Session ordinaire 2017-2018

MW/PR P.V. FRP 05

Commission de la Force publique

Procès-verbal de la réunion du 4 mai 2018

Ordre du jour :

1. Approbation du projet de procès-verbal de la réunion du 22 février 2018

2. 7151 Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

   - Désignation d'un rapporteur
   - Présentation du projet de loi
   - Examen de l'avis du Conseil d'État
   - Présentation des amendements gouvernementaux

*

Présents : M. Marc Angel, M. Alex Bodry, Mme Claudia Dall'Agnol, M. Gusty Graas, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Henri Kox, M. Alexander Krieps, M. Claude Lamberty (en rempl. de M. Max Hahn)

M. Etienne Schneider, Ministre de la Sécurité intérieure

M. Fränk Reimen, Direction, Mme Martine Schmit, du Ministère de la Sécurité intérieure

Police grand-ducale :

M. Alain Engelhardt, Premier Commissaire divisionnaire, M. Florent Goniva, Chef du Service des relations internationales

M. Bob Gengler, du Ministère de la Fonction publique et de la Réforme administrative

Mme Doris Woltz, Directrice du Service de renseignement de l'État du Luxembourg (SREL)

M. Jean-Paul Bever, de l'Administration parlementaire

*

Présidence : Mme Claudia Dall'Agnol, Présidente de la Commission

*

1. Approbation d'un projet de procès-verbal

Le projet de procès-verbal ne donne pas lieu à observation et est approuvé.

2. Projet de loi 7151

La commission désigne sa présidente, Mme Claudia Dall'Agnol, comme rapportrice du projet de loi.

En guise d'introduction, Monsieur le Ministre rappelle le rôle du Luxembourg dans la finalisation de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière. En effet, la présidence luxembourgeoise du Conseil de l'Union européenne a réussi, malgré le contexte difficile des attaques terroristes en Europe, à négocier un texte de compromis approuvé par le Conseil JAI[1] le 4 décembre 2015 et par le Parlement européen le 14 avril 2016.

Le délai de transposition de la directive est le 25 mai 2018. Le projet de loi ayant pour objet la transposition de la directive a été déposé le 19 juin 2017 et a fait l'objet d'un avis du Conseil d'État le 30 mars 2018. Une série d'amendements gouvernementaux a été adoptée par le gouvernement en conseil en date du 27 avril 2018.

Les auteurs font une présentation succincte du projet de loi, dont la structure est la suivante :

- Le chapitre 1er contient des dispositions générales, dont l'objet de la loi défini à l'article 1er : sont visés les transporteurs aériens, lesquels doivent transférer les données des dossiers passagers pour le traitement de celles-ci à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité, ces dernières étant énumérées à l'annexe II.
L'article 2 définit les différentes notions. Par amendement gouvernemental du 27 avril 2018, le point 7, en l'absence d'une définition de l'Unité d'informations passagers (UIP), a été complété par la référence à l'article 3 créant l'UIP, tel que suggéré par le Conseil d'État dans son avis du 30 mars 2018. Par ailleurs, un point 11 nouveau a été ajouté pour la notion de « services compétents », demande formulée par le Conseil d'État notamment à l'endroit de l'article 10, paragraphe 1er.

- Le chapitre 2 a trait à l'Unité d'informations passagers. L'article 3 met en place au sein de la Police grand-ducale l'UIP chargée de la collecte, du transfert et de l'échange des données et des résultats de leur traitement, tel que prévu par la future loi. L'UIP sera intégrée dans la direction « relations internationales » rattachée au comité de direction de la Police grand-ducale.

