Numéro du rôle : 6713
Arrêt n° 135/2019 du 17 octobre 2019

A R R Ê T

En cause : le recours en annulation totale ou partielle de la loi du 25 décembre 2016 « relative au traitement des données des passagers », introduit par l'ASBL « Ligue des Droits de l'Homme ».

La Cour constitutionnelle,

composée des présidents F. Daoût et A. Alen, et des juges L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman et M. Pâques, assistée du greffier F. Meersschaut, présidée par le président F. Daoût,

après en avoir délibéré, rend l'arrêt suivant :

*

* *

COPIE NON CORRIGÉE

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 24 juillet 2017 et parvenue au greffe le 26 juillet 2017, l'ASBL « Ligue des Droits de l'Homme » (actuellement « Ligue des droits humains »), assistée et représentée par Me C. Forget, avocat au barreau de Bruxelles, a introduit un recours en annulation totale ou partielle (les articles 3, § 1er, et 8, § 2, et le chapitre 11) de la loi du 25 décembre 2016 « relative au traitement des données des passagers » (publiée au *Moniteur belge* du 25 janvier 2017).

Le Conseil des ministres, assisté et représenté par Me E. Jacubowitz et Me C. Caillet, avocats au barreau de Bruxelles, a introduit un mémoire, la partie requérante a introduit un mémoire en réponse et le Conseil des ministres a également introduit un mémoire en réplique.

Par ordonnance du 26 juin 2019, la Cour, après avoir entendu les juges-rapporteurs T. Giet et R. Leysen, a décidé que l'affaire était en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 17 juillet 2019 et l'affaire mise en délibéré.

Aucune demande d'audience n'ayant été introduite, l'affaire a été mise en délibéré le 17 juillet 2019.

Les dispositions de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle relatives à la procédure et à l'emploi des langues ont été appliquées.

II. *En droit*

– A –

A.1. La partie requérante dit justifier d'un intérêt à agir en ce que son but est de lutter contre l'injustice et toute atteinte arbitraire aux droits d'un individu et de promouvoir toute initiative tendant à la formation et à la promotion des droits et libertés. Dénoncer une loi qui semble mettre à mal certains droits fondamentaux fait partie de ses missions. La Cour a d'ailleurs déjà reconnu son intérêt à agir, notamment par l'arrêt n° 84/2015, dans lequel elle attaquait la loi du 30 juillet 2013 « relative aux communications électroniques ».

Premier moyen

A.2. Le premier moyen, formulé à titre principal, est pris de la violation de l'article 22 de la Constitution, lu ou non en combinaison avec l'article 23 du Règlement général sur la protection des données (ci-après : le « RGPD »), avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et avec l'article 8 de la Convention européenne des droits de l'homme.

COPIE NON CORRIGÉE

A.3.1. La partie requérante constate que l'objectif de la loi du 25 décembre 2016 « relative au traitement des données des passagers » (ci-après : la loi « PNR »), attaquée, est double : d'une part, protéger les données « PNR » des passagers, cet objectif étant dès lors rattaché à l'article 16 du Traité sur le fonctionnement de l'Union européenne (ci-après : le TFUE), et, d'autre part, lutter contre les infractions terroristes et la criminalité transnationale grave, cet objectif étant rattaché à l'article 87 du TFUE, qui porte sur la coopération judiciaire en matière pénale et sur la coopération policière.

Eu égard à ce double objectif, tel qu'il ressort notamment de l'avis de la Cour de justice n° 1/15 du 26 juillet 2017 relatif au projet d'accord « PNR » entre l'Union européenne et le Canada, la loi « PNR » relève à la fois de l'application du RGPD et de celle de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive (UE) 2016/680).

A.3.2. La partie requérante rappelle que la Cour européenne des droits de l'homme interprète largement la notion de « vie privée », au sens de l'article 8 de la Convention européenne des droits de l'homme, lue à la lumière de la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », seul instrument contraignant en la matière, qui exige le respect des principes de loyauté, de licéité, de finalité, de qualité et de proportionnalité en cas de traitement de données à caractère personnel. La Cour de justice, elle, examine la compatibilité d'une ingérence dans les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne en tenant compte de la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la Convention européenne des droits de l'homme.

En l'espèce, la loi « PNR » implique une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel, au sens de l'article 8 de la Convention européenne des droits de l'homme et des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. À cet égard, la partie requérante se réfère aux conclusions de l'avocat général Mengozzi ayant précédé l'avis de la Cour de justice n° 1/15.

Pour que cette ingérence soit conforme à l'article 52, paragraphe 1, de ladite Charte, elle doit répondre aux critères de légalité, de nécessité au regard du but poursuivi et de proportionnalité, ce qui n'est pas le cas en l'espèce, selon la partie requérante.

A.4. La loi « PNR » confère une importante marge d'appréciation au pouvoir exécutif, qu'elle charge de définir, par arrêté royal, certains éléments essentiels – dont les données qui devront être collectées ou les modalités de leur transmission par secteur de transport et pour chaque opérateur (articles 3, § 2, et 7, § 3, *in fine*) –, ce qui est contraire au principe de la légalité, lequel exige que l'ingérence soit prévue par la loi ou, en cas de délégation au Roi, que les éléments essentiels soient prévus par la loi de manière suffisamment précise et détaillée.

