N° 7151[1]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

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

* * *

SOMMAIRE:

*

AVIS DU PARQUET GENERAL

(24.8.2017)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L'article 37 alinéa 1er prévoit des sanctions pénales identiques à celles prévues à l'article 49 (2) du projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. Si la violation de l'article 8 relatif à l'interdiction de révéler l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle peut se concevoir en tant qu'infraction pénale à condition cependant qu'il y ait eu intention délictuelle on s'interroge cependant sur les sanctions pénales relatives aux violations des articles 15 et 36 du projet de loi sous avis.

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

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

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

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

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

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

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

Martine SOLOVIEFF
Procureur général d'État

*

AVIS DES PARQUETS DE LUXEMBOURG ET DE DIEKIRCH

(15.10.2017)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L'article 8 interdit le traitement des données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle. L'UIP est tenue d'effacer, dès réception et de façon définitive, des informations de ce type lorsqu'elles lui seraient transférées.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L'article 18

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

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

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

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

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

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

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

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

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

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

Ainsi, l'interdiction prévue à l'article 8 de traiter des données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle est punie d'un emprisonnement de huit jours à un ans et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie pourra en outre prononcer la cessation du traitement contraire „aux dispositions du présent alinéa" sous peine d'une astreinte dont le maximum est fixé par la juridiction.

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

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

Jean-Paul FRISING
Procureur d'Etat à Luxembourg

Aloyse WEIRICH
Procureur d'Etat à Diekirch

*

AVIS DU TRIBUNAL D'ARRONDISSEMENT DE ET A LUXEMBOURG

(18.9.2017)

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

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

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

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

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

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

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

Article 8

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

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

Chapitre 5

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

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

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

Chapitre 7

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

Chapitre 8

Le chapitre 8 oeuvre dans le même sens.

Chapitre 9

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

Chapitre 10

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

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

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

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

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

Chapitre 11

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

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

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

ANNEXE II

Listing des infractions:

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

Point a):

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

Point e)

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

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

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

Point h)

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

Point I

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

Point O

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

Point X

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

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

Paul VOUEL

Impression: CTIE – Division Imprimés et Fournitures de bureau