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:

*

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