La section de législation du Conseil d'État a d'ailleurs indiqué, dans son avis sur le projet de loi devenu la loi « PNR », qu'il lui était impossible de vérifier la proportionnalité de la mesure, étant donné l'importante marge d'appréciation laissée au pouvoir exécutif.

A.5.1. Selon la partie requérante, la loi attaquée ne poursuit pas un but légitime. Elle prévoit en effet une démarche de « *pre-screening* », qui consiste à évaluer le risque que représentent les passagers, avant l'arrivée, le transit ou le départ national. Ce *pre-screening* comprend deux axes : d'une part, rechercher des correspondances positives dans les banques de données gérées par les services compétents, et, d'autre part, faire émerger des profils de passagers à risque, sur la base d' « indicateurs de la menace ». L' « Unité d'information des passagers » (ci-après : l'UIP), créée au sein du SPF Intérieur, est chargée de la conservation et du traitement des données transmises par les transporteurs et opérateurs de voyage, et doit valider la correspondance positive « hit », qui sera alors traduite en « match ». Le texte n'énumère pas les bases de données qui feront l'objet d'un croisement, ni les données exactes qui seront contenues dans la banque de données de l'UIP.

COPIE NON CORRIGÉE

La loi « PNR » s'inscrit donc dans la perspective proactive de déterminer des « profils » à risque, ce qui ne constitue pas un objectif « légitime » au sens de l'article 8 de la Convention européenne des droits de l'homme et de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne.

A.5.2. Si le choix des différentes méthodes d'enquête relève, certes, du pouvoir d'appréciation des États membres, ce pouvoir n'est pas illimité. En tout état de cause, l'objectif de « prévention » des infractions pénales, au sens de l'article 23 du RGPD, n'est pas pertinent en l'espèce, dès lors que la loi « PNR » a justement pour objectif de déterminer des profils à risque, indépendamment de la commission éventuelle ou future d'infractions pénales.

A.6.1. À titre préliminaire, la partie requérante fait valoir que les mesures attaquées ne sont pas nécessaires à la réalisation du but visé et qu'elles doivent donc être annulées.

Dans son avis n° 1/15, la Cour de justice a mentionné l'utilité du dispositif, sans toutefois faire le lien avec la lutte contre le terrorisme et contre la criminalité transfrontalière grave. L'absence de justification de ces mesures a pourtant été critiquée à plusieurs reprises par le « Groupe de travail Article 29 » – un organe consultatif européen indépendant chargé du respect du droit à la protection des données et de la vie privée –, par le Comité européen pour la protection des données, par le Comité consultatif de la Convention n° 108 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » et par le Parlement européen.

A.6.2. Dans son mémoire en réponse, la partie requérante indique qu'il est en toute hypothèse regrettable que la Cour de justice n'ait pas rappelé, à l'occasion de son avis n° 1/15, l'importance d'effectuer une analyse d'impact préalable sur la base d'une étude fondée sur des éléments probants, qui aurait permis d'établir la nécessité de la mesure. Le RGPD impose d'ailleurs la réalisation d'une analyse d'impact en cas de traitement de données à caractère personnel à grande échelle, ou de profilage.

En outre, le dispositif mis en place prévoit que les données sont collectées de manière indifférenciée et généralisée par les opérateurs, et transmises aux autorités compétentes pour être conservées pendant cinq ans, sans distinction, différenciation, limitation ou exception en fonction de l'objectif poursuivi, ce qui est manifestement disproportionné, puisque les données des voyageurs sont traitées indépendamment d'un quelconque lien avec une activité terroriste ou avec une infraction pénale.

S'il ressortait des arrêts *Digital Rights*, *Tele2* et *Schrems* que la Cour de justice condamnait le caractère « général et indifférencié » d'un traitement de données à caractère personnel, elle a néanmoins admis, dans son avis n° 1/15, une collecte systématique et indifférenciée des données, limitée à ce qui est strictement nécessaire, sans pour autant admettre la conservation généralisée des données.

A.6.3. La partie requérante estime que le caractère systématique, c'est-à-dire « non ciblé », de la mesure reste problématique et qu'il conviendrait, eu égard à la jurisprudence récente de la Cour de justice relative aux dispositions visées au moyen, d'interroger la Cour de justice à ce sujet.

A.7.1. De manière plus précise, la loi attaquée ne respecte pas le principe de proportionnalité, si on l'envisage eu égard (a) à son champ d'application et aux catégories de données visées, (b) aux traitements de données qu'elle instaure, (c) à ses finalités et (d) à la durée de conservation des données.

A.7.2.1. Tout d'abord, l'article 4, 10°, de la loi attaquée définit de manière très large les données collectées. Ensuite, l'article 9 de la loi attaquée distingue, d'une part, les données « API » (*Advance Passenger Information*), à savoir les données d'enregistrement et d'embarquement, et, d'autre part, les données « PNR » (*Passenger Name Record*), à savoir les données de réservation. Les données « PNR » contiennent plus d'informations que les données « API »; il s'agit notamment de l'itinéraire complet du passager, du nom de l'agence de voyage, du numéro de siège, des informations relatives aux bagages, des données d'enregistrement et d'embarquement, des modes de paiement et de l'adresse de facturation, etc. Ces données doivent permettre de déterminer, grâce à la méthode du *pre-screening*, les passagers qui sont susceptibles de constituer un risque pour la sécurité.