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

Le Conseil d'État pose la question du statut et des compétences du personnel détaché en rappelant que, suivant l'article 7 du Statut général des fonctionnaires de l'État, le détachement consiste en « l'assignation au fonctionnaire d'un autre emploi correspondant à sa catégorie et à son grade dans une autre administration, dans un établissement public ou

[1] Justice et Affaires intérieures

auprès d'un organisme international », qui a comme conséquence que « le fonctionnaire relève de l'autorité hiérarchique de l'administration, respectivement de l'établissement ou de l'organisme auquel il est détaché ». Par conséquent, les fonctionnaires détachés de l'ADA et du SRE « relèveront entièrement de la Police grand-ducale. Dès lors, en précisant que les personnes concernées continueront à agir « dans les limites des attributions légales de l'administration dont (elles) relève(nt) » le projet de loi sous examen est en contradiction avec la disposition précitée du Statut général ». En conséquence, le Conseil d'État a exprimé une opposition formelle pour incohérence et insécurité juridique. En outre, il s'interroge sur la définition des « services compétents ».

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

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

La solution retenue par les auteurs des amendements se distingue du détachement en mentionnant que « si la version française de la Directive parle d'agents détachés, la version allemande utilise les termes *« abgeordnet werden »* et la version anglaise prévoit que *« staff members of a PIU may be seconded from competent authorities » »*. Les auteurs s'inspirent de l'article 9, paragraphe 3, de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat qui dispose que *« Les agents du centre peuvent être placés auprès d'un département ministériel ou d'une administration de l'Etat par une décision conjointe du ministre et du ministre du ressort. Dans ce cas, et pendant toute la durée de leur placement, ils continuent de relever de l'autorité hiérarchique du directeur du centre. »* Il ressort du commentaire des articles du projet de loi ayant abouti à la loi précitée du 20 avril

2009 que « *En ce qui concerne le personnel, la seule particularité pour le CTIE est la possibilité de placer certains de ses agents auprès des départements ministériels, administrations ou services de l'Etat sur base d'une décision conjointe des membres du Gouvernement respectifs. Cette mesure est destinée à permettre au CTIE d'envoyer des informaticiens auprès d'autres entités administratives afin de mettre en place et de gérer les systèmes informatiques d'une administration en particulier. Contrairement aux agents détachés, les agents placés par le CTIE continuent de relever de leur autorité hiérarchique d'origine. Ceci est nécessaire en raison du fait qu'ils doivent effectuer leur travail d'après les directives et les critères que le CTIE fixe pour l'ensemble du réseau informatique de l'Etat. (…) Le mécanisme du placement des agents est inspiré de la situation des contrôleurs financiers qui relèvent de l'autorité du Ministre ayant le budget dans ses attributions, mais qui exercent leurs missions auprès des différents départements ministériels.*[2]

Ainsi, le personnel de l'ADA et le personnel du SRE seront désignés à l'UIP comme membres de leurs administrations respectives et agiront comme tels. Cette solution ne remet pas en cause le principe selon lequel l'UIP fonctionne sous forme de « closed box » et que les services désignés comme services compétents n'ont pas un accès direct aux données PNR. Le personnel de l'ADA et du SRE resteront placés sous l'autorité hiérarchique de leur administration d'origine. Pour permettre au responsable de l'UIP d'exercer les responsabilités qui lui incombent en vertu de la présente loi, il aura autorité fonctionnelle sur ce personnel. ».

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

- Le chapitre 3 est relatif au transfert des données par les transporteurs aériens.

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

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

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

Le texte initial a fait l'objet d'une opposition formelle en raison de l'ajout d'une « obligation supplémentaire à celles prévues par la directive, risquant ainsi en outre de créer une charge administrative supplémentaire pour les transporteurs qui utilisent l'aéroport de Luxembourg

[2] Projet de loi 5912

par rapport à ceux qui ont recours à des aéroports situés dans des pays n'imposant pas un même niveau d'obligations ».

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

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

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

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

- Le chapitre 4 concerne le traitement des données PNR.

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

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

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

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

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

- Le chapitre 5 est consacré aux services compétents.

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

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

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

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

- Le chapitre 6 traite de l'échange d'informations entre les États membres de l'Union européenne.

L'article 16 règle la transmission d'office d'informations aux UIP d'autres États membres.

