N° 7151[9]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

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

* * *

RAPPORT DE LA COMMISSION DE LA FORCE PUBLIQUE

(19.7.2018)

La Commission se compose de : Mme Claudia DALL'AGNOL, Présidente-Rapportrice ; Mme Diane ADEHM, M. Marc ANGEL, Mme Nancy ARENDT, MM. Alex BODRY, Felix EISCHEN, Léon GLODEN, Gusty GRAAS, Max HAHN, Jean-Marie HALSDORF, Fernand KARTHEISER, Henri KOX, Alexander KRIEPS, Membres.

*

I. PROCEDURE LEGISLATIVE

Le projet de loi sous rubrique a été déposé à la Chambre des Députés le 19 juin 2017 par Monsieur le Ministre de la Sécurité intérieure. Le texte du projet, comprenant deux annexes, était accompagné d'un exposé des motifs, d'un commentaire des articles, d'un tableau de correspondance, d'une fiche financière, d'une fiche d'évaluation d'impact et du texte de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, ainsi que de ses deux annexes.

Le projet de loi a fait l'objet des avis :

- du Parquet général en date du 24 août 2017 ;
- des Parquets de Luxembourg et de Diekirch en date du 15 octobre 2017 ;
- du Tribunal d'arrondissement de et à Luxembourg en date du 18 septembre 2017 ;
- de la Commission nationale pour la protection des données en date du 23 novembre 2017 ;
- de la Cour supérieure de Justice en date du 20 novembre 2017 ;
- de la Chambre de Commerce en date du 13 décembre 2017.

Une première série d'amendements gouvernementaux a été soumise au Conseil d'État le 27 février 2018.

Le Conseil d'État a émis son avis sur ces amendements et le projet de loi le 30 mars 2018.

Le 27 avril 2018, le texte a été amendé une seconde fois par les auteurs.

Dans sa réunion du 4 mai 2018, la commission a désigné Mme Claudia Dall'Agnol comme rapportrice et a procédé à l'examen du projet de loi à la lumière de l'avis du Conseil d'État.

L'avis complémentaire du Conseil d'État a été rendu le 26 juin 2018.

La réunion de la commission du 5 juillet 2018 était consacrée à l'examen de l'avis complémentaire du Conseil d'État.

La commission a adopté le présent rapport le 19 juillet 2018.

II. CONSIDERATIONS GENERALES

Les données des dossiers passagers (Passenger Name Records, « PNR ») sont des informations non vérifiées, communiquées par les passagers, qui sont recueillies et conservées dans le système de réservation et de contrôle des départs des transporteurs aériens pour leur usage commercial. Elles comprennent des informations telles que les coordonnées du passager, la date du voyage et d'émission du billet, le mode de paiement utilisé et le poids des bagages.

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

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

a) Le cadre européen

L'idée de créer un cadre légal européen pour l'utilisation des données passagers à des fins répressives remonte à une proposition de la Commission européenne du 6 novembre 2007. La proposition de décision-cadre n'ayant toutefois pas été adoptée par le Conseil de l'Union européenne (UE) au moment de l'entrée en vigueur du traité sur le fonctionnement de l'Union européenne le 1er décembre 2009, elle a dû être remplacée par un nouveau texte. Dans sa communication du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers aux pays tiers, la Commission a décrit un certain nombre d'éléments essentiels d'une politique européenne dans ce domaine. Finalement, le 2 février 2011, la Commission a présenté une proposition de directive sur laquelle le Conseil Justice et Affaires intérieures (JAI) a dégagé une orientation générale le 26 avril 2012. Un vote de rejet de la Commission Libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen du 24 avril 2013 a toutefois bloqué la proposition de directive.

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

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

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

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

En date du 27 avril 2016, le Parlement européen et le Conseil ont par ailleurs adopté parallèlement le paquet sur la protection des données. Les deux instruments européens qui constituent le paquet sur

la protection des données s'ajoutent à la directive PNR, réformant en profondeur le droit de la protection des données au niveau de l'Union européenne.

b) Les points de discussion principaux sur la directive

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

L'inclusion des vols intra-communautaires opposait les États membres qui plaidaient pour l'inclusion obligatoire de tous les vols intra-UE aux États membres qui étaient opposés à l'inclusion de ces vols. Le compromis trouvé dans l'orientation générale adoptée en avril 2012 avait laissé le choix aux États membres de collecter ou non les données PNR sur tous ou sur certains vols intra-UE. En raison de la menace sécuritaire constituée par les combattants étrangers et des stratégies de contournement entretemps développées, l'inclusion des vols intra-UE n'a plus été un sujet controversé au sein du Conseil en 2015. L'expérience acquise par les services répressifs montre en effet que les combattants étrangers empruntent des trajets de plus en plus compliqués à travers l'Union européenne pour dissimuler leur point de départ initial et leur destination finale. Le même phénomène est observé à propos des membres d'organisations criminelles. Le Parlement européen souhaitait cependant voir limiter l'application de la directive aux vols en provenance ou à destination d'États non membres de l'Union européenne. Le texte de la directive tel qu'adopté le 27 avril 2016 retient finalement que les États membres sont libres de collecter les données PNR sur tous ou sur certains vols intra-UE. Dans une déclaration commune du 4 décembre 2015, les ministres JAI se sont engagés à faire pleinement usage de la faculté de recueillir des données PNR pour les vols intra-UE dès la mise en application de la directive. Ce choix est entériné dans le texte du projet de loi.

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

Un troisième élément de discussion était la durée de conservation des données PNR. La proposition de la Commission prévoyait une période initiale de conservation de trente jours, suivie d'une période supplémentaire de cinq ans au cours de laquelle les données seraient masquées. Les négociations entre États membres ont toutefois fait apparaître qu'une période initiale de trente jours était trop courte d'un point de vue opérationnel et le Conseil a retenu une période de conservation globale de cinq ans, subdivisée en deux périodes, une première période de deux ans au cours de laquelle les données seraient pleinement accessibles, et une seconde période de trois ans où les données servant à identifier le passager seraient masquées et leur divulgation complète serait subordonnée à des conditions strictes. Selon l'avis et les expériences des services répressifs, le système PNR ne permet en effet de lutter de manière efficace contre le terrorisme et la criminalité organisée que si les données restent actives pendant une certaine période. Comme les actes de terrorisme se préparent généralement sur une période plus longue, le système PNR doit être conçu de manière à ce qu'il permette de reconstituer l'activité d'un ou de plusieurs individus en remontant sur une période suffisamment longue. Le suivi des groupes terroristes exige d'établir des profils de mouvements, procédure qui s'inscrit dans le long terme. La probabilité qu'une information intéressante se trouve dans les données PNR recueillies depuis moins de trente jours est minimale. Par ailleurs, concernant le cas particulier des individus se rendant dans des camps d'entraînement en Syrie ou en Irak, selon les renseignements des services spécialisés, ces séjours

dépassent généralement trente jours. Un délai de trente jours est également trop court pour lutter contre d'autres formes de criminalité telles que le trafic de drogue. Les critères d'évaluation sont en effet établis sur base de l'analyse répétée des données de voyage d'un individu en particulier ou de personnes qui apparaissent régulièrement dans le même dossier de voyage. Or, les trafiquants de drogues sont déployés tous les quatre à six mois. Une période de temps suffisamment longue avant le masquage est nécessaire pour découvrir de telles routes et pour comprendre comment les criminels adaptent leurs habitudes. Le Parlement européen a soutenu la proposition initiale de la Commission. La Présidence luxembourgeoise a toutefois réussi à démontrer, sur base d'exemples concrets fournis par les services compétents des États membres et décrits ci-dessus, qu'une période active de trente jours n'est pas suffisante. Le texte de compromis retient que les éléments des données qui peuvent servir à identifier directement le passager auquel se rapportent les données doivent être masqués à l'expiration d'une période de six mois à compter de leur transfert par les transporteurs aériens.

En général, l'adoption de la directive PNR et la mise en place du système de traitement des données PNR a été subordonnée à l'insertion dans le dispositif de garanties de protection strictes. Ces garanties consistent notamment à imposer des conditions limitatives d'accès et de transfert des données PNR aux différentes autorités nationales, européennes ou extra-européennes, à limiter la conservation des données PNR comme exposé ci-dessus, ou encore à désigner un délégué à la protection des données chargé de contrôler le traitement des données PNR.

*

III. OBJET DU PROJET DE LOI

Le projet de loi a pour objet de transposer en droit national la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

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

Le premier chapitre du projet de loi contient les dispositions générales du texte, dont le champ d'application et les définitions clés de la loi en projet. Il est précisé que la loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Le deuxième chapitre crée au sein de la Police grand-ducale une Unité d'informations passagers et en règle les missions et la composition. L'UIP peut comprendre du personnel de l'Administration des douanes et accises et du personnel du Service de renseignement de l'État qui continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

Le troisième chapitre précise les modalités du transfert des données PNR par les transporteurs aériens.

Le quatrième chapitre concerne le traitement des données PNR par l'UIP, dont l'obligation d'effacer des données transférées autres que celles énumérées à l'annexe I du texte ou la manière dont les données peuvent être traitées.

Le cinquième chapitre traite des services compétents qui peuvent demander à l'UIP ou recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, à savoir la Police grand-ducale, le Service de renseignement de l'État et l'Administration des douanes et accises.

Les chapitres six, sept et huit décrivent les procédures pour échanger des données PNR ou le résultat du traitement de ces données, respectivement entre les États membres de l'Union européenne, avec Europol et avec des pays non membres de l'Union européenne.

Le neuvième chapitre concerne la durée de conservation des données PNR et la dépersonnalisation de ces données.