COPIE NON CORRIGÉE

En outre, les données « PNR » sont indirectement susceptibles de contenir des données sensibles pouvant révéler, notamment, l'appartenance à une organisation syndicale, les affinités personnelles et les relations personnelles ou professionnelles (en fonction de la localisation du siège occupé dans l'avion), comme le souligne le Comité consultatif de la Convention n° 108 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ». Il conviendrait à tout le moins de limiter la catégorie des données visées à l'article 9, 12°, de la loi attaquée.

Ces données excèdent manifestement ce qui est strictement nécessaire, comme l'a souligné l'avocat général Mengozzi dans ses conclusions précédant l'avis de la Cour de justice n° 1/15. Dans cet avis n° 1/15, la Cour de justice critique également l'absence de précision concernant ces données. Il conviendrait dès lors de préciser ces catégories de données.

A.7.2.2. En tout état de cause, le champ d'application de la loi attaquée est plus large que le prévoit la directive « PNR », ce qui a été souligné par la Commission de la protection de la vie privée, dans son avis n° 55/2015.

Eu égard à ce large champ d'application, qui implique indirectement le traitement de données sensibles, et compte tenu de l'absence de précision et de clarté en ce qui concerne les données visées, la loi attaquée excède manifestement, au regard du principe de légalité, les limites du strict nécessaire conditionnant l'admission d'une ingérence dans le droit au respect de la vie privée.

A.7.3. La loi « PNR » donne lieu à différents traitements et flux de données à caractère personnel : (1°) les obligations des transporteurs et opérateurs de voyage; (2°) la création d'une banque de données « passagers », (3°) la corrélation entre les bases de données et (4°) les recherches ponctuelles.

Primo, en ce qui concerne les obligations des transporteurs et des opérateurs de voyage (article 3, § 2), la partie requérante renvoie à la critique relative au principe de légalité, d'autant que les notions de « document d'identité » et de « documents de voyage » ne sont pas définies à l'article 7, §§ 1er et 2.

Secundo, en ce qui concerne la création d'une banque de données « passagers » (articles 12 à 15), cette banque de données est gérée par l'UIP créée au sein du SPF Intérieur, qui est également en charge de l'échange de ces données avec les UIP étrangères et Europol. Le législateur n'explique pas la nécessité de créer une banque de données « passagers », alors qu'une mise en correspondance des données – qui serait nettement moins intrusive dans la vie privée que la création d'une banque de données – permettrait également de rencontrer l'objectif poursuivi. Dans son avis n° 1/15, la Cour de justice précise par ailleurs que la conservation de données doit être en lien avec l'objectif poursuivi.

Tertio, en ce qui concerne la corrélation entre les bases de données (article 24), la partie requérante constate qu'il semble – mais la loi n'est pas claire – que le *pre-screening* devrait être effectué dans la banque de données centralisée à l'UIP, à l'aide de critères préétablis servant d'indicateurs de la menace. Or, la loi « PNR » ne définit ni la nature précise des banques de données utilisées pour la corrélation, ni les modalités de cette dernière, dont les « indicateurs de la menace », ce qui a été critiqué par la Commission de la protection de la vie privée, dans son avis n° 55/2015. La loi « PNR » ne prévoit pas davantage que cette corrélation est limitée aux bases de données exploitées en rapport avec la lutte contre le terrorisme et contre la criminalité grave. À défaut de prévisibilité, la loi « PNR » n'offre pas de protection contre les atteintes arbitraires de la puissance publique au droit au respect de la vie privée.

Quarto, en ce qui concerne les recherches ponctuelles, l'article 27 de la loi « PNR » prévoit que, sur la base d'une requête individuelle, les services compétents pourront accéder à la banque de données, dans les limites de leurs missions et des finalités prévues par la loi (article 51). Or, l'article 46*septies* du Code d'instruction criminelle, introduit par l'article 50 de la loi « PNR », confirme le caractère imprécis des données accessibles. En outre, les détachés des services compétents au sein de l'UIP sont juges et parties, puisqu'ils sont chargés de traiter les demandes d'accès et de veiller au respect des conditions d'accès.

A.7.4. La directive « PNR » vise des « finalités spécifiques » et limite son champ d'application aux seules infractions terroristes et formes graves de criminalité, de sorte que les États membres ne sont pas autorisés à poursuivre des objectifs non établis par la directive.

COPIE NON CORRIGÉE

Or, l'article 8 de la loi « PNR » poursuit des finalités de traitement qui sont nettement plus larges que celles qui sont prévues par la directive « PNR », comme la lutte contre l'immigration illégale, des activités susceptibles de constituer une menace pour les intérêts fondamentaux de l'État ou encore la lutte contre la « radicalisation violente », définie uniquement dans une circulaire. Cette finalité de lutter contre la radicalisation violente est d'ailleurs extrêmement large et excède les limites du strict nécessaire, qui s'imposent en vertu de l'avis de la Cour de justice n° 1/15.

