peut être archivé par l'UIP aussi longtemps que les données de base n'ont pas été effacées, ceci pour éviter de futures fausses concordances positives.

Un député fait observer que le défaut de date dans le renvoi à d'autres lois est problématique en raison du manque de précision.

- Le chapitre 10 concerne la protection des données à caractère personnel.

L'article 28 transpose l'article 13 de la directive.

Dans son avis, le Conseil d'État constate « que le projet sous avis, contrairement à l'article 13 de la directive, retient le principe de la compétence de la CNPD[4] ainsi que l'application du régime général sur la protection des données[5] aux données PNR collectées, pour ne mentionner la loi de transposition de la directive (UE) 2016/680 qu'en début de la disposition pour réserver les droits des autorités judiciaires. Il est dès lors en porte-à-faux avec le texte à transposer qui vise expressément la décision-cadre 2008/977/JAI, remplacée par la directive (UE) 2016/680, et ne retient l'application du régime de droit commun de la protection des données que pour le traitement des données à caractère personnel effectué par les transporteurs aériens[6], de telle sorte que le Conseil d'État doit s'opposer formellement au texte actuel, qui constitue une transposition incorrecte de la directive. ».

Par amendement gouvernemental du 27 avril 2018, le texte a été reformulé et se réfère à l'article 40 de la future loi portant transposition de la directive sur la protection des données en matière pénale. Le commentaire précise que « Dans la mesure où cette loi désigne la CNPD comme autorité compétente pour contrôler les traitements des données en matière pénale autres que ceux effectués par les juridictions de jugement, ce sera également la CNPD qui sera compétente pour contrôler le traitement des données PNR. Etant donné que les missions et les pouvoirs de cette commission sont définis par la loi portant sur le régime général, il est renvoyé à cette loi pour ce qui est des missions et des pouvoirs de la CNPD. ».

L'article 29 est relatif au délégué à la protection des données désigné par le responsable de l'UIP. Il transpose l'article 5 et l'article 6, paragraphe 6 de la directive. Sur demande du Conseil d'État, le paragraphe 4, alinéa 2 a été complété pour préciser la base légale permettant la saisine de la CNPD.

L'article 30 détermine les informations que l'UIP met à la disposition du public.

L'article 31 transpose l'article 13, paragraphe 1er de la directive. Il est consacré aux droits des personnes dont les données sont traitées, ces droits étant définis par référence aux articles pertinents du projet de loi 7168 portant transposition de la directive sur la protection des données pénales.

[4] Commission nationale pour la protection des données
[5] Projet de loi 7184
[6] Directive (UE) 2016/681, article 13, paragraphe 3

L'article 32 transpose l'article 6, paragraphe 8 de la directive qui oblige les UIP à stocker, traiter et analyser les données PNR exclusivement dans un ou des endroits sécurisés situés sur le territoire de l'État membre.

Transposant l'article 13, paragraphes 2 et 7 de la directive, l'article 33 oblige le responsable de l'UIP de mettre en œuvre des mesures et des procédures techniques pour garantir un niveau élevé de sécurité des données.

En vertu de l'article 34 qui transpose l'article 13, paragraphe 5 de la directive, l'UIP doit conserver une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

L'article 35, transposant l'article 13, paragraphe 6 de la directive, a pour objet l'obligation pour l'UIP de tenir des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

L'article 36 transpose l'article 13, paragraphe 8 de la directive et prévoit l'information obligatoire, sans retard injustifié, de la personne concernée et de la CNPD, lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection de ces données ou d'affecter négativement la vie de la personne concernée.

- Le chapitre 11 est relatif aux sanctions.

L'article 37, alinéa 1er punit, dans sa version initiale, la violation des articles 8, 15 et 36 de sanctions pénales. S'agissant de l'article 8, le Conseil d'État demande, afin d'assurer le respect du principe constitutionnel de la légalité de la peine, de préciser lequel des deux comportements visés à l'article 8 est sanctionné : le traitement illicite ou le défaut d'effacement des données concernées ou les deux. Il exige en outre de préciser s'il s'agit d'une infraction intentionnelle ou non, considérant « qu'un simple dysfonctionnement au sein de l'unité, dépourvu de toute intention criminelle, qui serait éventuellement sanctionnable du point de vue disciplinaire, n'est pas de nature à entraîner la responsabilité pénale, que ce soit du responsable de l'unité ou du fonctionnaire à l'origine du traitement en question ».

La question de l'intention de l'auteur du fait incriminé se pose également pour l'article 15.

Pour ce qui est de l'article 36, lequel oblige l'UIP à informer sans retard injustifié la personne concernée et l'autorité de contrôle d'une atteinte aux données à caractère personnel, le Conseil d'État met en doute « la faisabilité matérielle de l'information de la personne concernée qui, dans la grande majorité des cas, risque de ne pas résider sur le territoire national ».