L'article 17 règle la transmission d'informations sur demande de l'UIP d'un autre État membre. Il définit les conditions de la demande adressée à l'UIP luxembourgeoise. Le paragraphe 1er distingue entre les données qui n'ont pas encore été dépersonnalisées par masquage tel que prévu par l'article 26 et les données masquées. Par amendement gouvernemental du 27 avril 2018, le paragraphe 1er a été complété par un alinéa 4. Suivant le commentaire de l'amendement, celui-ci « est à voir en relation avec la question, soulevée par le Parquet général à propos de l'article 21 réglant le transfert de données PNR à des États non membres de l'Union européenne, de savoir si cet échange échapperait aux dispositions traditionnelles de l'entraide judiciaire. Afin de dissiper toute incertitude à cet égard, une précision afférente a été apportée non seulement en ce qui concerne les échanges de données PNR avec des pays tiers, mais également l'échange de telles données avec d'autres États membres. ».[3]

Suivant le paragraphe 2, sauf en cas d'urgence, les demandes et les échanges de données ont lieu par l'intermédiaire des UIP. Le paragraphe 3 permet, en cas de menace précise et

[3] Dans son avis complémentaire du 26 juin 2018, le Conseil d'État a proposé une formulation plus précise qui a été reprise par la commission.

réelle, de demander des données auprès d'un transporteur aérien en dehors des délais prévus à l'article 6, paragraphe 1er.

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

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

- Le chapitre 7 est relatif aux conditions d'accès aux données PNR par Europol.

L'article 20 transpose l'article 10 de la directive, définissant les conditions d'accès aux données PNR par Europol.

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

- Le chapitre 8 règle le transfert de données vers des pays non membres de l'Union européenne.

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

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

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

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

- Le chapitre 9 a pour objet la durée de conservation et la dépersonnalisation des données.

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

L'article 26 transpose l'article 12, paragraphe 2 de la directive qui impose l'obligation de dépersonnaliser par le masquage des éléments des données qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR. Le commentaire du texte déposé explique que « Le masquage est une technique qui consiste à rendre ces éléments de données invisibles, sans toutefois les altérer. Des recherches automatisées restent ainsi possibles parmi les données masquées et des hits peuvent être générés. Toutefois les informations permettant d'identifier la personne à laquelle les données se rapportent ne sont pas affichées sur l'écran. Pour pouvoir visualiser ces informations, l'UIP doit obtenir l'accord

du procureur [général] d'Etat ou de son délégué ou, si la requête émane du Service de Renseignement de l'Etat, l'accord de la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de Renseignement de l'Etat. ».

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

Un député fait observer que le défaut de date dans le renvoi à d'autres lois est problématique en raison du manque de précision.

- Le chapitre 10 concerne la protection des données à caractère personnel.

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

Dans son avis, le Conseil d'État constate « que le projet sous avis, contrairement à l'article 13 de la directive, retient le principe de la compétence de la CNPD[4] ainsi que l'application du régime général sur la protection des données[5] aux données PNR collectées, pour ne mentionner la loi de transposition de la directive (UE) 2016/680 qu'en début de la disposition pour réserver les droits des autorités judiciaires. Il est dès lors en porte-à-faux avec le texte à transposer qui vise expressément la décision-cadre 2008/977/JAI, remplacée par la directive (UE) 2016/680, et ne retient l'application du régime de droit commun de la protection des données que pour le traitement des données à caractère personnel effectué par les transporteurs aériens[6], de telle sorte que le Conseil d'État doit s'opposer formellement au texte actuel, qui constitue une transposition incorrecte de la directive. ».

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

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

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

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

[4] Commission nationale pour la protection des données
[5] Projet de loi 7184
[6] Directive (UE) 2016/681, article 13, paragraphe 3

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

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

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

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

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

- Le chapitre 11 est relatif aux sanctions.