A.7.5. L'article 18 de la loi « PNR » prévoit une durée de conservation des données de cinq ans, ce qui est conforme au délai maximal prévu par l'article 12 de la directive « PNR ». Toutefois, le législateur n'a aucunement justifié le choix du délai maximal autorisé par la directive « PNR », que la Commission pour la protection de la vie privée a critiqué dans son avis n° 55/2015 et qui révèle le caractère disproportionné de la mesure.

A.8. Le Conseil des ministres soulève, à titre principal, l'irrecevabilité du premier moyen, en ce que celui-ci est pris de la violation de l'article 23 du RGPD, dès lors qu'il ressort clairement tant du considérant 19 du RGPD que de l'article 1er de la directive « PNR » que le traitement des données « PNR » ne relève pas du RGPD, mais bien de la coopération judiciaire et policière entre les États membres et de la directive (UE) 2016/680.

Le considérant 5 de la directive « PNR » prévoit d'ailleurs en soi un cadre assurant la protection des données « PNR ».

Enfin, le RGPD n'est entré en vigueur que le 25 mai 2018; un acte de l'Union adopté avant cette entrée en vigueur ne sera pas invalidé en tant que tel, mais il devra, au besoin, être modifié. Même si le RGPD était applicable en l'espèce, il ne pourrait être en contradiction avec la loi « PNR », la partie requérante n'ayant pas invoqué, pour le surplus, la violation de la directive (UE) 2016/680 à l'appui de son moyen.

A.9. Rappelant que les dispositions invoquées dans le moyen ne sont pas absolues, le Conseil des ministres estime qu'il est satisfait au principe de légalité.

En l'espèce, les données pouvant au maximum être requises par le Roi en vertu de la délégation qui Lui est conférée par l'article 3, § 2, de la loi « PNR » sont définies à l'article 9 de la loi attaquée. En ce qui concerne la critique dirigée contre l'article 7, § 3, attaqué, les obligations qui pèseront sur les transporteurs et sur les opérateurs de voyage sont précisément fixées dans les deux premiers paragraphes de l'article 7, seules les modalités de transmission des données et du contrôle pouvant être déterminées par le Roi. Il ressort par ailleurs des travaux préparatoires que les opérateurs de voyage sont soumis à une obligation de moyen, qui porte sur le contrôle de la correspondance entre les documents d'identité et les documents de voyage.

Comme l'indiquent les travaux préparatoires, ces délégations se justifient par la nécessité d'adapter les modalités d'exécution de ces obligations aux spécificités propres aux transporteurs et aux opérateurs de voyage. La section de législation du Conseil d'État n'a d'ailleurs pas critiqué en soi le principe de ces délégations, mais a uniquement observé qu'elle ne pourrait contrôler la proportionnalité des mesures d'exécution qu'au moment où les projets d'arrêtés royaux auront été élaborés. La mise en œuvre par le Roi d'une délégation qui lui a été conférée par la loi doit se faire dans le respect de la vie privée, mais elle ne relève pas de la compétence de la Cour.

Le principe de légalité n'est pas violé, puisque la loi contient les éléments essentiels des mesures qu'elle prévoit et que l'habilitation au Roi est suffisamment précise. D'ailleurs, la partie requérante ne démontre pas que les délégations au Roi manqueraient de précision. Pour le surplus, l'exigence de légalité s'entend dans un sens matériel selon la Cour européenne des droits de l'homme, de sorte que des actes réglementaires satisfont à la notion de « loi » au sens de la Convention européenne des droits de l'homme.

COPIE NON CORRIGÉE

A.10. Le Conseil des ministres estime que l'utilisation des données « PNR » constitue un outil non seulement utile, mais aussi essentiel, dans le cadre, notamment, de la lutte contre le terrorisme et contre la grande criminalité, ce qui a d'ailleurs été expressément admis par la Cour de justice, dans son avis n° 1/15, et par l'avocat général Mengozzi, dans les conclusions qui ont précédé cet avis. La loi « PNR » a d'ailleurs déjà permis de saisir à de multiples reprises de grandes quantités de drogues et de cigarettes, d'identifier des passeurs d'êtres humains, de procéder à des arrestations pour meurtre ou enlèvement, ainsi que de rechercher des personnes jusque-là inconnues mais qui ont dû faire l'objet d'une intervention au moment du départ ou de l'arrivée.

Pour le surplus, l'instauration d'une UIP et d'une banque de données « passagers » revient à mettre en œuvre une obligation de transposition de la directive « PNR ». La requérante essaie ainsi de remettre en cause la pertinence de cette directive, qui a été votée au sein des institutions européennes et qui n'a fait l'objet d'aucun recours.