Par conséquent, l'article 37 a été amendé pour tenir compte des avis du Conseil d'État et des autorités judiciaires. Le nouveau libellé précise que l'infraction consiste en une violation intentionnelle de l'interdiction de traiter des données sensibles, telle que prévue à l'article 8, alinéa 1er. Les auteurs de l'amendement indiquent ne pas avoir retenu la demande des Parquets de Luxembourg et de Diekirch de fixer un délai maximal pour l'effacement des données ; en effet, en fixant un délai pour ce faire, alors que la directive fait obligation d'effacer ces données immédiatement, il existe le risque que la Commission européenne considère que la législation luxembourgeoise ne serait sur ce point pas conforme à la directive.

Concernant l'article 15, l'article 37 amendé précise que la violation de la disposition, selon laquelle une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peut être prise sur la seule base du traitement automatisé de données PNR, doit être intentionnelle. Par ailleurs, a également été érigé en

infraction pénale le fait de prendre une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative qui serait fondée sur 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.

L'article 36 a été retiré de la liste des infractions pénales suite aux doutes du Conseil d'État au sujet de la faisabilité matérielle de l'information de la personne concernée.

Le Conseil d'État et les Parquets ont été suivis en faisant de la cessation du traitement illégal une obligation pour la juridiction de jugement.

Au sujet de l'article 49 [devenu l'article 47], paragraphe 2 du projet de loi 7168, les auteurs de l'amendement font remarquer que cette disposition n'est pas applicable en matière de données PNR, puisque l'article 37 du projet de loi PNR ne renvoie dans son alinéa 2 qu'aux paragraphes 1er, 3 et 5 du projet de loi n° 7168. Les auteurs « ne partagent dès lors pas la crainte soulevée par le Conseil d'État par rapport à une éventuelle incohérence entre les dispositions pénales mises en place par les deux textes ».

L'article 38 punit d'une amende maximale de 50 000 € le transporteur aérien pour chaque vol pour lequel il n'a pas transmis les renseignements visés à l'article 3, ne les a pas transmis dans le délai prévu ou selon les modalités ou dans les formes prescrites.

Dans son avis du 30 mars 2018, le Conseil d'État « constate que le droit positif connaît déjà à l'heure actuelle une disposition qui règle une situation tout à fait analogue.

En effet, l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration punit d'une amende d'un montant maximum de 5 000 euros les entreprises de transport aérien visées à l'article 108 de la même loi « à raison de chaque voyage pour lequel l'entreprise, par faute, n'a pas transmis les renseignements y visés ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis des renseignements incomplets ou erronés », amende qui est prononcée par le ministre ayant l'Immigration dans ses attributions. L'article 108, quant à lui, dispose en son paragraphe 1er qu'encourt les sanctions prévues aux articles 147 et 148 toute « entreprise de transport aérien qui (…) n'a pas transmis les renseignements visés à l'article 106 ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis les renseignements incomplets ou erronés ». L'article 106, de son côté, prévoit en son paragraphe 1er qu'« afin de prévenir un refus d'entrée sur le territoire, les entreprises de transport aérien ont l'obligation de transmettre à la Police grand-ducale les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire du Grand-duché de Luxembourg en provenance d'un pays non-membre de l'Union européenne ».

S'il est vrai que la disposition sous examen vise la transmission de données relatives à des vols en provenance non pas d'États non membres de l'Union européenne, mais provenant d'États membres, que la communication doit se faire non pas à la Police grand-ducale mais à l'UIP, qui fait cependant partie de cette même police, et que le ministre sanctionnateur est un autre, les faits incriminés sont identiques sur tous les autres points, de telle sorte que le Conseil d'État s'interroge sur les raisons qui ont fait que le projet sous avis prévoit une amende dont le maximum est le décuple des sanctions prévues dans la disposition déjà existante, créant ainsi une inégalité de traitement selon l'origine du passager transporté, toutes autres choses étant égales par ailleurs.

Dans l'attente de recevoir des explications sur cette différence de traitement, le Conseil d'État est obligé de réserver sa position quant à la dispense du second vote. »

Les auteurs du projet de loi donnent les explications demandées dans le contexte de l'amendement gouvernemental 26 du 27 avril 2018.

- Le chapitre 12 a trait aux dispositions modificatives.

L'article 39 a fait l'objet de deux oppositions formelles du Conseil d'État. La première concerne l'ajout d'un paragraphe 4 à l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État. Le Conseil d'État rappelle que l'article 5 de cette loi « énumère les moyens et mesures de recherche dont dispose le SRE et qui, pour leur mise en œuvre, nécessitent une autorisation écrite du directeur du service, suite à une demande motivée et écrite de l'agent du SRE chargé du dossier. La nouvelle disposition ajoute à ces moyens et mesures de recherche la possibilité pour le SRE de demander à l'UIP la communication des données PNR dans le cadre de ses activités.

L'amendement 2 est à lire avec l'amendement 3, qui tend à supprimer le point a) de l'article 8 de la loi précitée du 5 juillet 2016, prévoyant que le SRE peut être autorisé par le Comité ministériel du renseignement, instauré par le paragraphe 2 de l'article 2 de ladite loi, de « solliciter (…) les données des dossiers passagers relatives à une ou plusieurs personnes identifiées ou identifiables au sujet desquels le SRE dispose d'un ou de plusieurs indices concordants relatifs à une menace actuelle ou potentielle visant la sécurité nationale ou les intérêts visés à l'article 3. Le transporteur de personnes par voie aérienne visé par la demande doit fournir sa réponse sans délai. ». Cette mesure ne peut cependant être autorisée par ledit comité, au vœu du paragraphe 1er de l'article 8, que « si les moyens et les mesures de recherche dont dispose le SRE en vertu des articles 5, 6, et 7 (de la loi précitée) s'avèrent inopérants en raison de la nature des faits et des circonstances spécifiques de l'espèce ».