Le chapitre dix est consacré à la protection des données. La directive du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données est transposée en droit national parallèlement à la directive PNR. Le texte fait référence aux dispositions pertinentes du projet de loi de transposition de la directive du 27 avril 2016, notamment en ce qui concerne les droits des personnes et l'autorité de contrôle en matière de données PNR. En dehors de ces références, le présent chapitre comporte toute une série de dispositions spéciales qui sont destinées à garantir la protection des données PNR en particulier.

Le chapitre onze prévoit l'application de sanctions pénales lors de la violation intentionnelle de l'interdiction de traiter des données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle. En outre, une sanction administrative est prévue pour sanctionner le transporteur aérien qui n'a pas rempli ses obligations en vertu de cette loi.

Finalement, les chapitres douze et treize contiennent les dispositions modificatives et finale.

*

IV. LES AVIS RELATIFS AU PROJET DE LOI

1. Les avis du Conseil d'Etat

Dans son avis du 30 mars 2018, le Conseil d'État précise qu'il n'entend pas faire une appréciation de la directive elle-même au regard des critères établis dans l'avis 1/15 rendu par la Cour de justice de l'Union européenne en date du 26 juillet 2017 relative à la compatibilité du projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers avec l'article 16 du TFUE et les articles 7, 8 et l'article 52, paragraphe 1er, de la Charte des droits fondamentaux de l'Union européenne.

Dans son analyse article par article, le Conseil d'État émet une série d'oppositions formelles qui sont basées sur le fait que les auteurs du projet de loi n'ont pas repris correctement ou dans leur totalité les articles de la directive. Le détail de ces observations peut être retracé dans le commentaire des articles.

La Haute Corporation s'interroge en outre sur la composition de l'UIP. Le choix de la Police grand-ducale en tant qu'administration de rattachement de l'UIP est, en soi, conforme à la directive. L'unité nouvellement créée sera composée non seulement de personnel provenant de la Police, mais encore de personnel pouvant être détaché de l'Administration des douanes et accises ainsi que du SRE. Le Conseil d'État s'interroge sur le statut de ce personnel « détaché » et sur ses compétences. Il relève que le projet de loi est en contradiction avec le statut général des fonctionnaires de l'État, puisqu'il prévoit que les personnes concernées continueront à agir « dans les limites des attributions légales de l'administration dont (elles) relève(nt) ». Bien que le Conseil d'État comprenne l'utilité d'une disposition qui prévoit que les différents services compétents disposent d'un représentant en tant qu'« agent de liaison » au sein de l'UIP ainsi que l'utilité d'une solution qui assure que ces agents gardent un accès aux traitements de données propres aux différents services d'origine, il se doit d'émettre une opposition formelle pour insécurité juridique.

Concernant les sanctions en cas de violation des différents prescrits de la loi en projet, le Conseil d'État attire l'attention sur le fait que les trois projets composant le « Paquet protection des données » contiennent des approches différentes dans la mesure où les méconnaissances des règles imposées sont sanctionnées tantôt par des dispositions pénales classiques, tantôt par des sanctions administratives imposées par la CNPD. Concernant plus précisément l'interdiction du traitement de données révélant des données sensibles et l'obligation d'effacement définitif si de telles données étaient néanmoins collectées, la Haute Corporation estime qu'afin d'assurer le respect du principe constitutionnel de la légalité de la peine, il y a lieu de préciser lequel des deux comportements est sanctionné : le traitement illicite ou bien le défaut d'effacement ? Il y a également lieu de préciser s'il s'agit d'une infraction intentionnelle, nécessitant la volonté déterminée de contrevenir à la disposition légale, ou bien si le

simple fait de procéder à un tel traitement (ou non-effacement) est suffisant pour encourir la peine prévue par la loi, sans que la preuve d'un dol spécial doive être rapportée. Le Conseil d'État considère en effet qu'un simple dysfonctionnement au sein de l'unité, dépourvu de toute intention criminelle, qui serait éventuellement sanctionnable du point de vue disciplinaire, n'est pas de nature à entraîner la responsabilité pénale.

Finalement, le Conseil d'État réserve sa position quant à la dispense du second vote constitutionnel en attendant des explications sur la différence de traitement introduite en ce qui concerne l'amende qu'un transporteur aérien encourt en cas de manquement de transmettre les données PNR par rapport aux données relatives aux passagers dit « données API ». Le Conseil d'État compare en effet les amendes prévues aux amendes déjà prévues par l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration à l'encontre des entreprises de transport qui ne respectent pas les obligations leur imposées par l'article 106 de la même loi, et concernant les données API.

Après l'examen d'une série d'amendements gouvernementaux, le Conseil d'État a levé la plupart des oppositions formelles et a fait des propositions pour les deux autres dans son avis complémentaire du 26 juin 2018. La Haute Corporation rappelle encore qu'il est fait référence à la future loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale qui fait l'objet du projet de loi n° 7168 ainsi qu'à la loi en projet n° 7184 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. Il relève qu'il faudra, d'une part, veiller à compléter les références à ces lois par leurs dates de promulgation, une fois que celles-ci seront connues, et, d'autre part, éviter que la loi en projet entre en vigueur antérieurement aux lois auxquelles il est fait référence.

2. L'avis des autorités judiciaires

L'avis des autorités judiciaires se compose de l'avis du Parquet général du 24 août 2017, de l'avis des Parquets de Luxembourg et de Diekirch du 15 octobre 2017 et de l'avis du Tribunal d'arrondissement de et à Luxembourg du 18 septembre 2017 et a été soumis à la Chambre des Députés en date du 10 novembre 2017.

Dans son avis du 24 août 2017, le Parquet général rappelle tout d'abord la finalité et la nécessité de collecter les données PNR. Effectivement, selon le Parquet général, les données PNR se révèlent essentielles pour les évaluations des risques présentés par certaines personnes et l'établissement des liens entre les personnes déjà connues et des personnes inconnues. La finalité du traitement des données des passagers s'inscrit ainsi clairement dans le cadre de la prévention et de la recherche d'infractions terroristes, des formes graves de criminalité, des atteintes à l'ordre public dans le cadre de la radicalisation violente et des activités pouvant menacer les intérêts fondamentaux des États membres de l'Union européenne.

Le Parquet général déplore que le gouvernement ait opté à ne pas imposer l'obligation de transmettre les données PNR à d'autres opérateurs économiques autres que les transporteurs aériens, étant donné que les organisations terroristes et criminelles ne se limitent pas à l'utilisation du transport aérien pour organiser leurs activités.

Finalement, le Parquet général s'inquiète concernant le rôle et les droits des autorités judiciaires en la matière. Ainsi, concernant l'Unité d'informations passagers à créer au sein de la Police grand-ducale, le Parquet général pose la question s'il n'était pas opportun qu'un représentant des autorités judiciaires de poursuite en fasse partie, puisque la recherche, la constatation et la poursuite des infractions relèvent de la compétence des autorités judiciaires de poursuite, et si ce représentant ne devrait pas même être le responsable de l'UIP. Le Parquet propose également de procéder à une adaptation du Code de procédure pénale, à l'instar de ce qui a été fait en Belgique, pour que le Parquet général puisse charger un officier de police judiciaire de requérir l'UIP afin de communiquer des données PNR et que cette mesure peut même porter sur un ensemble de données relatives à une enquête pénale spécifique.

L'avis des Parquets de Luxembourg et de Diekirch du 15 octobre 2017 concerne principalement les dispositions qui impliquent l'intervention des parquets ou qui, selon l'avis, devraient les impliquer. Ils se rallient à l'avis du Parquet général en ce qui concerne la composition de l'UIP en posant la question s'il ne serait pas recommandable de faire présider l'UIP par un magistrat afin de veiller au mieux à la protection des données à caractère personnel dans le cadre de la recherche, de la constatation et de la

poursuite des infractions de terrorisme et de criminalité grave qui se déroulent sous la direction des autorités judiciaires. Il est en outre proposé, en vue d'une transposition correcte et intégrale de la directive, de faire figurer les autorités judiciaires dans l'énumération des autorités habilitées à demander et à recevoir de la part de l'UIP des données PNR ou le résultat du traitement de ces données.

Le Tribunal d'arrondissement de et à Luxembourg discute dans son avis du 18 septembre 2017 surtout la question du juste équilibre entre les nécessités de la politique sécuritaire et la protection des données personnelles. Selon cet avis, il est entendu que le but de la législation projetée n'est pas discutable, la connaissance des données en relation avec les déplacements effectués par les personnes constitue, à l'évidence, un élément très important dans la lutte, tant contre le terrorisme, que la criminalité grave. Il faudra néanmoins veiller à entourer la collecte de ces données essentiellement liées notamment à la liberté d'aller et de venir d'une protection adéquate. Après une révision des chapitres du projet de loi, le Tribunal d'arrondissement de et à Luxembourg conclut : « Dans l'ensemble le projet de loi reflète dès lors à suffisance un juste équilibre entre l'utilité et la nécessité indiscutable de la collecte des données PNR et le souci de protection des données personnelles qui ne devraient en aucun cas être accessibles et utilisables en dehors du champ légal dans le cadre duquel elles ont été collectées. »

3. L'avis de la Commission nationale pour la protection des données

L'avis de la Commission nationale pour la protection des données (CNPD) du 23 novembre 2017 est entré à la Chambre des Députés le 18 décembre 2017. En guise d'introduction, la CNPD se déclare bien consciente que le législateur a l'obligation de transposer la directive européenne en droit national au plus tard pour le 25 mai 2018, faute de risquer un recours en manquement de la part de la Commission européenne. Ainsi, elle n'a pas l'intention de remettre en cause en lui-même le système PNR, bien que la CNPD soit plutôt critique du système en tant que tel. La CNPD a limité ses remarques aux dispositions où les auteurs du projet de loi ont usé la marge de manœuvre laissée aux États membres lors de la transposition.