A.11.1. Le Conseil des ministres indique que la collecte non ciblée des données « PNR » est nécessaire et pertinente au regard des objectifs poursuivis par la loi attaquée, ce que confirment tant l'avis de la Cour de justice n° 1/15 que les conclusions ayant précédé cet avis. Certes, cet avis et ces conclusions concernent l'accord envisagé entre l'Union européenne et le Canada, mais ils sont transposables à la loi « PNR » et démontrent la proportionnalité de cette dernière. Tant la Cour européenne des droits de l'homme que la Cour de justice confèrent par ailleurs une large marge d'appréciation aux États quant au choix des modalités de surveillance mises en place, les sociétés démocratiques étant aujourd'hui menacées par des formes graves de terrorisme.

La loi « PNR » vise à assurer la sécurité publique, en permettant non seulement la poursuite des infractions terroristes ou de certaines formes graves de criminalité, mais aussi, par une analyse préalable de données recueillies, de la prévention de ces infractions. La Cour de justice a reconnu que ces objectifs sont légitimes au sens de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, tant dans son arrêt *Digital Rights* que dans son avis n° 1/15. L'objectif de prévention des infractions constitue d'ailleurs un des objectifs légitimes visés par l'article 23 du RGPD, pour autant qu'il soit applicable en l'espèce, *quod non*.

Enfin, le moyen critique uniquement la légitimité des évaluations préalables, qui ne peuvent toutefois être dissociées du reste de la loi, puisqu'elles concourent à la réalisation des objectifs légitimes poursuivis par la loi « PNR » dans son ensemble. L'identification de profils à risque permet précisément d'éviter que des infractions terroristes soient commises ou que des formes de criminalité grave voient le jour.

A.11.2. En ce qui concerne la critique relative à l'analyse de l'impact de la mesure, soulevée par la partie requérante dans son mémoire en réponse, le Conseil des ministres estime à titre principal qu'il s'agit d'un moyen pris de la violation de l'article 35 du RGPD, que ce moyen est nouveau et, partant, irrecevable. À titre subsidiaire, cette disposition ne peut remettre en cause la validité de la directive « PNR », ni celle de la loi qui la transpose, ces deux dernières ayant été adoptées avant son entrée en vigueur. Enfin, une analyse d'impact, fondée sur les avis des principaux intéressés et démontrant la nécessité des mesures concernées et leur aptitude à réaliser les objectifs poursuivis, avait été effectuée en 2011.

Le Conseil des ministres estime également que le grief doit être limité à la collecte systématique des données et non au délai de conservation de celles-ci, qui n'était pas critiqué dans la requête, et qu'il doit donc être jugé irrecevable. À titre subsidiaire, ce délai de conservation est nécessaire pour atteindre le but poursuivi par la loi attaquée.

A.11.3. Enfin, comme l'a admis la Cour de justice, l'exclusion de certaines personnes ou de certaines zones d'origine ou encore la limitation du système « PNR » à certains vols feraient obstacle à la réalisation de l'objectif poursuivi.

COPIE NON CORRIGÉE

A.12.1. Les données pouvant au maximum être sollicitées sont définies à l'article 9 de la loi attaquée et la notion de « passager » est définie à l'article 4, 10°, de la loi attaquée; ces articles visent essentiellement les mêmes données et personnes que celles qui sont visées dans la directive « PNR ». Comme il a été dit précédemment, il n'y a pas violation du principe de légalité, en ce que la partie requérante n'indique pas quelles données ne seraient pas suffisamment précises. Une éventuelle violation des dispositions visées au moyen ne pourrait donc résulter que d'arrêtés royaux, qui ne relèvent pas de la compétence de la Cour.

Par ailleurs, si des données sensibles devaient être transmises par les transporteurs ou par les opérateurs de voyage, l'UIP devrait, conformément aux articles 10 et 11 de la loi attaquée, les effacer définitivement dès leur réception. Cette interdiction de principe de l'utilisation des données sensibles va même au-delà de ce que préconisait l'avis du Comité consultatif de la Convention n° 108 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ». Enfin, l'article 6 de la loi attaquée prévoit l'obligation d'informer les passagers que leurs données seront transmises à l'UIP et pourront être traitées ultérieurement dans le cadre des finalités visées à l'article 8 de la loi attaquée.

A.12.2. Le Conseil des ministres estime que les mesures attaquées sont proportionnées.

Primo, en ce qui concerne l'identification des traitements, le Conseil des ministres renvoie à son argumentation relative au principe de légalité, la loi s'interprétant, pour le surplus, à la lumière de ses travaux préparatoires.

Secundo, en ce qui concerne la création d'une banque de données « passagers », le Conseil des ministres soulève à titre principal que la partie requérante se contente d'affirmer, sans le démontrer, qu'une mise en concordance aurait permis de rencontrer l'objectif poursuivi et qu'elle aurait été moins intrusive dans le droit au respect de la vie privée. Partant, le moyen est irrecevable, en ce qu'il ne démontre pas en quoi les dispositions invoquées auraient été violées.

À titre subsidiaire, le Conseil des ministres rappelle que la Cour ne peut substituer son appréciation à celle du législateur.