Il résulte de la combinaison de ces deux amendements que la mesure de l'article 8, permettant au SRE de contacter directement les opérateurs de transports aériens, sera remplacée par la possibilité pour ledit service de demander des renseignements à l'UIP et ne pourra plus être utilisée en conséquence.

Cet amendement pose cependant problème en ce que, en limitant les finalités de l'accès du SRE aux données de l'UIP, il reste en deçà de l'article 13 du projet de loi sous examen et en réduit par conséquent la portée, entraînant ainsi une transposition incorrecte de la directive, à laquelle le Conseil d'État doit s'opposer formellement. ».

Les auteurs de l'amendement ont par conséquent suivi le Conseil d'État en complétant l'article 13 par une référence à l'article 5, paragraphe 4, de la loi précitée du 5 juillet 2016.

La seconde opposition formelle se rapporte à l'alinéa 2 du paragraphe 4 nouveau ajouté par l'amendement 2 ci-dessus à l'article 5 de la loi précitée du 5 juillet 2016. Pour le Conseil d'État, le fait de prévoir « que le directeur du SRE « rapporte tous les six mois par écrit » au prédit comité « la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquelles l'exercice des missions a exigé la demande de communication » n'est pas de nature à garantir suffisamment les droits des personnes concernées, cela d'autant plus que la procédure invoquée par les auteurs de l'amendement et prévue à l'article 5, paragraphe 3, de la loi précitée du 5 juillet 2016, qui a trait aux observations dans les lieux publics ainsi qu'aux inspections de lieux publics, prévoit un rapport par écrit au comité une fois par mois, et non pas une fois chaque semestre.

Il s'oppose par conséquent formellement à l'amendement sous avis pour contravention à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 11, paragraphe 3, de la Constitution pour autant qu'il réduit la

fréquence du prédit rapport à un rapport semestriel, ce qui est totalement insuffisant pour garantir les droits des personnes concernées. ».

En conséquence, l'alinéa 2 du paragraphe 4 nouveau ajouté à l'article 5 de la loi précitée du 5 juillet 2016 a été amendé de manière à prévoir un rapport mensuel.

*

À l'aide d'une présentation PowerPoint, le Responsable du Service des relations internationales de la Police grand-ducale donne un aperçu de la mise en pratique de la directive.

L'UIP fait partie de la direction « relations internationales », puisque celle-ci est en charge de l'échange d'informations avec les autres États, que ce soit par le système d'information Schengen (SIS) et précisément le bureau SIRENE (Supplementary Information Request at the National Entries), Interpol ou Europol, et en raison de l'expérience de celle-ci avec le système API (Advanced Passenger Information).

Les interlocuteurs de l'UIP sont le SREL, l'ADA et les services policiers compétents, à savoir le Service de Police judiciaire (SPJ), les actuels services de recherche et d'enquête criminelle (SREC), l'Unité Centrale de la Police de l'Aéroport (UCPA), les bureaux policiers internes SIRENE, Europol et Interpol, de même que les autorités judiciaires.

Les missions de l'UIP consistent en la collecte des données, leur traitement et analyse et leur échange.

Suite à la collecte des données suivant les modalités et dans les formes prévues par la directive, le travail policier proprement dit commence, c'est-à-dire le traitement et l'analyse des données.

Le traitement et l'analyse revêtent deux aspects : d'une part, il est procédé à des contrôles automatisés en temps réel. Ces contrôles se font en trois étapes : 1) le criblage consiste à vérifier si les personnes qui se trouvent sur les listes des passagers ne sont pas des personnes recherchées dans le SIS par le biais du réseau Interpol. 2) Le ciblage personnalisé, connu sous le nom de « Watchlist », concerne des personnes spécialement surveillées par les enquêteurs, lesquels sont informés au moyen de la « Watchlist » de l'arrivée et du départ de ces personnes. 3) Le ciblage de précision (rules based targeting, Musterfahndung) permet de cibler des personnes en fonction de critères déterminés. Chaque personne qui correspond à ces critères est signalée par le système. Contrairement au criblage et au ciblage personnalisé, lesquels visent des personnes ou objets recherchés connus, le ciblage de précision a pour objet de détecter des personnes suspectes inconnues.

D'autre part, des requêtes sont effectuées dans le passé. Il s'agit de vérifications dans le cadre d'une enquête et de vérifications pour l'UIP des autres pays.

Pour ce qui est du trafic aérien, 3,6 millions passagers sont passés par le Luxembourg en 2017 qui se répartissent sur différentes compagnies aériennes comme suit : Luxair 51%, Ryanair 10%, Lufthansa 8%, Easyjet 7%, KLM 5%, autres 19%.