Quant au champ d'application, la CNPD prend note que les auteurs du projet de loi ont opté, à l'instar de leurs homologues belges, français ou allemands, d'inclure les vols intra-UE dans le champ d'application du projet de loi afin de maximiser l'efficacité du système PNR. Par ailleurs, la CNPD approuve la décision des auteurs du projet de loi de ne pas avoir étendu le système PNR aux agences ou organisateurs de voyages, ainsi qu'aux opérateurs économiques autres que les transporteurs ou auprès de transporteurs autres que les transporteurs aériens. Comme un tel élargissement du champ d'application du système PNR menacerait de manière encore plus importante les droits fondamentaux des personnes concernées, il paraît raisonnable d'attendre l'évaluation de la Commission européenne de tous les éléments de la directive PNR. Finalement, la CNPD se demande si l'obligation de transmettre à l'UIP les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg s'impose aussi aux taxis aériens privés.

S'agissant des bases de données et critères d'évaluation auxquels les données PNR peuvent être comparées, la CNPD est d'avis que le projet de loi dans sa première version ne définit pas avec exactitude les banques de données en cause, ni une liste exhaustive énumérant les critères d'évaluation. Dans l'optique de la CNPD, le projet de loi devrait identifier et énumérer expressément dans le corps du texte les différentes banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions. Un règlement grand-ducal pourra alors prévoir une liste exhaustive des critères d'évaluation prédéterminés qui pourrait au besoin être complétée ou modifiée si nécessaire.

Quant aux différentes catégories de données PNR, qui ont été critiquées pour ne pas être suffisamment claires et précises par le Contrôleur européen de la protection des données (CEPD), la CNPD recommande de décrire de manière plus précise et concise les catégories de données PNR « grands-voyageurs » et « remarques générales ».

Pour ce qui est de la conservation des données, la CNPD recommande d'inclure dans le corps du texte législatif une durée de conservation maximale à respecter par les services compétents en cas de transfert de données par l'UIP.

Finalement, quant au droit à l'information des personnes concernées, la CNPD suggère d'inclure dans le projet de loi les indications sur la durée de conservation et, le cas échéant, des catégories de destinataires des données PNR, dans les informations que l'UIP doit transmettre au public. La CNPD

recommande en outre de prévoir dans le projet de loi une disposition selon laquelle l'UIP est obligée d'informer les personnes concernées dont les données PNR ont été utilisées ou transférées, tout en y incluant la possibilité d'un retard ou d'une limitation du droit à l'information des personnes concernées conformément à l'article 13, paragraphe 3 du projet de loi transposant la directive 2016/680.

4. L'avis de la Cour supérieure de Justice

L'avis de la Cour supérieure de Justice du 20 novembre 2017 est intervenu à la Chambre des Députés en date du 18 décembre 2017.

La Cour supérieure de Justice souligne que le projet de loi doit être considéré avec les projets de loi ayant pour objet la mise en œuvre et la transposition en droit national du règlement (UE) 2016/679 et la directive européenne (UE) 2016/680 visant à l'harmonisation des dispositions nationales des États membres en matière de protection de données personnelles, puisque les trois projets forment un paquet de dispositions sur cette protection de données. Ils instaurent une réforme du cadre existant, visant à renforcer la protection des données à caractère personnel et à adapter les règles aux nouveaux défis réglementaires, dans un souci de pérennité et de neutralité technologique, en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

La Cour supérieure de Justice rappelle, à titre d'introduction, que la Cour de justice de l'Union européenne (CJUE) a dans son avis n° 1/15 du 26 juillet 2017 relatif à un projet d'accord entre le Canada et l'Union européenne sur le transfert de données des dossiers passagers aériens depuis l'Union européenne vers le Canada estimé que cet accord, qui reprend des dispositions identiques à celles de la directive PNR, était incompatible avec les articles 7, 8 et 21 ainsi qu'avec l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne.

Cet avis de la CJUE a amené la Cour supérieure de Justice à s'interroger sur la compatibilité de la directive PNR avec les susdits articles de la Charte. La Cour supérieure de Justice en a tiré la conclusion que « la CJUE a conclu la très longue polémique suscitée par les accords PNR et la directive (UE) 2016/681 et elle a validé le système PNR dans son principe tout en émettant des réserves ». La Cour continue à analyser les réserves en détail comme suit :

> « Parmi les points listés, la CJUE estime tout d'abord que les 19 catégories de données qui figurent dans l'accord (les mêmes dans tous les accords PNR ainsi que dans la directive européenne) devraient être définies de manière claire et précise et des termes comme *« toutes les coordonnées disponibles »* ou *« remarques générales »* sont à exclure dès lors qu'ils ne fixent aucune limitation quant à l'étendue et à la nature des informations susceptibles d'y figurer. La CJUE exclut par ailleurs le transfert de données sensibles (celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou concernant l'état de santé ou la vie sexuelle d'une personne), comme étant contraire à la Charte des droits fondamentaux.
>
> La CJUE relève encore que les autorités devront produire des « *modèles et critères préétablis (...) spécifiques et fiables* » de sorte à aboutir à des « *résultats ciblant les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou de criminalité transnationale grave* ». Les avancées technologiques devront être un outil au service de la société et non un prétexte à instituer des politiques ultra-sécuritaires violant les droits fondamentaux.
>
> S'agissant de la conservation des données, la CJUE relève que la conservation dans le pays destinataire doit être limité au strict nécessaire après le départ du passager, mais la durée de cinq ans prévue par la directive (UE) 2016/681 et reprise par le projet de loi sous avis ne semble pas « *excéder les limites de ce qui est strictement nécessaire à des fins de lutte contre le terrorisme et la criminalité transnationale grave* ».
>
> Quant au possible transfert de données PNR vers un pays tiers, la CJUE ne l'admet que si la Commission a constaté l'existence d'un « *niveau adéquat* » de protection dans le pays destinataire (art. 25, paragraphe 6 de la directive 95/46), ou « *substantiellement équivalent* » à celui assuré au sein de l'UE.
>
> Quant au contrôle du respect des exigences de la protection des données par le biais d'une autorité indépendante, exigence figurant tant dans la Charte (art. 8, paragraphe 3) que dans le Traité (Article 16, paragraphe 2 TFUE), seule une « *autorité publique indépendante* » présente les qualités requises et la CJUE n'admet pas d'autres termes pour définir l'autorité visée. »

La Cour fournit en outre quelques remarques et observations dans une analyse chapitre par chapitre du projet de loi. Dans ses remarques, la Cour se rallie aux avis des autres autorités judiciaires qu'il serait opportun de prévoir la possibilité d'un détachement d'un membre des Parquets ou du Parquet général vers l'UIP afin d'assurer une meilleure liaison à ce niveau. Concernant la méthode de transmission des données PNR, la Cour explique que la méthode à employer dite « push » est la méthode plus protectrice des données personnelles, mais qu'il serait opportun de la préciser davantage dans le texte du projet de loi.

En outre, la Cour qualifie le texte de l'article 13 comme étant pas très clair en ce qu'il semble limiter la transmission des données PNR aux autorités judiciaires seulement selon les règles du Code de procédure pénale et non en vertu du projet de loi. Si le fait de limiter la demande et la réception des données au seul cadre de prévention et de détection des infractions visées par la loi s'inscrit dans les principes prévalant en matière de protection des données à caractère personnel, il y a lieu d'observer que les termes de « dans la limite du besoin d'en connaître » sont imprécis et risquent de donner lieu à des interprétations diverses.

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

5. L'avis de la Chambre de Commerce

L'avis de la Chambre de Commerce du 13 décembre 2017 a été soumis à la Chambre des Députés en date du 20 décembre 2017. Dans ses considérations générales, la Chambre de Commerce attire l'attention du législateur sur la nécessité de coordonner l'entrée en vigueur du projet de loi avec les deux autres projets de loi auxquels il fait référence (projets de loi n° 7168 et n°7184).

Quant aux implications financières de l'adoption du projet de loi, la Chambre de Commerce regrette que la mise en place du système de transfert des données PNR entraîne des coûts supplémentaires à charge des opérateurs du secteur. En ce qui concerne l'impact du projet de loi sur les finances de l'État, la Chambre de Commerce regrette que la fiche financière ne contienne aucune donnée précise concernant la mise en place effective du système de traitement des données PNR.

Le transfert des données PNR par les transporteurs aériens est à la base du système de traitement des données PNR mis en place par le projet de loi. Soucieuse que cette obligation n'engendre pas d'incertitude juridique pour les transporteurs aériens, la Chambre de Commerce souhaite mettre en évidence plusieurs points sur lesquels il lui semble particulièrement important de faire évoluer le projet de loi. Tout d'abord, la Chambre de Commerce regrette que l'article 5 du projet de loi ne reflète pas de manière suffisamment explicite le principe fondamental du système mis en place en vertu duquel les données PNR visées par l'obligation de transfert sont exclusivement les données recueillies par les transporteurs dans le cours normal de leurs activités de transport aérien au jour du transfert. Elle constate ensuite que l'obligation systématique de transfert des données d'un vol par le transporteur aérien devrait être destinée aux UIP de chaque État membre sur le territoire duquel le vol décollera ou atterrira, et non pas uniquement à l'UIP luxembourgeoise. De manière plus générale, la Chambre de Commerce s'interroge quant aux limites du système envisagé au sein duquel le traitement des données PNR sera, selon sa compréhension, limité à un contrôle national, transmis aux autres autorités compétentes uniquement en cas de correspondance positive. La Chambre de Commerce suggère également de limiter les échéances du transfert de données PNR à deux par vol.

