# N° 7151[3]

## 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**

* * *

## AVIS DE LA COUR SUPERIEURE DE JUSTICE

(20.11.2017)

En date du 29 juin 2017, Monsieur le Ministre de la Justice a sollicité de la de la Cour Supérieure de Justice (la Cour) pour Monsieur le Ministre de la Sécurité Intérieure un avis sur 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 constituant la transposition de la directive 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.

Parallèlement, un avis sur le 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 a été sollicité par Monsieur Ministre de la Justice (transposition de la directive (UE) 2016/680) et un avis sur le projet de loi portant création de la Commission nationale pour la protection des données et la mise en oeuvre du règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données a été sollicité par Monsieur le Ministre des Communications et des Médias.

Les projets de loi sous avis constituent la mise en oeuvre et la transposition en droit national du règlement UE 2016/679, précité et de deux directives européennes (UE 2016/680 et UE 2016/681) visant à l'harmonisation des dispositions nationales des Etats membres en matière de protection de données personnelles et ils forment un paquet de dispositions sur cette protection de données qui devront de ce fait être considérées ensemble.

Ils instaurent une réforme du cadre existant, visant à renforcer la protection des données à caractère personnel et à adapter les règles aux nouveaux défis réglementaires, dans un souci de pérennité et de neutralité technologique, en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

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) (*Passenger Name Record*) 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 et qui 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.

L'objectif de la directive (UE) 2016/681 est de permettre un échange de données passagers en temps réel afin de prévenir toute atteinte à la sécurité des citoyens européens marqués par les évènements tragiques récents et d'aboutir à une harmonisation et à une interopérabilité entre les unités d'information de passagers des Etats membres.

Les données PNR qui font l'objet de la directive sont issues des données fournies lors des réservations auprès des entreprises de transport aérien, contiennent davantage d'éléments et sont plus rapidement disponibles.

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 Etats membres de l'Union européenne. Ces menaces terroristes, tout comme la criminalité grave et organisée, appellent une approche commune des Etats membres et la directive permet de prévoir la possibilité d'étendre l'obligation de collecte des données des passagers à d'autres transporteurs, tels les transporteurs ferroviaires ou maritimes. Contrairement aux législateurs français et belges, le législateur luxembourgeois n'a pas choisi d'appliquer les dispositions découlant de la directive à d'autres opérateurs de transport que les transporteurs aériens.

Il convient d'observer que dans un récent avis n° 1/15 du 27 juillet 2017 relatif à l'accord PNR UE-Canada et après plusieurs arrêts historiques mettant au premier plan le droit fondamental à la protection des données personnelles (arrêts *Digital Rights Ireland Ltd*, C-293/12 et C-592/12, 8 avril 2014, *Schrems*, C-362/14, 6 octobre 2015 et *Tele2 Sverige* (C-203/15, 21 juillet 2016) qui pouvaient laisser entrevoir une invalidation du système PNR en raison de la condamnation par la Cour de justice de l'Union européenne (CJUE) de tout stockage de données de masse, et ce de façon indifférenciée, la CJUE a conclu la très longue polémique suscitée par les accords PNR et la directive (UE) 2016/681 et elle a validé le système PNR dans son principe tout en émettant des réserves auxquelles la Cour se rallie.

Ainsi, le juge européen a indiqué un certain nombre de dispositions de l'accord PNR UE-Canada, qui nécessitent une révision afin d'assurer leur conformité avec la Charte des droits fondamentaux. Parmi les points listés, la CJUE estime tout d'abord que les 19 catégories de données qui figurent dans l'accord (les mêmes dans tous les accords PNR ainsi que dans la directive européenne) devraient être définies de manière claire et précise et des termes comme «*toutes les coordonnées disponibles* » ou «*remarques générales*» sont à exclure dès lors qu'ils ne fixent aucune limitation quant à l'étendue et à la nature des informations susceptibles d'y figurer. La CJUE exclut par ailleurs le transfert de données sensibles (celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou concernant l'état de santé ou la vie sexuelle d'une personne), comme étant contraire à la Charte des droits fondamentaux.