Depuis 2006, un autre système est en vigueur au Luxembourg en matière de données relatives aux passagers, à savoir le système API (Advanced Passenger Information). La directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (directive API) a été transposée au Luxembourg par la loi du 21 décembre 2006 portant 1. transposition – de la

directive 2001/40/CE du Conseil du 28 mai 2001 relative à la reconnaissance mutuelle des décisions d'éloignement des ressortissants de pays tiers ; – de la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 ; – de la directive 2002/90/CE du Conseil du 28 novembre 2002 définissant l'aide à l'entrée, au transit et au séjour irréguliers ; – de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers ; 2. modification de la loi modifiée du 28 mars 1972 concernant 1. l'entrée et le séjour des étrangers ; 2. le contrôle médical des étrangers ; 3. l'emploi de la main-d'oeuvre étrangère. Le dispositif API se limite aux vols extra-Schengen et impose la transmission préalable, précisément au moment du départ (ATD – at time departure), à la Police des listes de passagers des vols en provenance d'un pays non membre de l'Union européenne. Les données recueillies lors de l'enregistrement (check-in) sont les éléments d'identification de base d'une personne, à savoir nom, le prénom, la date de naissance, le numéro du passeport et la nationalité.

La directive PNR résulte d'un compromis entre les États membres et d'une déclaration commune des ministres du Conseil Justice et Affaires intérieures (JAI) du 4 décembre 2015. Elle étend le contenu de la directive API en prévoyant l'obligation de transmission des listes de passagers également pour les vols intra-Schengen et de transit. Dix-neuf champs de données PNR sont prévus. Les données sont transmises 48 heures avant l'heure de départ programmée du vol et immédiatement après la clôture du vol et elles sont consolidées dans le dossier des données Passager et traitées par l'UIP. Les données sont conservées pendant cinq ans. Elles restent visibles pendant six mois à compter de leur transfert par les compagnies aériennes et sont ensuite masquées. Si la Police a besoin pendant cette période de telles données, l'UIP doit obtenir l'accord du procureur général d'Etat ou de son délégué pour visualiser les informations masquées. Il convient de préciser que les données PNR ne sont pas spécialement recueillies pour les besoins de la Police, mais elles seront désormais transférées à celle-ci.

Concrètement, la mise en œuvre de la transposition de la directive PNR nécessitera onze semaines pour atteindre une collecte de 99% des données passagers. L'UIP a été mise en place par deux policiers et sera renforcée par deux autres policiers ; elle comptera par ailleurs respectivement un membre du SREL et de l'ADA. Le personnel sera renforcé en fonction des besoins et le travail sera organisé sur base des expériences qui seront faites.

Les systèmes API et PNR fonctionneront parallèlement, puisqu'ils ont des finalités différentes : tandis que l'API n'a pour objet que le contrôle de l'immigration, le PNR a pour but la prévention et la répression du terrorisme et de la criminalité grave, ce qui justifie des sanctions plus élevées pour non-transmission de données. La mise en œuvre de la directive signifie une augmentation considérable des données à traiter, le nombre de mouvements à l'aéroport s'élevant à environ 40 000 par an et les champs de données passant de 5 à dix-neuf. Le traitement se fera suivant deux critères prioritaires, à savoir la provenance du vol (les vols extra-Schengen étant d'un intérêt particulier) et le volume du vol (nombre de passgers). Les compagnies aériennes peuvent choisir parmi trois formats informatiques pour le transfert des données et chaque compagnie est connectée séparément. En ce qui concerne les vols privés, des pourparlers sont en cours avec Luxaviation, bien que le volume de ces vols soit petit.

Quant à l'utilité des données recueillies, on distingue plusieurs hypothèses. La première est celle du contrôle, par le SIS, Interpol ou le fichier central national, du signalement d'une personne. S'agissant d'une personne recherchée par les autorités judiciaires, la Police a une conduite à tenir. Elle dispose d'un mandat d'arrêt européen ou international et est donc en mesure d'agir. Par contre, dans l'hypothèse où une personne utilise un passeport déclaré comme volé ou perdu dans un des systèmes précités, la Police n'a pas la possibilité de saisir ce document de voyage, mais doit suivre une procédure déterminée.

Dans le cas des « Watchlists », les enquêteurs qui les transmettent doivent indiquer la manière de procéder en cas d'apparition d'une personne ciblée. Il en va de même en matière de « rules based targeting ».

La Police ne peut interdire à une compagnie aérienne de réaliser un vol à destination du Luxembourg pour empêcher l'arrivée sur le territoire national d'une personne déterminée. Toutefois, sur base de la législation applicable en matière d'immigration, une compagnie aérienne peut être obligée à ramener à ses frais un passager au lieu de provenance du vol.

Concernant les passagers des vols extra-Schengen, un visa est obligatoire pour les citoyens de certains pays non membres de l'espace Schengen pour entrer dans celui-ci. Pour les soixante pays non membres de l'UE, mais exempts de visa, il est prévu de mettre en place le « European Travel Information and Authorization System (ETIAS) »[7]. De cette manière, chaque personne en provenance d'un pays extra-Schengen sera contrôlée.