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

Quant au régime de sanctions, la Chambre de Commerce s'interroge sur l'opportunité d'adopter un texte de nature à porter atteinte à un régime de protection unifié et cohérent tel qu'il a vocation à être régi par le projet de loi n°7168. La Chambre de Commerce s'interroge également quant à la légalité de certaines peines visées par le projet de loi. La Chambre de Commerce dénonce enfin le caractère

manifestement disproportionné de l'amende pouvant aller jusqu'à 50 000 € par vol pour lequel un transporteur aérien ne remplirait pas son obligation de transfert de données PNR.

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

*

V. COMMENTAIRE DES ARTICLES

Chapitre 1er – *Dispositions générales*

Articles 1er et 2

L'article 1er transpose l'article 1er de la directive PNR et détermine l'objet de la loi et précise et limite les finalités pour lesquelles les données PNR peuvent être traitées : sont visés les transporteurs aériens, lesquels doivent transférer les données des dossiers passagers pour le traitement de celles-ci à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

L'article 2 définit les différentes notions. Par amendement gouvernemental du 27 avril 2018, le point 7, en l'absence d'une définition de l'Unité d'informations passagers (UIP), a été complété par la référence à l'article 3 créant l'UIP, tel que suggéré par le Conseil d'État dans son avis du 30 mars 2018. Par ailleurs, un point 11 nouveau a été ajouté pour la notion de « services compétents », demande formulée par le Conseil d'État notamment à l'endroit de l'article 10, paragraphe 1er.

Chapitre 2 – *Unité d'informations passagers*

Articles 3 et 4

L'article 3 met en place au sein de la Police grand-ducale l'UIP chargée de la collecte, du transfert et de l'échange des données et des résultats de leur traitement, tel que prévu par la future loi.

L'UIP sera intégrée dans la direction « relations internationales » rattachée au comité de direction de la Police grand-ducale.

Dans son avis, le Conseil d'État approuve le choix de la Police grand-ducale en tant qu'administration de rattachement de l'UIP. Ce choix est conforme à l'article 4, paragraphe 1er de la directive, selon lequel « Chaque État membre met en place ou désigne une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité (…). ». Ce choix se justifie d'autant plus que « la Police grand-ducale est déjà à l'heure actuelle destinataire des données transférées en vertu de la loi précitée du 21 décembre 2006[1] ».

L'article 4 prévoit que l'UIP peut comprendre, outre le personnel policier, du personnel de l'Administration des douanes et accises (ADA) et du Service de renseignement de l'État (SRE).

Le Conseil d'État pose la question du statut et des compétences du personnel détaché en rappelant que, suivant l'article 7 du Statut général des fonctionnaires de l'État, le détachement consiste en « l'assignation au fonctionnaire d'un autre emploi correspondant à sa catégorie et à son grade dans une autre administration, dans un établissement public ou auprès d'un organisme international », qui a comme conséquence que « le fonctionnaire relève de l'autorité hiérarchique de l'administration, respectivement de l'établissement ou de l'organisme auquel il est détaché ». Par conséquent, les fonctionnaires détachés de l'ADA et du SRE « relèveront entièrement de la Police grand-ducale. Dès lors, en précisant que les personnes concernées continueront à agir « dans les limites des attributions légales de l'administration dont (elles) relève(nt) » le projet de loi sous examen est en contradiction avec la

1 Loi du 21 décembre 2006 portant 1. transposition – de la directive 2001/40/CE du Conseil du 28 mai 2001 relative à la reconnaissance mutuelle des décisions d'éloignement des ressortissants de pays tiers ; – de la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 ; – de la directive 2002/90/CE du Conseil du 28 novembre 2002 définissant l'aide à l'entrée, au transit et au séjour irréguliers ; – de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers ; 2. modification de la loi modifiée du 28 mars 1972 concernant 1. l'entrée et le séjour des étrangers ; 2. le contrôle médical des étrangers ; 3. l'emploi de la main-d'œuvre étrangère

disposition précitée du Statut général ». En conséquence, le Conseil d'État a exprimé une opposition formelle pour incohérence et insécurité juridique. En outre, il s'interroge sur la définition des « services compétents ».

Dans la lettre d'amendements gouvernementaux du 27 avril 2018, les auteurs confirment que « le projet de loi limite le traitement des données à une finalité de prévention et de répression du terrorisme et de la criminalité grave. Conformément à l'article 3, paragraphe 1er, de la loi du 5 juillet 2016 portant réorganisation du SRE, « *le SRE a pour mission de rechercher, d'analyser et de traiter, dans une perspective d'anticipation et de prévention, […] les renseignements relatifs à toute activité qui menace ou pourrait menacer la sécurité nationale […]* ». Le paragraphe 2 de l'article 3 de la loi précitée du 5 juillet 2016 précise qu'on « *entend par toute activité qui menace ou pourrait menacer la sécurité nationale […], toute activité […] qui peut avoir un rapport avec l'espionnage, l'ingérence, le terrorisme, l'extrémisme à propension violente, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, le crime organisé ou la cyber-menace dans la mesure où ces deux derniers sont liés aux activités précitées* ». Il est donc permis de conclure que les missions du SRE, et notamment ses missions de prévention en matière de lutte contre le terrorisme, l'espionnage, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes ou la cyber-menace dans la mesure où elle est liée aux activités précitées, correspondent parfaitement à la finalité définie par le projet de loi sous examen. Le SRE est partant justifié à traiter des données PNR. Le traitement de données PNR par un service de renseignement correspond d'ailleurs aux législations en place des pays européens dans la matière. Par exemple, l'article 14 de la loi belge du 25 décembre 2016 relative au traitement des données des passagers prévoit une UIP composée de la Sûreté de l'Etat visée par la loi organique du 30 novembre 1998 des services de renseignement et de sécurité et du Service général de Renseignement et de Sécurité visé par la loi organique du 30 novembre 1998 organique des services de renseignement et de sécurité. ».

Le Conseil d'État souligne aussi que les personnes détachées « ne sont plus en droit d'accéder aux données et informations traitées dans leur service d'origine sur base de leur première affectation, étant donné qu'en vertu de leur détachement ils n'en font plus partie », sauf à ajouter des dispositions spécifiques au texte de loi. Comprenant « l'utilité d'une disposition qui prévoit que les différents services compétents disposent d'un représentant en tant qu'« agent de liaison » au sein de l'UIP », le Conseil d'État propose notamment comme solution, s'inspirant de la loi belge de transposition de la directive PNR, de mettre en place une unité indépendante de la Police grand-ducale, à l'instar de la Cellule de renseignement financier auprès du parquet de Luxembourg.

La solution retenue par les auteurs des amendements se distingue du détachement en mentionnant que « si la version française de la Directive parle d'agents détachés, la version allemande utilise les termes « *abgeordnet werden* » et la version anglaise prévoit que « *staff members of a PIU may be seconded from competent authorities* » ». Les auteurs s'inspirent de l'article 9, paragraphe 3, de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat qui dispose que « *Les agents du centre peuvent être placés auprès d'un département ministériel ou d'une administration de l'Etat par une décision conjointe du ministre et du ministre du ressort. Dans ce cas, et pendant toute la durée de leur placement, ils continuent de relever de l'autorité hiérarchique du directeur du centre.* » Il ressort du commentaire des articles du projet de loi ayant abouti à la loi précitée du 20 avril 2009 que « *En ce qui concerne le personnel, la seule particularité pour le CTIE est la possibilité de placer certains de ses agents auprès des départements ministériels, administrations ou services de l'Etat sur base d'une décision conjointe des membres du Gouvernement respectifs. Cette mesure est destinée à permettre au CTIE d'envoyer des informaticiens auprès d'autres entités administratives afin de mettre en place et de gérer les systèmes informatiques d'une administration en particulier. Contrairement aux agents détachés, les agents placés par le CTIE continuent de relever de leur autorité hiérarchique d'origine. Ceci est nécessaire en raison du fait qu'ils doivent effectuer leur travail d'après les directives et les critères que le CTIE fixe pour l'ensemble du réseau informatique de l'Etat. (…) Le mécanisme du placement des agents est inspiré de la situation des contrôleurs financiers qui relèvent de l'autorité du Ministre ayant le budget dans ses attributions, mais qui exercent leurs missions auprès des différents départements ministériels*.[2]

Ainsi, le personnel de l'ADA et le personnel du SRE seront désignés à l'UIP comme membres de leurs administrations respectives et agiront comme tels. Cette solution ne remet pas en cause le principe

---

2 Projet de loi 5912

selon lequel l'UIP fonctionne sous forme de « closed box » et que les services désignés comme services compétents n'ont pas un accès direct aux données PNR. Le personnel de l'ADA et du SRE resteront placés sous l'autorité hiérarchique de leur administration d'origine. Pour permettre au responsable de l'UIP d'exercer les responsabilités qui lui incombent en vertu de la présente loi, il aura autorité fonctionnelle sur ce personnel. ».

Par ailleurs, quant à la critique du Conseil d'État que le texte ne donne aucune indication sur le grade ou la fonction du responsable de l'UIP, ni ne précise s'il doit s'agir d'un membre du personnel du cadre policier ou si un membre du cadre civil de la Police peut également remplir cette tâche de direction, le paragraphe 1er a été complété par un alinéa 2 précisant que le responsable de l'UIP est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

Le Conseil d'État relève que, « Dans leurs avis respectifs, tant la Cour supérieure de justice que les deux parquets d'arrondissement ont estimé que l'UIP devrait également comprendre, parmi son personnel, un magistrat détaché à cette fin ; les parquets se sont même demandés « s'il ne serait pas recommandable de faire présider cette unité » par un tel magistrat. Le Conseil d'État soulève que le détachement de magistrats au sein de cette unité y compris à sa direction, équivaudrait à un changement de statut de l'UIP, sans que ce changement contienne une plus-value évidente. Une telle possibilité ne serait par ailleurs envisageable que si l'UIP était mise en place en tant qu'unité indépendante des structures de la Police grand-ducale (…). ».