La CJUE relève encore que les autorités devront produire des « *modèles et critères préétablis (...) spécifiques et fiables* » de sorte à aboutir à des «*résultats ciblant les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou de criminalité transnationale grave*» Les avancées technologiques devront être un outil au service de la société et non un prétexte à instituer des politiques ultra-sécuritaires violant les droits fondamentaux.

S'agissant de la conservation des données, la CJUE relève que la conservation dans le pays destinataire doit être limité au strict nécessaire après le départ du passager, mais la durée de cinq ans prévue par la directive (UE) 2016/681 et reprise par le projet de loi sous avis ne semble pas « *excéder les limites de ce qui est strictement nécessaire à des fins de lutte contre le terrorisme et la criminalité transnationale grave* ».

Quant au possible transfert de données PNR vers un pays tiers, la CJUE ne l'admet que si la Commission a constaté l'existence d'un « *niveau adéquat* » de protection dans le pays destinataire (art. 25, paragraphe 6 de la directive 95/46), ou « *substantiellement équivalent* » à celui assuré au sein de l'UE.

Quant au contrôle du respect des exigences de la protection des données par le biais d'une autorité indépendante, exigence figurant tant dans la Charte (art. 8, paragraphe 3) que dans le Traité (Article 16, paragraphe 2 TFUE), seule une « *autorité publique indépendante* » présente les qualités requises et la CJUE n'admet pas d'autres termes pour définir l'autorité visée.

Quant au projet de loi sous avis, le chapitre 1er relatif aux dispositions générales définit la finalité de la collecte des données des passagers limitée au transport aérien, finalité consistant dans la prévention, la recherche, la constatation et la poursuite des infractions terroristes et des formes graves de criminalité. Or, si la finalité première de la collecte des données personnelles de passagers aériens est de nature commerciale, le projet de loi sous avis concerne les autorités chargées de la prévention et de la répression du terrorisme et de la criminalité grave.

S'agissant des données (au nombre de 19) à recueillir, elles sont définies à l'annexe I du projet de loi et constituent la reprise textuelle de l'annexe I de la directive (UE) 2016/681, sauf que la numérotation du projet de loi sous avis est constituée par les lettres de l'alphabet dans le projet de loi sous avis et par des chiffres dans la directive.

S'agissant des formes de criminalité grave, il s'agit de 26 infractions faisant l'objet de l'annexe II du projet de loi reprises textuellement de l'annexe II de la directive, infractions qui doivent en outre être sanctionnées d'une peine privative de liberté d'un maximum d'au moins trois ans. La première infraction libellée est la « *participation à une organisation criminelle* » et l'on peut se poser la question si cette infraction inclut l'association de malfaiteurs du titre VI chapitre Ier de notre Code pénal.

Le chapitre 2 du projet de loi sous avis traite de l'Unité d'information passagers (UIP) que chaque Etat membre est obligé d'instituer. Or, selon le projet de loi c'est la Police grand-ducale qui composera cette UIP avec comme personnel détaché possible des membres de l'Administration des Douanes et Accises ou du Service de renseignement de l'Etat. Etant donné que les autorités de poursuite judiciaires sont également compétentes en la matière, il serait opportun de prévoir la possibilité d'un détachement d'un membre des Parquets ou du Parquet général afin d'assurer une meilleure liaison à ce niveau.

Le chapitre 3 du projet de loi traite de la transmission des données PNR par les entreprises de transport aérien à l'UIP prévoyant la méthode de transmission, les délais et le procédé technique. Quant à la méthode à employer dite «push», l'exposé de motifs explique qu'il s'agit de la méthode la plus protectrice des données personnelles alors qu'il s'agit de la transmission par les entreprises de transport de leurs données aux Etats membres ce qui leur permet de garder le contrôle de ces données, la méthode alternative étant la méthode dite «pull» consistant dans l'accès aux données des entreprises de transport par les Etats membres. Il serait opportun de préciser la méthode visée afin de ne pas laisser de doute à ce sujet (article 5 du projet). Quant aux délais dans lesquels les données doivent être transmises, le projet de loi est plus strict que la directive en ce qu'il prévoit deux transmissions, la première transmission devant se faire 48 heures avant le départ et la seconde 24 avant le départ, tandis que la directive ne prévoit qu'une communication de 24 à 48 heures avant l'heure du départ programmé (article 6 du projet).