Discussion

- Un député pose la question de savoir pour quelle raison le ministère des Affaires étrangères et européennes n'est pas inclus dans ce système de transfert de données, alors qu'il a intérêt à obtenir des informations sur les personnes qui demandent l'autorisation d'entrer dans le pays. En réponse, il est précisé que la directive a pour objet la prévention et la détection d'infractions terroristes et non la migration et l'immigration. La mission de prévention incombe pour l'essentiel au SREL. En effet, en premier lieu, la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État dispose dans son article 3, paragraphe 1er que : « (1) Le SRE a pour mission de rechercher, d'analyser et de traiter, dans une perspective d'anticipation et de prévention, mais à l'exclusion de toute surveillance politique interne, les renseignements relatifs à: a) toute activité qui menace ou pourrait menacer la sécurité nationale ou la sécurité des États étrangers ou des organisations internationales ou supranationales avec lesquelles le Luxembourg poursuit des objectifs communs sur base d'accords ou de conventions bilatérales respectivement multilatérales, ou b) toute activité qui menace ou pourrait menacer les relations internationales du Grand-Duché de Luxembourg, son potentiel scientifique ou ses intérêts économiques définie par le Comité. ». En second lieu, les données recueillies concernent notamment des personnes sous surveillance discrète. Par ailleurs, les données permettent au SREL de répondre aux demandes de pays étrangers concernant les personnes voyageant en provenance ou à destination du Luxembourg ou en transit.

Si la loi précitée du 5 juillet 2016 donne au SREL déjà parmi les moyens et mesures de recherche applicables aux menaces d'espionnage, de prolifération et de terrorisme la possibilité de solliciter les données des dossiers passagers (article 8, paragraphe 1er, lettre a)), le projet de loi transposant la directive complète ces dispositions.

- Pour ce qui est de la qualité des données recueillies, la Police ne peut se baser à présent que sur l'expérience API acquise depuis 2006. Il s'agit des données de base contenues dans le document de voyage, prélevées lors de l'enregistrement des passagers.

En matière de PNR, les vols intra-Schengen pouvant être réservés 48 heures à l'avance, le passager peut indiquer des données qui ne correspondent pas à celles du document de voyage. Le « conformity check » effectué par la compagnie aérienne permet toutefois de vérifier la conformité des données du « boarding pass » avec celles du document de voyage. La Police ne s'intéresse qu'aux listes des passagers, pas aux billets.

[7] https://www.schengenvisainfo.com/fr/etias/

- L’article 8, transposant l’article 13, paragraphe 4 de la directive, interdit le traitement de données PNR qui révèlent notamment les opinions politiques ou la religion. Rappelant que la directive a pour objet la prévention et la détection des infractions terroristes et des formes graves de criminalité, un député souhaiterait connaître la raison pour laquelle le facteur « opinions politiques », en particulier, ne peut être pris en considération, alors qu’une opinion politique peut constituer un risque pour la sécurité.

Monsieur le Ministre indique que les critères ont fait l’objet de longues discussions. Le contenu finalement retenu forme l’accord trouvé entre les 28 États membres et le Parlement européen.

Dans ce contexte, un membre de la commission rappelle l’existence d’une liste noire des organisations terroristes établie par l’Union européenne.

Luxembourg, le 16 juillet 2018

Le Secrétaire-administrateur,
Marianne Weycker

La Présidente de la Commission de la Force publique,
Claudia Dall'Agnol

7151

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 690 du 16 août 2018

Loi du 1er août 2018 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Notre Conseil d'État entendu ;

De l'assentiment de la Chambre des Députés ;

Vu la décision de la Chambre des Députés du 26 juillet 2018 et celle du Conseil d'État du 27 juillet 2018 portant qu'il n'y a pas lieu à second vote ;

Avons ordonné et ordonnons :

Chapitre 1er - Dispositions générales

Art.1er.

La présente loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Art. 2.

Pour l'application de la présente loi, on entend par :

1° « transporteur aérien » : toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes ;
2° « passager » : toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers ;
3° « dossier passager » : le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités ;
4° « système de réservation » : le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations ;
5° « système de contrôle des départs » : le système utilisé pour contrôler les passagers lors de l'embarquement ;
6° « données PNR » : les données contenues dans le dossier passager et énumérées à l'annexe I ;
7° « méthode push » : la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'informations passagers telle que créée à l'article 3 ;
8° « infractions terroristes » : les infractions visées au Livre II, Titre 1ier, Chapitre III-1 du Code pénal ;
9° « formes graves de criminalité » : les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans ;
10° « dépersonnaliser par le masquage d'éléments des données » : rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée ;

11° « services compétents » : les services visés à l'article 13.

Chapitre 2 - Unité d'informations passagers

Art. 3.

Il est créé au sein de la Police grand-ducale une Unité d'informations passagers, ci-après désignée « UIP », qui est chargée :

1° de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données ;
2° du transfert de ces données et des résultats de leur traitement aux services compétents ;
3° de l'échange de ces données et des résultats de leur traitement avec les unités d'informations passagers des autres États membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4.

(1) Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Il est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

(2) Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel de l'Administration des douanes et accises et du Service de renseignement de l'État. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Les membres du personnel de l'Administration des douanes et accises et du Service de renseignement de l'État sont désignés à l'UIP par une décision conjointe du ministre ayant la Police grand-ducale dans ses attributions et du ministre du ressort. Ils continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

Chapitre 3 - Transfert des données par les transporteurs aériens

Art. 5.

Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la méthode push, les données PNR de tous les passagers en provenance de, à destination de ou transitant par le Luxembourg pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien.

Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR incombe au transporteur aérien qui assure le vol.

Art. 6.

(1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes :

1° 48 heures avant l'heure de départ programmée du vol ;
2° 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 qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point 2°, peut se limiter à une mise à jour du transfert visé à l'alinéa 1er, point 1°.

(2) Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP peut demander, au cas par cas, le transfert de données PNR en dehors des délais prévus au paragraphe 1er.

Art. 7.

(1) Les données PNR sont transférées à l'UIP par voie électronique au moyen de protocoles communs et de formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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.

Les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisés pour leurs transferts.

(2) En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union européenne en matière de protection des données soit pleinement respecté.

(3) Dans l'hypothèse où un transporteur aérien ne conserve pas les données API énumérées à l'annexe I, point 18, par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, il transfère également ces données par la méthode « push » à l'UIP. Dans le cas d'un tel transfert, toutes les dispositions de la présente loi s'appliquent à ces données API.

Chapitre 4 - Traitement des données PNR

Art. 8.

Le traitement de données PNR qui révèlent 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 est interdit.

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive.

Art. 9.

Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données supplémentaires dès réception et de façon définitive.

Art. 10.

(1) L'UIP traite les données PNR en vue de réaliser une évaluation des passagers avant leur arrivée prévue sur le territoire national ou leur départ prévu du territoire national afin d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis compte tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

(2) Pour réaliser cette évaluation l'UIP peut comparer les données PNR :

1° aux traitements de données à caractère personnel mis en œuvre par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;
2° à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur 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.

(3) L'UIP réexamine individuellement, par des moyens non automatisés, toute concordance positive obtenue à la suite d'un traitement automatisé des données PNR effectué en vertu du présent article.

(4) L'UIP transmet aux services compétents, au cas par cas, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au présent article ou le résultat du traitement de ces données.

(5) Les conséquences de l'évaluation des passagers ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union européenne à la libre circulation sur le territoire du Grand-Duché de Luxembourg tel que prévu par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.

(6) Lorsque les évaluations sont réalisées pour des vols entre le Grand-Duché de Luxembourg et un autre État membre de l'Union européenne auquel s'applique le règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), les conséquences de ces évaluations doivent respecter ledit règlement.

Art. 11.

L'UIP traite les données PNR afin de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations visées à l'article 10.

Art. 12.

L'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, dûment motivées et fondées sur des motifs suffisants visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques aux fins visées à l'article 1er, et visant à communiquer aux services compétents ou, le cas échéant, à Europol, le résultat de ce traitement.

Chapitre 5 - Services compétents

Art.13.

Sont habilités à demander à l'UIP ou à recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, en vue de procéder à un examen approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et poursuites en la matière :

1° la Police grand-ducale ;
2° le Service de renseignement de l'État conformément à l'article 5, paragraphe 4, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ;
3° l'Administration des douanes et accises.

En recherchant les crimes et délits visés à l'article 2, points 8° et 9°, le procureur d'État peut, par une décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 12.

Art. 14.

Les services compétents ne peuvent traiter les données PNR et le résultat du traitement de ces données que pour les finalités de la présente loi telles que définies à l'article 1er.

L'alinéa 1er est sans préjudice des compétences de la Police grand-ducale et de l'Administration des douanes et accises lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement.

Art. 15.

Les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Les décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peuvent pas être fondées sur 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.

Chapitre 6 - Échange d'informations entre les États membres de l'Union européenne

Art. 16.

Lorsqu'une personne est identifiée conformément à l'article 10, l'UIP communique toutes les données pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP des autres États membres de l'Union européenne concernés.

Lorsque l'UIP est destinataire d'informations telles que visées à l'alinéa 1er de la part d'une autre UIP, elle transmet ces informations aux services compétents.

Art. 17.

(1) L'UIP transmet, dès que possible, à l'UIP d'un autre État membre de l'Union européenne qui en fait la demande, les données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par masquage conformément à l'article 26, et, si nécessaire, le résultat de tout traitement de ces données, s'il a déjà été réalisé conformément à l'article 10.

La demande, dûment motivée, peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière.

Si les données demandées ont été dépersonnalisées par masquage conformément à l'article 26, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que le transfert est nécessaire aux fins visées à l'article 12 et si elle y est autorisée par le procureur général d'État ou son délégué.

Les dispositions du présent paragraphe ne portent pas atteinte aux dispositions tant internationales que nationales sur l'entraide judiciaire internationale en matière pénale.

(2) Dans des cas d'urgence, les autorités compétentes des autres États membres, désignées conformément à l'article 7, paragraphe 1er , de la directive (UE) 2016/661 du Parlement européen et du Conseil du 27 avril 2016 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 et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe 1er sont applicables.

(3) À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un État membre a le droit de demander à ce que l'UIP obtienne des données PNR conformément à l'article 6, paragraphe 2, et les communique à l'UIP requérante.