À titre infiniment subsidiaire, le Conseil des ministres estime que le moyen n'est pas fondé. La directive « PNR » vise elle-même à la création d'une base de données « PNR » au sein des UIP des différents États membres. Ensuite, une simple mise en concordance ne suffirait pas pour réaliser les évaluations préalables en vue d'identifier les risques pour la sécurité. Que ces évaluations préalables soient ou non définies comme étant du profilage, elles supposent l'existence d'une banque de données, sous quelque forme que ce soit. La création d'une base de données permet d'ailleurs de rencontrer le considérant 25 de la directive « PNR », qui invite à conserver les données pendant la période nécessaire eu égard aux objectifs poursuivis. Enfin, les services compétents n'auront jamais accès à toutes les données, mais uniquement à certaines de celles-ci, lorsqu'ils soumettront une recherche sur la base de critères précis ou par le biais d'une corrélation avec diverses banques de données. Pour le surplus, la création de cette banque de données est entourée de nombreuses garanties pour la protection de la vie privée, comme la désignation d'un délégué pour la protection des données ou l'intervention de la Commission de la protection de la vie privée.

Tertio, en ce qui concerne la corrélation entre les différentes bases de données, le Conseil des ministres rappelle que les articles 24 et 25 de la loi « PNR » transposent l'article 6 de la directive « PNR ». Les critères préétablis peuvent être mis à jour par l'UIP et doivent être ciblés, proportionnés, spécifiques et non discriminatoires, et la correspondance doit être validée par l'UIP. Il ressort par ailleurs des travaux préparatoires que le législateur n'entend pas opérer de corrélation entre la banque de données « passagers » et l'ensemble des banques de données auxquelles ont accès les autorités compétentes, mais uniquement entre la banque de données « passagers » et celles qui correspondent aux finalités poursuivies par la loi attaquée. Ces mesures sont conformes aux enseignements de l'avis de la Cour de justice n° 1/15, dès lors que l'article 6, paragraphe 3, de la directive « PNR » ne précise pas non plus quelles banques de données peuvent être mises en corrélation. Un pouvoir d'appréciation n'est pas incompatible non plus avec le principe de légalité, tel qu'il est interprété par la Cour européenne des droits de l'homme.

COPIE NON CORRIGÉE

L'objectif de la loi ne pourrait par ailleurs pas être atteint si les voyageurs connaissaient à l'avance les critères qui donneront lieu à une correspondance positive car ils pourraient adapter leur comportement en conséquence. L'article 16 de la loi attaquée indique en outre clairement que le *pre-screening* doit être effectué au sein de la base de données « passagers », ce qui est donc conforme au principe de légalité.

Quarto, en ce qui concerne les recherches ponctuelles, le Conseil des ministres estime à titre principal que le moyen est irrecevable en ce qu'il soutient que la loi excède « ce qui est strictement nécessaire », sans identifier la règle violée et en quoi cette règle serait méconnue.

À titre subsidiaire, le Conseil des ministres estime que la critique n'est pas fondée. Les articles 27, 50 et 51 attaqués visent par « données pouvant être sollicitées » les « données ' passagers ' », qui sont elles-mêmes définies à l'article 4, 17°, de la loi « PNR », lequel fait référence à l'article 9 de la même loi. Ces données sont donc bien identifiées dans la loi « PNR ».

Par ailleurs, il existe plusieurs formes de contrôle préalable à la demande d'obtention des informations contenues dans un dossier « PNR » en vue de procéder à des recherches ponctuelles, qui imposent soit une demande écrite et motivée de la part du procureur du Roi, sauf en cas d'extrême urgence où un accord oral du procureur du Roi suffit, soit une décision écrite et motivée du fonctionnaire dirigeant de l'un des deux services de renseignement et de sécurité du Royaume.

Pendant la période de leur détachement, les membres détachés des services compétents sont placés sous l'autorité fonctionnelle du fonctionnaire dirigeant de l'UIP, qui est responsable du respect de la légalité et de la régularité des traitements, de sorte que les demandes reçues par l'UIP seront traitées par des personnes indépendantes. Il ne peut être soutenu que les détachés des services compétents seraient à la fois juges et parties.

Enfin, la Commission de la protection de la vie privée a salué ces différentes garanties qui entourent les recherches ponctuelles.

A.12.3. En ce qui concerne la finalité des traitements, le Conseil des ministres estime que la loi attaquée pouvait viser à la lutte contre l'immigration illégale. Il souligne que ce ne seront pas les données « PNR » qui seront transférées dans le cadre du chapitre 11 de la loi attaquée, mais uniquement les données « API ».

Comme la directive 2004/82/CE, la loi « PNR » définit la notion de « frontières extérieures » comme les « frontières extérieures des États membres de l'Union européenne avec des pays tiers ». Seules les données « API » qui concernent des passagers franchissant les frontières extérieures de la Belgique seront donc transmises aux services de police chargés du contrôle aux frontières et, en cas de besoin, à l'Office des étrangers.

En ce qui concerne la finalité de suivi des activités visées dans la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité », le Conseil des ministres rappelle que cette finalité a été intégrée dans la loi « PNR » en réponse à une remarque formulée par la section de législation du Conseil d'État. La Commission pour la protection de la vie privée soulignait d'ailleurs les garanties qui entourent cette finalité, laquelle consiste à protéger les intérêts essentiels de l'État contre les activités terroristes ou contre les agissements d'organisations criminelles.