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

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

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

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

Concernant l'article 15, l'article 37 amendé précise que la violation de la disposition, selon laquelle une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peut être prise sur la seule base du traitement automatisé de données PNR, doit être intentionnelle. Par ailleurs, a également été érigé en

infraction pénale le fait de prendre une décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative qui serait fondée sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

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

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

Au sujet de l'article 49 [devenu l'article 47], paragraphe 2 du projet de loi 7168, les auteurs de l'amendement font remarquer que cette disposition n'est pas applicable en matière de données PNR, puisque l'article 37 du projet de loi PNR ne renvoie dans son alinéa 2 qu'aux paragraphes 1er, 3 et 5 du projet de loi n° 7168. Les auteurs « ne partagent dès lors pas la crainte soulevée par le Conseil d'État par rapport à une éventuelle incohérence entre les dispositions pénales mises en place par les deux textes ».

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

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

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

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

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

Les auteurs du projet de loi donnent les explications demandées dans le contexte de l'amendement gouvernemental 26 du 27 avril 2018.

- Le chapitre 12 a trait aux dispositions modificatives.

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

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

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

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

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

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

Il s'oppose par conséquent formellement à l'amendement sous avis pour contravention à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 11, paragraphe 3, de la Constitution pour autant qu'il réduit la

fréquence du prédit rapport à un rapport semestriel, ce qui est totalement insuffisant pour garantir les droits des personnes concernées. ».

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

*

À l'aide d'une présentation PowerPoint, le Responsable du Service des relations internationales de la Police grand-ducale donne un aperçu de la mise en pratique de la directive.

L'UIP fait partie de la direction « relations internationales », puisque celle-ci est en charge de l'échange d'informations avec les autres États, que ce soit par le système d'information Schengen (SIS) et précisément le bureau SIRENE (Supplementary Information Request at the National Entries), Interpol ou Europol, et en raison de l'expérience de celle-ci avec le système API (Advanced Passenger Information).

Les interlocuteurs de l'UIP sont le SREL, l'ADA et les services policiers compétents, à savoir le Service de Police judiciaire (SPJ), les actuels services de recherche et d'enquête criminelle (SREC), l'Unité Centrale de la Police de l'Aéroport (UCPA), les bureaux policiers internes SIRENE, Europol et Interpol, de même que les autorités judiciaires.

Les missions de l'UIP consistent en la collecte des données, leur traitement et analyse et leur échange.

Suite à la collecte des données suivant les modalités et dans les formes prévues par la directive, le travail policier proprement dit commence, c'est-à-dire le traitement et l'analyse des données.

Le traitement et l'analyse revêtent deux aspects : d'une part, il est procédé à des contrôles automatisés en temps réel. Ces contrôles se font en trois étapes : 1) le criblage consiste à vérifier si les personnes qui se trouvent sur les listes des passagers ne sont pas des personnes recherchées dans le SIS par le biais du réseau Interpol. 2) Le ciblage personnalisé, connu sous le nom de « Watchlist », concerne des personnes spécialement surveillées par les enquêteurs, lesquels sont informés au moyen de la « Watchlist » de l'arrivée et du départ de ces personnes. 3) Le ciblage de précision (rules based targeting, Musterfahndung) permet de cibler des personnes en fonction de critères déterminés. Chaque personne qui correspond à ces critères est signalée par le système. Contrairement au criblage et au ciblage personnalisé, lesquels visent des personnes ou objets recherchés connus, le ciblage de précision a pour objet de détecter des personnes suspectes inconnues.

D'autre part, des requêtes sont effectuées dans le passé. Il s'agit de vérifications dans le cadre d'une enquête et de vérifications pour l'UIP des autres pays.

Pour ce qui est du trafic aérien, 3,6 millions passagers sont passés par le Luxembourg en 2017 qui se répartissent sur différentes compagnies aériennes comme suit : Luxair 51%, Ryanair 10%, Lufthansa 8%, Easyjet 7%, KLM 5%, autres 19%.