Art. 18.

L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres États membres de l'Union européenne des données PNR ou les résultats du traitement de ces données.

Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre État membre de l'Union européenne, il transmet copie de sa demande à l'UIP.

Art. 19.

L'échange de données effectué en application du présent chapitre peut avoir lieu par l'intermédiaire de tous les canaux de coopération existant entre les services compétents des États membres de l'Union européenne.

La langue utilisée pour la demande et l'échange des données est celle applicable au canal utilisé.

Chapitre 7 - Conditions d'accès aux données PNR par Europol

Art. 20.

(1) Dans les limites de ses compétences et pour l'accomplissement de ses missions, Europol peut présenter à l'UIP, au cas par cas, par l'intermédiaire de son unité nationale, une demande électronique dûment motivée visant à obtenir des données PNR spécifiques ou le résultat du traitement de ces données :

1° lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des États membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes dans la matière et ;
2° dans la mesure où ladite infraction relève de la compétence d'Europol.

(2) La demande énonce les motifs sur lesquels s'appuie Europol pour estimer que la transmission de données PNR ou du résultat de traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée ou à des enquêtes en la matière.

Chapitre 8 - Transfert de données vers des pays non membres de l'Union européenne

Art. 21.

L'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si :

1° l'une des conditions prévues à l'article 34, paragraphe 1er, point d) de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est remplie ;
2° l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité ;
3° le transfert est nécessaire aux fins telles que définies à l'article 1er ;
4° le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er ;
5° les conditions prévues à l'article 17, paragraphe 1er sont remplies.

Les dispositions du présent article ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

Art. 22.

(1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre État membre de l'Union européenne à un pays non membre de l'Union européenne que si l'État membre auprès duquel les données ont été collectées a donné son accord au transfert.

(2) Dans des circonstances exceptionnelles, les données PNR peuvent être transférées à un pays non membre de l'Union européenne sans l'accord du pays membre de l'Union européenne auprès duquel les données ont été collectées si les conditions suivantes sont remplies :

1° 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 de l'Union européenne ou un pays tiers ;
2° l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'État membre de l'Union européenne, qui n'a pas pu donner son accord en temps utile, est informée sans retard et le transfert est dûment enregistré et soumis à une vérification à posteriori.

Art. 23.

L'UIP ne peut transférer des données PNR et les résultats du traitement de ces données aux autorités compétentes de pays non membres de l'Union européenne qu'après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte les conditions et garanties de la présente loi.

Art. 24.

Le délégué à la protection des données visé à l'article 29 est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

Chapitre 9 - Durée de conservation et dépersonnalisation des données

Art. 25.

L'UIP conserve les données PNR pendant une durée maximale de cinq ans à compter du transfert par le transporteur aérien.

À l'issue de cette période de cinq ans, elle efface les données PNR de manière définitive. Cette disposition ne s'applique pas si les données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière.

Art. 26.

(1) À l'expiration d'une période de six mois à compter du transfert par le transporteur aérien, l'UIP dépersonnalise les données PNR par le masquage des éléments suivants :

1° le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR ;
2° l'adresse et les coordonnées ;
3° des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne ;
4° les informations « grands voyageurs » ;
5° les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte ;
6° toute donnée API qui a été recueillie.

(2) À l'expiration de la période de six mois visée au paragraphe 1er, la communication de l'intégralité des données PNR n'est autorisée que sous les conditions suivantes :

1° elle est nécessaire aux fins visées à l'article 12 ;
2° elle a été approuvée par le procureur général d'État ou son délégué ou, si les données sont destinées à être communiquées au Service de renseignement de l'État, par la commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Art. 27.

L'UIP ne conserve le résultat de l'évaluation réalisée en vertu de l'article 10 que le temps nécessaire pour informer les services compétents et, s'il y a lieu, les UIP des autres États membres de l'Union européenne de l'existence d'une concordance positive.

Lorsque, à la suite du réexamen individuel par des moyens non automatisés conformément à l'article 10, paragraphe 3, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées en vertu de l'article 25, de manière à éviter de futures fausses concordances positives.

Chapitre 10 - Protection des données à caractère personnel

Art. 28.

L'autorité de contrôle visée à l'article 39 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 8 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et elle dispose, à cette fin, des pouvoirs prévus à l'article 14 de la même loi.

Art. 29.

(1) Le responsable de l'UIP désigne un délégué à la protection des données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

(2) Le délégué à la protection des données contrôle le traitement des données PNR et met en œuvre les garanties pertinentes au sein de l'UIP.

Il informe et conseille le responsable et le personnel de l'UIP sur les obligations qui leur incombent en matière de protection des données.

Il fait office de point de contact pour les personnes concernées pour toutes les questions relatives au traitement de leurs données PNR et pour la Commission nationale pour la protection des données.

(3) Le délégué à la protection des données effectue ses missions en toute indépendance.

Il fait directement rapport au responsable de l'UIP.

Par dérogation à l'alinéa 2, et sans préjudice du paragraphe 4, alinéa 2, en cas de problèmes relevant de la protection des données, le délégué à la protection des données rapporte directement au directeur général de la Police grand-ducale ou, s'il juge nécessaire, au ministre ayant la Police grand-ducale dans ses attributions.