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

Articles 5 à 7

L'article 5, transposant l'article 8, paragraphe 1er de la directive, prévoit que les transporteurs aériens transfèrent à l'UIP les données PNR de tous les passagers en provenance ou à destination du Luxembourg ou transitant par le Luxembourg.

Le transfert des données se fait sans préjudice des obligations imposées par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, à savoir la transmission des informations préalables recueillies sur les passagers (Advanced Passenger Information (API) au Service de contrôle à l'aéroport. Dans son avis, le Conseil d'État rappelle que ces informations sont déjà actuellement recueillies pour les passagers provenant d'un État non membre de l'Union européenne. Il rend attentif à l'obligation, prévue par l'article 8, paragraphe 2 de la directive, pour les États « d'adopter les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent également ces données, par la « méthode push », à l'UIP ». Il réserve sa position quant à la dispense du second vote constitutionnel dans l'attente des renseignements « de nature à établir que ce transfert est effectué dans les conditions requises par le législateur européen ».

Par amendement gouvernemental du 27 avril 2018, l'article 7 a été complété par un paragraphe 3 tenant compte de la réserve exprimée par le Conseil d'État.

L'article 6 concerne les moments du transfert des données à l'UIP, prévues par l'article 8, paragraphe 3 de la directive.

Le texte initial a fait l'objet d'une opposition formelle en raison de l'ajout d'une « obligation supplémentaire à celles prévues par la directive, risquant ainsi en outre de créer une charge administrative supplémentaire pour les transporteurs qui utilisent l'aéroport de Luxembourg par rapport à ceux qui ont recours à des aéroports situés dans des pays n'imposant pas un même niveau d'obligations ».

Par amendement gouvernemental du 27 avril 2018, l'obligation supplémentaire a été supprimée.

L'article 7 précise les procédés techniques de transfert des données et transpose l'article 16 de la directive.

Dans son avis du 30 mars 2018, le Conseil d'État demande, sous peine d'opposition formelle, la suppression de la seconde phrase du paragraphe 1er, alinéa 1er au regard de l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne (TFUE), selon lequel « Les actes législatifs sont publiés dans le Journal officiel de l'Union européenne. Ils entrent en vigueur à la date qu'ils fixent ou, à défaut, le vingtième jour suivant leur publication. ». Le libellé de ladite phrase figurant à l'article 7 dans sa version initiale est le suivant : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg dès leur publication au Journal officiel de l'Union européenne. ».

Par amendement gouvernemental du 27 avril 2018, cette phrase est modifiée comme suit : « Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg ~~dès leur publication au Journal officiel de l'Union européenne~~conformément à l'article 297, paragraphe 1er, alinéa 3 du Traité sur le fonctionnement de l'Union européenne. ».

Dans son avis complémentaire, le Conseil d'État maintient son opposition formelle, constatant que l'amendement ne répond pas à l'opposition formelle, puisqu'« il n'appartient pas au législateur national de déterminer les modalités de l'applicabilité sur le territoire du Luxembourg des actes de l'Union ». Il indique que la suppression de la phrase concernée assurera la conformité du dispositif luxembourgeois avec le dispositif européen.

La commission a par conséquent suivi le Conseil d'État et supprimé la phrase.

Chapitre 4 – *Traitement des données PNR*

Articles 8 à 12

L'article 8 transpose l'article 13, paragraphe 4 de la directive qui interdit le traitement de données PNR qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance à un syndicat, l'état de santé, la vie sexuelle ou l'orientation sexuelle. Ces données doivent être effacées dès réception et de façon définitive.

L'article 9 impose à l'UIP d'effacer celles des données transférées qui ne sont pas énumérées à l'annexe I.

Le Conseil d'État note dans son avis « que, contrairement à l'article 8, l'article 9 ne figure pas à l'article 37 du projet de loi sous examen parmi les articles dont la violation peut entraîner une sanction pénale. Étant donné cependant que le défaut d'effacement visé à l'article 9 vise un comportement similaire au défaut d'effacement visé à l'article 8, alinéa 2, le Conseil d'État suggère d'inclure cette disposition également à l'article 37 même si le Conseil d'État admet qu'un défaut d'effacement de données légalement collectées et transférées, mais ne figurant pas à l'annexe I du projet, est un comportement qui n'atteint pas le même seuil de gravité qu'une violation de l'article 8, de telle sorte que la sanction devrait être adaptée à cette gravité moindre. En effet, s'il est vrai que l'article 14, paragraphe 1er, de la directive n'oblige pas expressément les États à incriminer le comportement en question, une disposition prévoyant une sanction n'y est cependant pas contraire et sera indiquée pour assurer une meilleure protection des données personnelles. ».

Les auteurs n'ont pas suivi le Conseil d'État, « étant donné que le défaut d'effacement des données sensibles a été retiré parmi les faits sanctionnables pénalement ».

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

L'article 10 a trait à l'utilisation des données PNR pour réaliser une évaluation des passagers avant leur arrivée ou leur départ dans le but « d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis ». Cette évaluation se fait par comparaison des données PNR avec les données à caractère personnel traitées par les services compétents ou auxquelles ils ont accès dans l'exercice de leurs missions ou avec des critères préétablis. Le paragraphe 2, alinéa 2 édicte des règles strictes pour ces critères. En vertu du paragraphe 3, « toute concordance positive obtenue » engendre un réexamen individuel. Le paragraphe 4 prévoit la transmission des données « au cas par cas, en vue d'un examen plus approfondi ».

Suivant l'article 11, les données PNR peuvent aussi être traitées pour mettre à jour les critères d'évaluation ou pour définir de nouveaux critères.

L'article 12 prévoit comme autre finalité de traitement des données PNR celle de répondre aux demandes des services compétents, « dûment motivées et fondées sur des motifs suffisants ». Le commentaire du document tel que déposé explique que ces données peuvent servir comme éléments de preuve dans le cadre d'enquêtes judiciaires ; ainsi, elles peuvent aider à orienter les enquêteurs sur le lieu de séjour d'une personne suspecte au moment où les faits ont été commis.

Chapitre 5 – *Services compétents*

Articles 13 à 15

L'article 13 énumère les services habilités à demander et à recevoir des données PNR ou le résultat du traitement de ces données et détermine la finalité de la transmission des données aux services concernés. Il reprend l'article 7, paragraphe 1er de la directive, tenant ainsi compte d'une opposition formelle du Conseil d'État et des critiques du Parquet général et de la Cour supérieure de Justice pour transposition incorrecte de la directive et manque de précision en ce qui concerne la finalité de la transmission des données aux services concernés.

Par ailleurs, l'alinéa 1er, point 2 a été complété suite à une opposition formelle du Conseil d'État exprimée à l'égard de l'article 39 ajouté au projet de loi par amendement gouvernemental du 27 février 2018 (cf. sous article 39).

Le second alinéa résulte des propositions du Conseil d'État et du Parquet général d'introduire dans le cadre juridique national, à l'instar de la loi belge ayant transposé la directive PNR, un accès simplifié des procureurs d'État « aux données PNR détenues par l'UIP en leur évitant d'avoir à saisir le juge d'instruction ne fût-ce que par le biais d'une procédure dite « mini-instruction », tout en sachant qu'en tant qu'acte d'enquête, la réquisition serait susceptible du recours inscrit à l'article 48-2 du Code de procédure pénale ».

L'article 14 limite le traitement des données PNR et du résultat du traitement aux finalités déterminées par l'article 1er, sans préjudice des compétences de la Police grand-ducale et de l'ADA, « lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement ». Il transpose l'article 7, paragraphes 4 et 5 de la directive.

L'article 15, transposant l'article 7, paragraphe 6 de la directive, prévoit que les services compétents ne peuvent prendre aucune décision ayant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR. Même si l'article 8 du projet de loi interdit le traitement des données sensibles y visées, l'interdiction de prendre des décisions qui seraient basées sur de telles données, si celles-ci avaient néanmoins été collectées, a été ajoutée suite à l'opposition formelle du Conseil d'État.

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

Articles 16 à 19

Les articles 16 et 17 transposent l'article 9, paragraphes 1 à 4 de la directive. Le commentaire du texte déposé souligne que ces deux articles représentent des éléments-clés du système PNR européen, comme une grande importance avait été attachée lors des négociations en trilogues à l'échange d'informations entre États membres. Alors que l'article 16 règle la transmission d'office d'informations aux UIP d'autres États membres, l'article 17 règle la transmission d'informations sur demande de l'UIP d'un autre État membre.

L'article 16 vise à préciser que, lorsque l'UIP luxembourgeoise reçoit des informations d'une UIP étrangère, elle les continue aux services nationaux compétents.

L'article 17 définit les conditions de la demande adressée à l'UIP luxembourgeoise. Le paragraphe 1er distingue entre les données qui n'ont pas encore été dépersonnalisées par masquage tel que prévu par l'article 26 et les données masquées. Suivant le paragraphe 2, sauf en cas d'urgence, les demandes et les échanges de données ont lieu par l'intermédiaire des UIP. Le paragraphe 3 permet, en cas de menace précise et réelle, de demander des données auprès d'un transporteur aérien en dehors des délais prévus à l'article 6, paragraphe 1er.

Par amendement gouvernemental du 27 avril 2018, l'article 17, paragraphe 1er a été complété par un alinéa 4. Suivant le commentaire de l'amendement, celui-ci « est à voir en relation avec la question, soulevée par le Parquet général à propos de l'article 21 réglant le transfert de données PNR à des États non membres de l'Union européenne, de savoir si cet échange échapperait aux dispositions traditionnelles de l'entraide judiciaire. Afin de dissiper toute incertitude à cet égard, une précision afférente a été apportée non seulement en ce qui concerne les échanges de données PNR avec des pays tiers, mais également l'échange de telles données avec d'autres États membres. ». Dans son avis complémentaire, le Conseil d'État a proposé une formulation plus précise qui a été reprise par la commission.