Depuis 2006, un autre système est en vigueur au Luxembourg en matière de données relatives aux passagers, à savoir le système API (Advanced Passenger Information). La directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (directive API) a été transposée au Luxembourg par la loi du 21 décembre 2006 portant 1. transposition – de la

directive 2001/40/CE du Conseil du 28 mai 2001 relative à la reconnaissance mutuelle des décisions d'éloignement des ressortissants de pays tiers ; – de la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 ; – de la directive 2002/90/CE du Conseil du 28 novembre 2002 définissant l'aide à l'entrée, au transit et au séjour irréguliers ; – de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers ; 2. modification de la loi modifiée du 28 mars 1972 concernant 1. l'entrée et le séjour des étrangers ; 2. le contrôle médical des étrangers ; 3. l'emploi de la main-d'oeuvre étrangère. Le dispositif API se limite aux vols extra-Schengen et impose la transmission préalable, précisément au moment du départ (ATD – at time departure), à la Police des listes de passagers des vols en provenance d'un pays non membre de l'Union européenne. Les données recueillies lors de l'enregistrement (check-in) sont les éléments d'identification de base d'une personne, à savoir nom, le prénom, la date de naissance, le numéro du passeport et la nationalité.

La directive PNR résulte d'un compromis entre les États membres et d'une déclaration commune des ministres du Conseil Justice et Affaires intérieures (JAI) du 4 décembre 2015. Elle étend le contenu de la directive API en prévoyant l'obligation de transmission des listes de passagers également pour les vols intra-Schengen et de transit. Dix-neuf champs de données PNR sont prévus. Les données sont transmises 48 heures avant l'heure de départ programmée du vol et immédiatement après la clôture du vol et elles sont consolidées dans le dossier des données Passager et traitées par l'UIP. Les données sont conservées pendant cinq ans. Elles restent visibles pendant six mois à compter de leur transfert par les compagnies aériennes et sont ensuite masquées. Si la Police a besoin pendant cette période de telles données, l'UIP doit obtenir l'accord du procureur général d'Etat ou de son délégué pour visualiser les informations masquées. Il convient de préciser que les données PNR ne sont pas spécialement recueillies pour les besoins de la Police, mais elles seront désormais transférées à celle-ci.

Concrètement, la mise en œuvre de la transposition de la directive PNR nécessitera onze semaines pour atteindre une collecte de 99% des données passagers. L'UIP a été mise en place par deux policiers et sera renforcée par deux autres policiers ; elle comptera par ailleurs respectivement un membre du SREL et de l'ADA. Le personnel sera renforcé en fonction des besoins et le travail sera organisé sur base des expériences qui seront faites.

Les systèmes API et PNR fonctionneront parallèlement, puisqu'ils ont des finalités différentes : tandis que l'API n'a pour objet que le contrôle de l'immigration, le PNR a pour but la prévention et la répression du terrorisme et de la criminalité grave, ce qui justifie des sanctions plus élevées pour non-transmission de données. La mise en œuvre de la directive signifie une augmentation considérable des données à traiter, le nombre de mouvements à l'aéroport s'élevant à environ 40 000 par an et les champs de données passant de 5 à dix-neuf. Le traitement se fera suivant deux critères prioritaires, à savoir la provenance du vol (les vols extra-Schengen étant d'un intérêt particulier) et le volume du vol (nombre de passgers). Les compagnies aériennes peuvent choisir parmi trois formats informatiques pour le transfert des données et chaque compagnie est connectée séparément. En ce qui concerne les vols privés, des pourparlers sont en cours avec Luxaviation, bien que le volume de ces vols soit petit.

Quant à l'utilité des données recueillies, on distingue plusieurs hypothèses. La première est celle du contrôle, par le SIS, Interpol ou le fichier central national, du signalement d'une personne. S'agissant d'une personne recherchée par les autorités judiciaires, la Police a une conduite à tenir. Elle dispose d'un mandat d'arrêt européen ou international et est donc en mesure d'agir. Par contre, dans l'hypothèse où une personne utilise un passeport déclaré comme volé ou perdu dans un des systèmes précités, la Police n'a pas la possibilité de saisir ce document de voyage, mais doit suivre une procédure déterminée.

Dans le cas des « Watchlists », les enquêteurs qui les transmettent doivent indiquer la manière de procéder en cas d'apparition d'une personne ciblée. Il en va de même en matière de « rules based targeting ».