(4) Le délégué à la protection des données a accès à toutes les données traitées par l'UIP.

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données conformément à la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Art. 30.

L'UIP met à la disposition du public, par les moyens de communication appropriés, les informations suivantes :

1° ses coordonnées ;
2° les coordonnées du délégué à la protection des données ;
3° les finalités du traitement auquel sont destinées les données PNR ;
4° le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité ;
5° l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31.

(1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 13 à 17 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 44 à 46 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 32.

L'UIP conserve, traite et analyse les données PNR en un ou des endroits sécurisés situés sur le territoire du Grand-Duché de Luxembourg.

Art. 33.

Le responsable de l'UIP met en œuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et la nature des données PNR.

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en œuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 28, paragraphe 2 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 34.

L'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

Cette documentation comprend :

1° le nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès ;
2° les demandes formulées par les services compétents et les UIP des autres États membres de l'Union européenne ;
3° toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Art. 35.

L'UIP tient des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

Les registres des opérations de consultation et de communication indiquent la finalité, la date et l'heure de l'opération et l'identité de la personne qui a consulté ou communiqué les données PNR ainsi que l'identité des destinataires de ces données.

Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit.

L'UIP met les registres à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Les registres sont conservés pendant cinq ans.

Art. 36.

Lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe sans retard injustifié la personne concernée et la Commission nationale pour la protection des données de cette atteinte.

Chapitre 11 - Sanctions

Art. 37.

La violation intentionnelle de l'article 8, alinéa 1er et de l'article 15 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125 000 euros ou d'une de ces peines seulement. La juridiction saisie prononce la cessation du traitement contraire aux dispositions de l'article 8, alinéa 1er et de l'article 15 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 47, paragraphes 1er, 2, 4, 5 et 6 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38.

(1) Est puni d'une amende d'un montant maximum de 50 000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements visés à l'article 3, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

(2) Le manquement est constaté par un procès-verbal établi par la Police grand-ducale. Copie en est transmise au transporteur aérien.

Le transporteur aérien a accès au dossier et est mis à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction.

L'amende est prononcée par le ministre ayant la Police grand-ducale dans ses attributions.

(3) La décision du ministre qui est motivée est susceptible d'un recours en réformation à introduire devant le Tribunal administratif dans un délai d'un mois à compter de la notification.

Chapitre 12 - Dispositions modificatives

Art. 39.

Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

« (4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, ou de cyber-menace dans la mesure où celle-ci est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12, de la loi du 1er août 2018 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Le directeur du SRE rapporte tous les mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en œuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Art. 40.

À l'article 8, paragraphe 1er de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, la lettre a) est supprimée.

Chapitre 13 - Disposition finale

Art. 41.

La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « Loi du 1er août 2018 relative au traitement des données des dossiers passagers ».

ANNEXE I

Liste des données PNR

1° Code repère du dossier passager ;
2° Date de réservation/d'émission du billet ;
3° Date(s) prévue(s) du voyage ;
4° Nom(s) ;
5° Adresse et coordonnées (numéro de téléphone, adresse électronique) ;
6° Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation ;
7° Itinéraire complet pour le PNR concerné ;
8° Informations « grands voyageurs » ;
9° Agence de voyages/agent de voyages ;
10° Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation ;
11° Indications concernant la scission/division du PNR ;
12° Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée) ;
13° Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix ;
14° Numéro du siège et autres informations concernant le siège ;
15° Informations sur le partage de code ;
16° Toutes les informations relatives aux bagages ;
17° Nombre et autres noms de voyageurs figurant dans le PNR ;
18° Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée) ;
19° Historique complet des modifications des données PNR énumérées aux points 1 à 18.

Annexe II

Liste des infractions visées à l'article 2, point 9

1° Participation à une organisation criminelle ;
2° Traite des êtres humains ;
3° Exploitation sexuelle des enfants et pédopornographie ;
4° Trafic de stupéfiants et de substances psychotropes ;
5° Trafic d'armes, de munitions et d'explosifs ;
6° Corruption ;
7° Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union ;
8° Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro ;
9° Cybercriminalité ;
10° Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées ;
11° Aide à l'entrée et au séjour irréguliers ;
12° Meurtre, coups et blessures graves ;
13° Trafic d'organes et de tissus humains ;
14° Enlèvement, séquestration et prise d'otage ;
15° Vol organisé ou vol à main armée ;
16° Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art ;
17° Contrefaçon et piratage de produits ;
18° Falsification de documents administratifs et trafic de faux ;
19° Trafic de substances hormonales et d'autres facteurs de croissance ;
20° Trafic de matières nucléaires et radioactives ;
21° Viol ;
22° Infractions graves relevant de la Cour pénale internationale ;
23° Détournement d'avion/de navire ;
24° Sabotage ;
25° Trafic de véhicules volés ;
26° Espionnage industriel.

Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.

Le Ministre de la Sécurité intérieure,
Étienne Schneider

Cabasson, le 1er août 2018.
Henri

Doc. parl. 7151 ; sess. ord. 2016-2017 et 2017-2018 ; Dir. (UE) 2016/681.