L'article 18 est relatif aux cas où les autorités luxembourgeoises adressent des demandes de données à l'UIP d'un autre État membre.

L'article 19 transpose l'article 9, paragraphe 5 de la directive qui concerne les modalités techniques d'échange des informations entre États membres.

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

Article 20

Cet article transpose l'article 10 de la directive, définissant les conditions d'accès aux données PNR par Europol.

Le Conseil d'État reconnaît à cette disposition une pure valeur déclaratoire, « étant donné que les compétences d'Europol ainsi que ses droits et obligations dans le cadre desdites compétences, font l'objet d'instruments européens et ne nécessitent pas de mesures de transposition particulières en droit national ».

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

Articles 21 à 24

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

Suite aux observations du Conseil d'État faites dans son avis, l'article 21 a été restructuré par amendement gouvernemental pour « clarifier le texte en ce qu'il énonce, parmi les conditions à respecter, celles prévues à l'article 35 [devenu l'article 34], paragraphe 1er, point d) de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, à savoir que la Commission européenne doit avoir adopté une décision d'adéquation ou, en l'absence d'une telle décision, que des garanties appropriées ont été prévues ou existent ou, en l'absence de décision d'adéquation et de garanties appropriées, que des dérogations pour des situations particulières s'appliquent. Afin de ne pas surcharger la présente loi avec des dispositions figurant déjà dans une autre loi, les auteurs des amendements ont préféré faire un renvoi à la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ».

L'article 22 transpose l'article 11, paragraphe 2 de la directive qui a trait au transfert de données PNR, obtenues d'un autre État membre, à un pays non membre de l'Union européenne.

L'article 23 transpose l'article 11, paragraphe 3 de la directive. Il prévoit une condition supplémentaire aux transferts de données vers des pays tiers. Suite aux interrogations du Conseil d'État, le texte a été amendé « de manière à n'ajouter comme condition supplémentaire par rapport aux conditions fixées aux articles 21 et 22 que celle d'avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données respecte les conditions et garanties de la présente loi ».

L'article 24 transpose l'article 11, paragraphe 4 de la directive, en vertu duquel « Chaque fois qu'un État membre transfère des données PNR en vertu du présent article, le délégué à la protection des données de l'UIP de cet État membre en est informé. ».

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

Articles 25 à 27

L'article 25 transpose l'article 12, paragraphes 1er et 4 de la directive et dispose que la durée maximale de conservation des données PNR est de cinq ans. Les données sont ensuite effacées de manière définitive, sauf celles qui ont été transférées à un service compétent et qui sont utilisées dans le cadre d'une enquête ou poursuite.

L'article 26 transpose l'article 12, paragraphe 2 de la directive qui impose l'obligation de dépersonnaliser par le masquage des éléments des données qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR. Le commentaire du texte déposé explique que « Le masquage est une technique qui consiste à rendre ces éléments de données invisibles, sans toutefois les altérer. Des recherches automatisées restent ainsi possibles parmi les données masquées et des hits

peuvent être générés. Toutefois les informations permettant d'identifier la personne à laquelle les données se rapportent ne sont pas affichées sur l'écran. Pour pouvoir visualiser ces informations, l'UIP doit obtenir l'accord du procureur [général] d'Etat ou de son délégué ou, si la requête émane du Service de Renseignement de l'Etat, l'accord de la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de Renseignement de l'Etat.

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

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

L'article 27 transpose l'article 12, paragraphe 5 de la directive et concerne la durée de conservation du résultat de l'évaluation réalisée sur base de l'article 10. Cette durée correspond au temps nécessaire pour informer les services compétents et, le cas échéant, les UIP, de l'existence d'une concordance positive. Au cas où le réexamen individuel manuel révèle un résultat du traitement automatisé négatif, celui-ci peut être archivé par l'UIP aussi longtemps que les données de base n'ont pas été effacées, ceci pour éviter de futures fausses concordances positives.

Chapitre 10 – *Protection des données à caractère personnel*

Articles 28 à 36

L'article 28 transpose l'article 13 de la directive.

Dans son avis, le Conseil d'État constate « que le projet sous avis, contrairement à l'article 13 de la directive, retient le principe de la compétence de la CNPD[3] ainsi que l'application du régime général sur la protection des données[4] aux données PNR collectées, pour ne mentionner la loi de transposition de la directive (UE) 2016/680 qu'en début de la disposition pour réserver les droits des autorités judiciaires. Il est dès lors en porte-à-faux avec le texte à transposer qui vise expressément la décision-cadre 2008/977/JAI, remplacée par la directive (UE) 2016/680, et ne retient l'application du régime de droit commun de la protection des données que pour le traitement des données à caractère personnel effectué par les transporteurs aériens[5], de telle sorte que le Conseil d'État doit s'opposer formellement au texte actuel, qui constitue une transposition incorrecte de la directive. ».

Par amendement gouvernemental du 27 avril 2018, le texte a été reformulé et se réfère à l'article 40 [devenu l'article 39] de la future loi portant transposition de la directive sur la protection des données en matière pénale. Le commentaire précise que « Dans la mesure où cette loi désigne la CNPD comme autorité compétente pour contrôler les traitements des données en matière pénale autres que ceux effectués par les juridictions de jugement, ce sera également la CNPD qui sera compétente pour contrôler le traitement des données PNR. Etant donné que les missions et les pouvoirs de cette commission sont définis par la loi portant sur le régime général, il est renvoyé à cette loi pour ce qui est des missions et des pouvoirs de la CNPD. ».

L'article 29 est relatif au délégué à la protection des données désigné par le responsable de l'UIP. Il transpose l'article 5 et l'article 6, paragraphe 6 de la directive. Sur demande du Conseil d'État, le paragraphe 4, alinéa 2 a été complété pour préciser la base légale permettant la saisine de la CNPD.

L'article 30 détermine les informations que l'UIP met à la disposition du public.

L'article 31 transpose l'article 13, paragraphe 1er de la directive. Il est consacré aux droits des personnes dont les données sont traitées, ces droits étant définis par référence aux articles pertinents du projet de loi 7168 portant transposition de la directive sur la protection des données pénales.

L'article 32 transpose l'article 6, paragraphe 8 de la directive qui oblige les UIP à stocker, traiter et analyser les données PNR exclusivement dans un ou des endroits sécurisés situés sur le territoire de l'État membre.

---

3 Commission nationale pour la protection des données

4 Projet de loi 7184

5 Directive (UE) 2016/681, article 13, paragraphe 3

Transposant l'article 13, paragraphes 2 et 7 de la directive, l'article 33 oblige le responsable de l'UIP de mettre en œuvre des mesures et des procédures techniques pour garantir un niveau élevé de sécurité des données.

En vertu de l'article 34 qui transpose l'article 13, paragraphe 5 de la directive, l'UIP doit conserver une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

L'article 35, transposant l'article 13, paragraphe 6 de la directive, a pour objet l'obligation pour l'UIP de tenir des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

L'article 36 transpose l'article 13, paragraphe 8 de la directive et prévoit l'information obligatoire, sans retard injustifié, de la personne concernée et de la CNPD, lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection de ces données ou d'affecter négativement la vie de la personne concernée.

Chapitre 11 – *Sanctions*

Articles 37 et 38

Ces articles transposent l'article 14 de la directive.

L'article 37, alinéa 1er punit, dans sa version initiale, la violation des articles 8, 15 et 36 de sanctions pénales. S'agissant de l'article 8, le Conseil d'État demande, afin d'assurer le respect du principe constitutionnel de la légalité de la peine, de préciser lequel des deux comportements visés à l'article 8 est sanctionné : le traitement illicite ou le défaut d'effacement des données concernées ou les deux. Il exige en outre de préciser s'il s'agit d'une infraction intentionnelle ou non, considérant « qu'un simple dysfonctionnement au sein de l'unité, dépourvu de toute intention criminelle, qui serait éventuellement sanctionnable du point de vue disciplinaire, n'est pas de nature à entraîner la responsabilité pénale, que ce soit du responsable de l'unité ou du fonctionnaire à l'origine du traitement en question ».

La question de l'intention de l'auteur du fait incriminé se pose également pour l'article 15.

Pour ce qui est de l'article 36, lequel oblige l'UIP à informer sans retard injustifié la personne concernée et l'autorité de contrôle d'une atteinte aux données à caractère personnel, le Conseil d'État met en doute « la faisabilité matérielle de l'information de la personne concernée qui, dans la grande majorité des cas, risque de ne pas résider sur le territoire national ».

Par conséquent, l'article 37 a fait l'objet d'un amendement gouvernemental tenant compte des avis du Conseil d'État et des autorités judiciaires. Le nouveau libellé précise que l'infraction consiste en une violation intentionnelle de l'interdiction de traiter des données sensibles, telle que prévue à l'article 8, alinéa 1er. Les auteurs de l'amendement indiquent ne pas avoir retenu la demande des Parquets de Luxembourg et de Diekirch de fixer un délai maximal pour l'effacement des données ; en effet, en fixant un délai pour ce faire, alors que la directive fait obligation d'effacer ces données immédiatement, il existe le risque que la Commission européenne considère que la législation luxembourgeoise ne serait sur ce point pas conforme à la directive.

Concernant l'article 15, l'article 37 amendé précise que la violation de la disposition, selon laquelle une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peut être prise sur la seule base du traitement automatisé de données PNR, doit être intentionnelle. Par ailleurs, a également été érigé en infraction pénale le fait de prendre une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative qui serait fondée sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

L'article 36 a été retiré de la liste des infractions pénales suite aux doutes du Conseil d'État au sujet de la faisabilité matérielle de l'information de la personne concernée.

Le Conseil d'État et les Parquets ont été suivis en faisant de la cessation du traitement illégal une obligation pour la juridiction de jugement.