La Police ne peut interdire à une compagnie aérienne de réaliser un vol à destination du Luxembourg pour empêcher l'arrivée sur le territoire national d'une personne déterminée. Toutefois, sur base de la législation applicable en matière d'immigration, une compagnie aérienne peut être obligée à ramener à ses frais un passager au lieu de provenance du vol.

Concernant les passagers des vols extra-Schengen, un visa est obligatoire pour les citoyens de certains pays non membres de l'espace Schengen pour entrer dans celui-ci. Pour les soixante pays non membres de l'UE, mais exempts de visa, il est prévu de mettre en place le « European Travel Information and Authorization System (ETIAS) »[7]. De cette manière, chaque personne en provenance d'un pays extra-Schengen sera contrôlée.

Discussion

- Un député pose la question de savoir pour quelle raison le ministère des Affaires étrangères et européennes n'est pas inclus dans ce système de transfert de données, alors qu'il a intérêt à obtenir des informations sur les personnes qui demandent l'autorisation d'entrer dans le pays. En réponse, il est précisé que la directive a pour objet la prévention et la détection d'infractions terroristes et non la migration et l'immigration. La mission de prévention incombe pour l'essentiel au SREL. En effet, en premier lieu, la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État dispose dans son article 3, paragraphe 1er que : « (1) Le SRE a pour mission de rechercher, d'analyser et de traiter, dans une perspective d'anticipation et de prévention, mais à l'exclusion de toute surveillance politique interne, les renseignements relatifs à: a) toute activité qui menace ou pourrait menacer la sécurité nationale ou la sécurité des États étrangers ou des organisations internationales ou supranationales avec lesquelles le Luxembourg poursuit des objectifs communs sur base d'accords ou de conventions bilatérales respectivement multilatérales, ou b) toute activité qui menace ou pourrait menacer les relations internationales du Grand-Duché de Luxembourg, son potentiel scientifique ou ses intérêts économiques définie par le Comité. ». En second lieu, les données recueillies concernent notamment des personnes sous surveillance discrète. Par ailleurs, les données permettent au SREL de répondre aux demandes de pays étrangers concernant les personnes voyageant en provenance ou à destination du Luxembourg ou en transit.

Si la loi précitée du 5 juillet 2016 donne au SREL déjà parmi les moyens et mesures de recherche applicables aux menaces d'espionnage, de prolifération et de terrorisme la possibilité de solliciter les données des dossiers passagers (article 8, paragraphe 1er, lettre a)), le projet de loi transposant la directive complète ces dispositions.

- Pour ce qui est de la qualité des données recueillies, la Police ne peut se baser à présent que sur l'expérience API acquise depuis 2006. Il s'agit des données de base contenues dans le document de voyage, prélevées lors de l'enregistrement des passagers.

En matière de PNR, les vols intra-Schengen pouvant être réservés 48 heures à l'avance, le passager peut indiquer des données qui ne correspondent pas à celles du document de voyage. Le « conformity check » effectué par la compagnie aérienne permet toutefois de vérifier la conformité des données du « boarding pass » avec celles du document de voyage. La Police ne s'intéresse qu'aux listes des passagers, pas aux billets.

[7] https://www.schengenvisainfo.com/fr/etias/

- L’article 8, transposant l’article 13, paragraphe 4 de la directive, interdit le traitement de données PNR qui révèlent notamment les opinions politiques ou la religion. Rappelant que la directive a pour objet la prévention et la détection des infractions terroristes et des formes graves de criminalité, un député souhaiterait connaître la raison pour laquelle le facteur « opinions politiques », en particulier, ne peut être pris en considération, alors qu’une opinion politique peut constituer un risque pour la sécurité.

Monsieur le Ministre indique que les critères ont fait l’objet de longues discussions. Le contenu finalement retenu forme l’accord trouvé entre les 28 États membres et le Parlement européen.

Dans ce contexte, un membre de la commission rappelle l’existence d’une liste noire des organisations terroristes établie par l’Union européenne.

Luxembourg, le 16 juillet 2018

Le Secrétaire-administrateur,
Marianne Weycker

La Présidente de la Commission de la Force publique,
Claudia Dall'Agnol