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:

*

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