Au sujet de l'article 49 [devenu l'article 47], paragraphe 2 [devenu le paragraphe 3] du projet de loi 7168, les auteurs de l'amendement font remarquer que cette disposition n'est pas applicable en matière de données PNR, puisque l'article 37 du projet de loi PNR ne renvoie dans son alinéa 2 qu'aux

paragraphes 1er, 3 à 5 [devenus les paragraphes 2 et 4 à 6] du projet de loi n° 7168. Les auteurs « ne partagent dès lors pas la crainte soulevée par le Conseil d'État par rapport à une éventuelle incohérence entre les dispositions pénales mises en place par les deux textes ».

L'article 38 punit d'une amende maximale de 50 000 € le transporteur aérien pour chaque vol pour lequel il n'a pas transmis les renseignements visés à l'article 3, ne les a pas transmis dans le délai prévu ou selon les modalités ou dans les formes prescrites.

Dans son avis du 30 mars 2018, le Conseil d'État « constate que le droit positif connaît déjà à l'heure actuelle une disposition qui règle une situation tout à fait analogue.

En effet, l'article 148 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration punit d'une amende d'un montant maximum de 5 000 euros les entreprises de transport aérien visées à l'article 108 de la même loi « à raison de chaque voyage pour lequel l'entreprise, par faute, n'a pas transmis les renseignements y visés ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis des renseignements incomplets ou erronés », amende qui est prononcée par le ministre ayant l'Immigration dans ses attributions. L'article 108, quant à lui, dispose en son paragraphe 1er qu'encourt les sanctions prévues aux articles 147 et 148 toute « entreprise de transport aérien qui (…) n'a pas transmis les renseignements visés à l'article 106 ou qui ne les a pas transmis dans le délai prévu, ou qui a transmis les renseignements incomplets ou erronés ». L'article 106, de son côté, prévoit en son paragraphe 1er qu'« afin de prévenir un refus d'entrée sur le territoire, les entreprises de transport aérien ont l'obligation de transmettre à la Police grand-ducale les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire du Grand-duché de Luxembourg en provenance d'un pays non-membre de l'Union européenne ».

S'il est vrai que la disposition sous examen vise la transmission de données relatives à des vols en provenance non pas d'États non membres de l'Union européenne, mais provenant d'États membres, que la communication doit se faire non pas à la Police grand-ducale mais à l'UIP, qui fait cependant partie de cette même police, et que le ministre sanctionnateur est un autre, les faits incriminés sont identiques sur tous les autres points, de telle sorte que le Conseil d'État s'interroge sur les raisons qui ont fait que le projet sous avis prévoit une amende dont le maximum est le décuple des sanctions prévues dans la disposition déjà existante, créant ainsi une inégalité de traitement selon l'origine du passager transporté, toutes autres choses étant égales par ailleurs.

Dans l'attente de recevoir des explications sur cette différence de traitement, le Conseil d'État est obligé de réserver sa position quant à la dispense du second vote. »

Les auteurs du projet de loi ont donné les explications demandées dans le contexte de l'amendement gouvernemental 26 du 27 avril 2018. Dans son avis complémentaire, le Conseil en prend acte et retire sa réserve.

Les auteurs rappellent que « La sanction à laquelle fait référence le Conseil d'État a été introduite par la loi du 21 décembre 2006 portant transposition, entre autres, de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (« directive API »). S'il est partant vrai que la loi de transposition de la directive API et le projet de loi de transposition de la directive PNR prévoient tous les deux des sanctions administratives à l'encontre des transporteurs aériens qui ne transfèrent pas les données ou ne les transfèrent pas selon les conditions requises, la différence fondamentale entre les deux textes, et qui d'après les auteurs du projet de loi PNR justifie la différence au niveau des sanctions encourues, réside dans la finalité pour laquelle les données des passagers sont recueillies. Ainsi, l'objectif de la directive API consiste, tel qu'il ressort de son article 1er, à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine. Les données API sont des informations biographiques extraites de la partie du passeport lisible par machine et servent d'outils de vérification des identités et de gestion aux frontières. Ces données ne présentent pas d'intérêt pour l'évaluation des personnes ni pour le dépistage des délinquants ou terroristes « inconnus ». En effet, « *une utilisation à la fois proactive et en temps réel des données PNR permet donc aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent, par rapport à ce que permet le traitement d'autres catégories de données à caractère personnel. Comme expliqué ci-dessous, le traitement de données à caractère personnel accessibles aux services répressifs dans le cadre d'instruments de l'UE actuels et futurs, tels que la directive relative aux informations préalables sur les passagers, le système d'information Schengen (SIS) et le système d'information Schengen de deuxième génération (SIS II), ne donne pas aux services répressifs la possibilité d'identifier des suspects « inconnus » comme le permet l'analyse*

de données PNR. Deuxièmement, après la commission d'une infraction, les données PNR aident les services répressifs à prévenir et à détecter d'autres infractions graves, dont des actes de terrorisme, et à enquêter sur celles-ci et à poursuivre leurs auteurs. À cet effet, les services répressifs doivent utiliser les données PNR en temps réel, pour les confronter à diverses bases de données de personnes « connues » et d'objets recherchés. Ils doivent également en faire un usage réactif, pour rassembler des preuves et, au besoin, trouver d'éventuels complices et démanteler des réseaux criminels. »[6]

Les données PNR sont recueillies pour une finalité complètement différente, à savoir qu'ils constituent un moyen de prévention et de lutte contre le terrorisme et les formes graves de criminalité telles que la traite des êtres humains, l'exploitation sexuelle des enfants, le trafic d'armes, le vol organisé ou l'aide à l'entrée et le séjour irréguliers. Cette dernière infraction illustre d'ailleurs très bien la différence entre les finalités des traitements des données API et des données PNR. Ainsi, si la directive API vise à prévenir l'immigration illégale, qui ne constitue pas une infraction pénale, la directive PNR crée des moyens destinés à protéger la sécurité et la vie des personnes. Il n'y a aucun doute que les conséquences d'un défaut de transmission de données à des fins de contrôle des frontières ne sont pas les mêmes qu'un défaut de transmission de données qui peuvent permettre de prévenir une attaque terroriste ou un autre crime grave. La différence entre les sanctions encourues dans les deux cas de figure est dès lors justifiée.

Il importe par ailleurs de relever que l'article 14 de la directive PNR oblige les États membres à prévoir des sanctions effectives, proportionnées et dissuasives à l'encontre des transporteurs aériens qui ne transmettent pas les données comme le prévoit l'article 8 ou ne les transmettent pas dans le format requis. Comme il a été expliqué dans le commentaire de l'article 38, les auteurs du texte se sont alignés sur les montant[s] des amendes fixées dans d'autres États membres, notamment la France, la Belgique et l'Allemagne. Il est à craindre que si le Luxembourg alignait la sanction encourue par le transporteur aérien qui omet de transférer les données PNR sur la sanction prévue par la loi précitée de 2008 sur l'immigration, la Commission européenne risquerait de considérer la sanction prévue dans le présent projet de loi comme ne remplissant pas les exigences posées par l'article 14 de la Directive. ».

Chapitre 12 – *Dispositions modificatives*

Articles 39 et 40

Ce chapitre a été ajouté par amendement gouvernemental du 27 février 2018.

L'article 39 a fait l'objet de deux oppositions formelles du Conseil d'État. La première concerne l'ajout d'un paragraphe 4 à l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État. Le Conseil d'État rappelle que l'article 5 de cette loi « énumère les moyens et mesures de recherche dont dispose le SRE et qui, pour leur mise en œuvre, nécessitent une autorisation écrite du directeur du service, suite à une demande motivée et écrite de l'agent du SRE chargé du dossier. La nouvelle disposition ajoute à ces moyens et mesures de recherche la possibilité pour le SRE de demander à l'UIP la communication des données PNR dans le cadre de ses activités.

L'amendement 2 est à lire avec l'amendement 3, qui tend à supprimer le point a) de l'article 8 de la loi précitée du 5 juillet 2016, prévoyant que le SRE peut être autorisé par le Comité ministériel du renseignement, instauré par le paragraphe 2 de l'article 2 de ladite loi, de « solliciter (…) les données des dossiers passagers relatives à une ou plusieurs personnes identifiées ou identifiables au sujet desquels le SRE dispose d'un ou de plusieurs indices concordants relatifs à une menace actuelle ou potentielle visant la sécurité nationale ou les intérêts visés à l'article 3. Le transporteur de personnes par voie aérienne visé par la demande doit fournir sa réponse sans délai. ». Cette mesure ne peut cependant être autorisée par ledit comité, au vœu du paragraphe 1er de l'article 8, que « si les moyens et les mesures de recherche dont dispose le SRE en vertu des articles 5, 6, et 7 (de la loi précitée) s'avèrent inopérants en raison de la nature des faits et des circonstances spécifiques de l'espèce ».

Il résulte de la combinaison de ces deux amendements que la mesure de l'article 8, permettant au SRE de contacter directement les opérateurs de transports aériens, sera remplacée par la possibilité pour ledit service de demander des renseignements à l'UIP et ne pourra plus être utilisée en conséquence.

---

6 Proposition de Directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (COM/2011/0032 final)

Cet amendement pose cependant problème en ce que, en limitant les finalités de l'accès du SRE aux données de l'UIP, il reste en deçà de l'article 13 du projet de loi sous examen et en réduit par conséquent la portée, entraînant ainsi une transposition incorrecte de la directive, à laquelle le Conseil d'État doit s'opposer formellement. ».

Les auteurs de l'amendement ont par conséquent suivi le Conseil d'État en complétant l'article 13 par une référence à l'article 5, paragraphe 4, de la loi précitée du 5 juillet 2016.