Le chapitre 4 concerne le traitement des données à caractère personnel en interdisant tout traitement des données personnelles révélant l'origine raciale ou ethnique de la personne, ses opinions politiques, sa religion, ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie ou son orientation sexuelles et en imposant l'effacement de toutes informations complémentaires à celles prévues à l'annexe I du projet de loi. Les articles 10,11 et 12 prévoient les différentes manières dont les données PNR peuvent être utilisées, ainsi que leur évaluation et il faut observer d'abord que la notion de « services compétents » apparaît pour la première fois dans ce chapitre, la notion de services étant traitée plus amplement au chapitre 5 dudit projet. Or, dans les autres projets de loi, précités et dans les directives, il est toujours question des *autorités compétentes* et il y aurait lieu de préciser la notion de service compétent à l'article 2 du projet sous avis relatif aux définitions. En outre, le texte de l'article 13 n'est pas très clair en ce qu'il semble limiter la transmission des données PNR aux autorités judiciaires seulement selon les règles du code de procédure pénale et non en vertu du projet de loi sous avis. Enfin, si le fait de limiter la demande et la réception des données au seul cadre de prévention et de détection des infractions visées par la loi s'inscrit dans les principes prévalant en matière de protection des données à caractère personnel, il y a lieu d'observer que les termes de « *dans la limite du besoin d'en connaître* » sont imprécis et risquent de donner lieu à des interprétations diverses.

Le chapitre 6 vise l'échange d'informations entre Etats membres de l'Union européenne et entre les UIP des Etats membres et les articles 16 et 17 sont parmi les éléments-clé du système PNR européen dès lors qu'ils règlent les transmissions d'office et sur demande des informations PNR au sein de l'Union européenne.

La question se pose cependant s'il n'est pas opportun d'ajouter une référence à l'application des dispositions nationales et internationales en matière d'entraide et de coopération judiciaire qui risquent de se voir en concours avec les dispositions du projet de loi sous avis. La même remarque vaut pour le chapitre 8 relatif au transfert des données PNR à des pays tiers.

Le chapitre 7 relatif aux conditions d'accès aux données PNR par Europol n'appelle pas d'observation de la part de la Cour.

Le chapitre 9 relatif à la durée de conservation et à la dépersonnalisation des données constitue la transposition de l'article 12, paragraphes 1 et 4 de la directive (UE) 2016/681 et la durée de cinq ans a été approuvée par la CJUE.

Quant au chapitre 10, il faut observer ici que c'est l'autorité de contrôle judiciaire qui reçoit compétence pour toiser les réclamations tombant sous l'application des articles 1er et 2 de la loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, tandis que la Commission Nationale de Protection des données (CNDP) reste compétente pour toiser les réclamations tombant sous le champ d'application du règlement (UE) 2016/679. Or, cette dualité de compétences peut comporter un risque de conflits.

Quant aux recours juridictionnels applicables en vertu de la loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale auxquels l'article 31 (2) du projet sous avis se réfère, ils constituent une garantie adéquate et suffisante.

S'agissant du chapitre 11 relatif aux sanctions, les notions «*effets juridiques préjudiciables*» ou d'«*affectation significative*» de l'article 15 et de «*risque élevé*» de l'article 36 du projet de loi sous avis sont des notions d'un contour plutôt flou.

La cessation du traitement contraire aux dispositions en cause pourrait être obligatoire.

S'agissant du recours juridictionnel contre la décision du Ministre prononçant une amende administrative contre l'entreprise de transport dans le cadre de l'article 38, il y a lieu de préciser que le recours en question a lieu devant les juridictions administratives (y compris, en cas d'appel, la Cour administrative) selon les règles de procédure et de délais applicables devant elles.

Luxembourg, le 20 novembre 2017

Impression: CTIE – Division Imprimés et Fournitures de bureau