Enfin, la prévention de troubles graves à la sécurité publique dans le cadre de la radicalisation violente est mise en œuvre concrètement par le suivi des phénomènes et groupements visés à l'article 44/5, § 2, de la loi du 5 août 1992 « sur la fonction de police ». La circulaire évoquée n'est pas pertinente en l'espèce, puisque les travaux préparatoires indiquent que seul le phénomène de la radicalisation violente et des groupements liés est visé. La référence à cette disposition permet donc de déterminer de manière suffisamment précise la finalité poursuivie en l'espèce, qui est de ne rendre accessibles que les données « API » et non les données « PNR ».

A.12.4. En ce qui concerne la durée de conservation des données, le Conseil des ministres précise que celle-ci est régie non seulement par l'article 18 de la loi attaquée, mais aussi par l'ensemble du chapitre 9 de cette même loi.

COPIE NON CORRIGÉE

Les membres du personnel de l'UIP ne disposent par ailleurs pas d'un accès direct à l'ensemble des données contenues dans la banque de données « passagers ». En outre, après une période de six mois, ces données seront dépersonnalisées et il ne pourra y être accédé que dans les cas et conditions strictes prévus par l'article 27 de la loi attaquée, qui visent essentiellement la recherche et la poursuite de diverses infractions. Il n'est pas déraisonnable de prévoir un délai de conservation de cinq ans, ce qui correspond d'ailleurs à la durée minimum de prescription de l'action publique en ce qui concerne les délits et crimes correctionnalisés.

L'UIP sera en outre chargée de procéder à une « journalisation » de tous les systèmes et procédures de traitement placés sous sa responsabilité, dans le but de tenir ces traces documentaires à la disposition de la Commission de la protection de la vie privée. Le délégué à la protection des données assurera également diverses missions de contrôle des traitements de données effectués.

La durée de conservation de ces données, qui est conforme à la durée prévue par la directive « PNR », associée aux garanties contenues dans le chapitre 9 de la loi attaquée, n'est donc nullement disproportionnée.

Second moyen

A.13. Le second moyen, qui est formulé à titre subsidiaire, est pris de la violation de l'article 22 de la Constitution, combiné avec l'article 3, paragraphe 2, du Traité sur le fonctionnement de l'Union européenne et avec l'article 45 de la Charte des droits fondamentaux de l'Union européenne.

Les articles 3, § 1er, et 8, § 2, ainsi que le chapitre 11 de la loi attaquée sont contraires à la libre circulation des personnes, qui est reconnue comme l'une des quatre grandes libertés de circulation, en ce qu'ils visent non seulement les transports intra-UE, mais aussi les transports extra-UE (y compris les escales). Alors que les accords de Schengen abolissent les frontières intérieures entre les États membres, les frontières belges ne pourront plus être franchies sans qu'existe un contrôle des personnes, puisque, dès lors qu'une personne se trouvera sur le territoire belge – que ce soit à son arrivée, à son départ ou pour une escale –, ses données seront automatiquement collectées. Dans son mémoire en réponse, la partie requérante indique qu'il est de jurisprudence constante qu'un contrôle aux frontières est susceptible de comporter une ingérence dans le droit au respect de la vie privée et familiale des personnes concernées.

La libre circulation des personnes implique que les contrôles des États ne se fassent qu'aux frontières extérieures de l'Europe et non aux frontières intérieures de la Belgique, alors que c'est pourtant ce qu'instaure indirectement la loi « PNR » en violation du principe de la libre circulation des personnes, comme l'a souligné la Commission de la protection de la vie privée dans son avis n° 55/2015. Par ailleurs, la directive « PNR » interdit les contrôles aux frontières. La partie requérante demande dès lors qu'une question préjudicielle soit posée à cet égard à la Cour de justice.

Pour le surplus, l'exception permise par le règlement (UE) n° 1051/2013 du Parlement européen et du Conseil du 22 octobre 2013 « modifiant le règlement (CE) n° 562/2006 afin d'établir des règles communes relatives à la réintroduction temporaire du contrôle aux frontières intérieures dans des circonstances exceptionnelles » ne peut être invoquée pour justifier la réintroduction d'un contrôle aux frontières, dès lors que cette mesure ne peut être que temporaire et qu'elle ne peut s'expliquer que par une menace grave pour l'ordre public et pour la sécurité nationale.

A.14. À titre principal, le Conseil des ministres soulève l'irrecevabilité du moyen.

En l'espèce, même si elle invoque formellement l'article 22 de la Constitution, la partie requérante n'indique nullement en quoi son grief est articulé autour de cette disposition constitutionnelle; le moyen est donc irrecevable en ce qu'il invoque cette disposition. Le fait que la partie requérante essaie, dans son mémoire en réponse, de faire un lien avec l'article 22 de la Constitution n'est pas suffisant, puisqu'elle n'indiquait aucunement, dans sa requête, en quoi l'article 22 de la Constitution aurait pu être violé.

Par ailleurs, le Conseil des ministres conteste le lien entre les contrôles aux frontières et le droit au respect de la vie privée. Il convient en effet de distinguer le contrôle aux frontières en tant que tel des conséquences de ce contrôle qui, dans certains cas, peuvent conduire à un constat de violation du droit au respect de la vie privée. Or, le franchissement d'une frontière n'est pas toujours justifié par un regroupement familial.