La seconde opposition formelle se rapporte à l'alinéa 2 du paragraphe 4 nouveau ajouté par l'amendement 2 ci-dessus à l'article 5 de la loi précitée du 5 juillet 2016. Pour le Conseil d'État, le fait de prévoir « que le directeur du SRE « rapporte tous les six mois par écrit » au prédit comité « la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquelles l'exercice des missions a exigé la demande de communication » n'est pas de nature à garantir suffisamment les droits des personnes concernées, cela d'autant plus que la procédure invoquée par les auteurs de l'amendement et prévue à l'article 5, paragraphe 3, de la loi précitée du 5 juillet 2016, qui a trait aux observations dans les lieux publics ainsi qu'aux inspections de lieux publics, prévoit un rapport par écrit au comité une fois par mois, et non pas une fois chaque semestre.

Il s'oppose par conséquent formellement à l'amendement sous avis pour contravention à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 11, paragraphe 3, de la Constitution pour autant qu'il réduit la fréquence du prédit rapport à un rapport semestriel, ce qui est totalement insuffisant pour garantir les droits des personnes concernées. ».

En conséquence, l'alinéa 2 du paragraphe 4 nouveau ajouté à l'article 5 de la loi précitée du 5 juillet 2016 a été amendé de manière à prévoir un rapport mensuel.

Chapitre 13 – *Disposition finale*

Article 41

Sans observation.

Annexes I et II

Sans observation.

*

Compte tenu des observations qui précèdent, la Commission de la Force publique propose en sa majorité à la Chambre des Députés d'adopter le projet de loi dans la teneur suivante :

*

7151

PROJET DE LOI

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

Chapitre 1er – *Dispositions générales*

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

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

1° « transporteur aérien » : toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes ;

2° « passager » : toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers ;

3° « dossier passager » : le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités ;

4° « système de réservation » : le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations ;

5° « système de contrôle des départs » : le système utilisé pour contrôler les passagers lors de l'embarquement ;

6° « données PNR » : les données contenues dans le dossier passager et énumérées à l'annexe I ;

7° « méthode push » : la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'informations passagers telle que créée à l'article 3 ;

8° « infractions terroristes » : les infractions visées au Livre II, Titre 1ier, Chapitre III-1 du Code pénal ;

9° « formes graves de criminalité » : les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans ;

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

11° « services compétents » : les services visés à l'article 13.

Chapitre 2 – *Unité d'informations passagers*

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

1° de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données ;

2° du transfert de ces données et des résultats de leur traitement aux services compétents ;

3° de l'échange de ces données et des résultats de leur traitement avec les unités d'informations passagers des autres Etats membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4. (1) Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Il est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

(2) Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel de l'Administration des douanes et accises et du Service de renseignement de l'Etat. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Les membres du personnel de l'Administration des douanes et accises et du Service de renseignement de l'Etat sont désignés à l'UIP par une décision conjointe du ministre ayant la Police grand-ducale dans ses attributions et du ministre du ressort. Ils continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

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

Art. 5. Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la méthode push, les données PNR de tous les passagers en provenance de, à destination de ou transitant par le Luxembourg pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien.

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

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

1° 48 heures avant l'heure de départ programmée du vol ;

2° immédiatement après la clôture du vol, c'est-à-dire dès que les passagers ont embarqué à bord de l'aéronef prêt à partir et qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point 2°, peut se limiter à une mise à jour du transfert visé à l'alinéa 1er, point 1°.

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

Art. 7. (1) Les données PNR sont transférées à l'UIP par voie électronique au moyen de protocoles communs et de formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

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

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

(3) Dans l'hypothèse où un transporteur aérien ne conserve pas les données API énumérées à l'annexe I, point 18, par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, il transfère également ces données par la méthode « push » à l'UIP. Dans le cas d'un tel transfert, toutes les dispositions de la présente loi s'appliquent à ces données API.

Chapitre 4 – *Traitement des données PNR*

Art. 8. Le traitement de données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle est interdit.

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

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

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

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

1° aux traitements de données à caractère personnel mis en œuvre par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;

2° à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

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

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

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

(6) Lorsque les évaluations sont réalisées pour des vols entre le Grand-Duché de Luxembourg et un autre Etat membre de l'Union européenne auquel s'applique le règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), les conséquences de ces évaluations doivent respecter ledit règlement.

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

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

Chapitre 5 – *Services compétents*

Art. 13. Sont habilités à demander à l'UIP ou à recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, en vue de procéder à un examen approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et poursuites en la matière :

1° la Police grand-ducale ;

2° le Service de renseignement de l'Etat conformément à l'article 5, paragraphe 4, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat ;

3° l'Administration des douanes et accises.

En recherchant les crimes et délits visés à l'article 2, points 8° et 9°, le procureur d'Etat peut, par une décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 12.

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

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

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

Les décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peuvent pas être fondées sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

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

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

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

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

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

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

Les dispositions du présent paragraphe ne portent pas atteinte aux dispositions tant internationales que nationales sur l'entraide judiciaire internationale en matière pénale.

(2) Dans des cas d'urgence, les autorités compétentes des autres Etats membres, désignées conformément à l'article 7, paragraphe 1er , de la directive (UE) 2016/661 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe 1er sont applicables.

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

Art. 18. L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres Etats membres de l'Union européenne des données PNR ou les résultats du traitement de ces données.

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

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

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

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

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

1° lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des Etats membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes dans la matière et ;

2° dans la mesure où ladite infraction relève de la compétence d'Europol.

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

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

Art. 21. L'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si :

1° l'une des conditions prévues à l'article 34, paragraphe 1er, point d) de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est remplie ;

2° l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité ;

3° le transfert est nécessaire aux fins telles que définies à l'article 1er ;

4° le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er ;

5° les conditions prévues à l'article 17, paragraphe 1er sont remplies.

Les dispositions du présent article ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

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

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

1° ces transferts sont essentiels pour répondre à une menace précise et réelle liée à une infraction terroriste ou à une forme grave de criminalité dans un Etat membre de l'Union européenne ou un pays tiers ;

2° l'accord préalable n'a pas pu être obtenu en temps utile.

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

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

Art. 24. Le délégué à la protection des données visé à l'article 29 est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

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

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

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

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

1° le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR ;

2° l'adresse et les coordonnées ;

3° des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne ;

4° les informations « grands voyageurs » ;

5° les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte ;

6° toute donnée API qui a été recueillie.

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

1° elle est nécessaire aux fins visées à l'article 12 ;

2° elle a été approuvée par le procureur général d'Etat ou son délégué ou, si les données sont destinées à être communiquées au Service de renseignement de l'Etat, par la commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

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

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

Chapitre 10 – *Protection des données à caractère personnel*

Art. 28. L'autorité de contrôle visée à l'article 39 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 8 de la loi du jj/mm/aaaa portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et elle dispose, à cette fin, des pouvoirs prévus à l'article 14 de la même loi.

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

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

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

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

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

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

Il fait directement rapport au responsable de l'UIP.

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

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

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données conformément à la loi du jj/mm/aaaa portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

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

1° ses coordonnées ;

2° les coordonnées du délégué à la protection des données ;

3° les finalités du traitement auquel sont destinées les données PNR ;

4° le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité ;

5° l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31. (1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 13 à 17 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 44 à 46 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

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

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

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en œuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 28, paragraphe 2 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

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

Cette documentation comprend :

1° le nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès ;

2° les demandes formulées par les services compétents et les UIP des autres Etats membres de l'Union européenne ;

3° toutes les demandes et tous les transferts de données PNR vers un pays tiers.

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

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

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

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

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

Les registres sont conservés pendant cinq ans.

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

Chapitre 11 – *Sanctions*

Art. 37. La violation intentionnelle de l'article 8, alinéa 1er et de l'article 15 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125 000 euros ou d'une de ces peines seulement. La juridiction saisie prononce la cessation du traitement contraire aux dispositions de l'article 8, alinéa 1er et de l'article 15 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 47, paragraphes 1er, 2, 4, 5 et 6 de la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38. (1) Est puni d'une amende d'un montant maximum de 50 000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements visés à l'article 3, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

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

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

L'amende est prononcée par le ministre ayant la Police grand-ducale dans ses attributions.

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

Chapitre 12 – *Dispositions modificatives*

Art. 39. Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

« (4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, ou de cyber-menace dans la mesure où celle-ci est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12, de la loi du jj/mm/aaaa relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Le directeur du SRE rapporte tous les mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en œuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Art. 40. À l'article 8, paragraphe 1er de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, la lettre a) est supprimée.

Chapitre 13 – *Disposition finale*

Art. 41. La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « Loi du jj/mm/aaaa relative au traitement des données des dossiers passagers ».

*

ANNEXE I

Liste des données PNR

1° Code repère du dossier passager ;

2° Date de réservation/d'émission du billet ;

3° Date(s) prévue(s) du voyage ;

4° Nom(s) ;

5° Adresse et coordonnées (numéro de téléphone, adresse électronique) ;

6° Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation ;

7° Itinéraire complet pour le PNR concerné ;

8° Informations « grands voyageurs » ;

9° Agence de voyages/agent de voyages ;

10° Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation ;

11° Indications concernant la scission/division du PNR ;

12° Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée) ;

13° Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix ;

14° Numéro du siège et autres informations concernant le siège ;

15° Informations sur le partage de code ;

16° Toutes les informations relatives aux bagages ;

17° Nombre et autres noms de voyageurs figurant dans le PNR ;

18° Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée) ;

19° Historique complet des modifications des données PNR énumérées aux points 1 à 18.

*

ANNEXE II

Liste des infractions visées à l'article 2, point 9

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

Luxembourg, le 19 juillet 2018

La Présidente-Rapportrice,
Claudia DALL'AGNOL

Impression: CTIE – Division Imprimés et Fournitures de bureau