COPIE NON CORRIGÉE

La partie requérante invite en réalité la Cour à effectuer un contrôle direct de la loi attaquée au regard du droit européen, ce qui ne relève pas de sa compétence.

A.15. À titre subsidiaire, le Conseil des ministres estime que la loi attaquée ne consiste aucunement à réinstaurer un contrôle aux frontières et qu'elle ne contrevient aucunement à la liberté de circulation des personnes. La directive « PNR » ne s'applique pas à l'immigration illégale et la loi attaquée transpose non seulement la directive « PNR », mais aussi la directive « API ».

Le moyen, tel qu'il est formulé, vise uniquement les articles 3, § 1er, et 8, § 2, ainsi que le chapitre 11 de la loi attaquée. Or, il ressort de la définition de la notion de « frontières extérieures » que la loi « PNR » ne vise que les contrôles extra-UE. En outre, la loi « PNR » transpose la directive 2004/82/CE, de sorte qu'elle ne peut être interprétée comme réinstaurant un contrôle aux frontières de l'espace Schengen.

À titre infiniment subsidiaire, le considérant 10 de la directive « PNR » prévoit expressément la possibilité d'étendre l'utilisation des données « PNR » aux vols intra-UE, ce qui démontre que cette mesure n'est en soi pas contraire à la liberté de circulation ni au règlement (CE) n° 562/2006.

Demande de renvoi préjudiciel à la Cour de justice

A.16. Dès lors que la loi « PNR » transpose principalement la directive « PNR », elle met en œuvre le droit de l'Union européenne et doit respecter les droits fondamentaux reconnus dans ladite Charte.

La Cour étant, conformément à l'article 267 du Traité sur l'Union européenne [lire : du Traité sur le fonctionnement de l'Union européenne], une juridiction nationale dont les décisions ne sont pas susceptibles de recours, la partie requérante estime qu'il s'impose de poser à la Cour de justice les deux questions préjudicielles soulevées dans le cadre des deux moyens.

A.17. Se référant à la jurisprudence *Cilfit*, le Conseil des ministres invite la Cour à ne pas interroger la Cour de justice.

En ce qui concerne la première question préjudicielle suggérée par la partie requérante, la Cour de justice y a déjà répondu dans son avis n° 1/15. En ce qui concerne la seconde question préjudicielle suggérée, le Conseil des ministres estime que l'application correcte du droit européen dans les articles 3, § 1er, 8, § 2, et dans le chapitre 11 de la loi « PNR » ne laisse planer aucun doute raisonnable.

– B –

Quant à la loi attaquée et à son contexte

B.1. Le recours en annulation, introduit par l'ASBL « Ligue des Droits de l'Homme » (actuellement « Ligue des droits humains »), est dirigé contre la loi du 25 décembre 2016 « relative au traitement des données des passagers » (ci-après : la loi du 25 décembre 2016), qui impose aux transporteurs et aux opérateurs de voyage l'obligation de communiquer les données relatives aux passagers, dites données « PNR » (*Passenger Name Record*).

COPIE NON CORRIGÉE

B.2.1. Conformément à son article 2, la loi du 25 décembre 2016 transpose trois directives européennes.

B.2.2. La loi du 25 décembre 2016 transpose tout d'abord la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 « relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière » (ci-après : la directive « PNR »).

La directive « PNR » prévoit la collecte et le transfert par les transporteurs aériens, des données des dossiers passagers de vols hors Union européenne, à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi qu'à des fins d'enquêtes et de poursuites en la matière. Cette directive s'applique au traitement des données « PNR » relatives aux transports aériens, mais, conformément à son considérant 33, elle n'exclut pas la possibilité, pour les États membres, en vertu de leur droit national, d'étendre le mécanisme « PNR » qu'elle prévoit à d'autres moyens de transport ou à d'autres opérateurs économiques que les transporteurs. En outre, conformément à son article 2, la directive « PNR » peut également s'appliquer aux vols intra-UE.

B.2.3. La loi du 25 décembre 2016 transpose aussi la directive 2004/82/CE du Conseil du 29 avril 2004 « concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers » (ci-après : la directive « API »).

Elle règle donc l'utilisation des données des passagers aux fins prévues par la directive 2004/82/CE, qui reprend le contenu de l'arrêté royal du 11 décembre 2006 « concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers » (ci-après : l'arrêté royal du 11 décembre 2006).

COPIE NON CORRIGÉE

B.2.4. Enfin, la loi du 25 décembre 2016 transpose, partiellement, la directive 2010/65/UE du Parlement européen et du Conseil du 20 octobre 2010 « concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres et abrogeant la directive 2002/6/CE ». Cette directive a pour objet de simplifier et d'harmoniser les procédures administratives appliquées aux transports maritimes par la généralisation de la transmission électronique des renseignements et la rationalisation des formalités déclaratives (article premier, paragraphe 1).

B.3.1. La loi du 25 décembre 2016 vise à « créer un cadre légal afin d'imposer à différents secteurs de transport de personnes à caractère international (aérien, ferroviaire, routier international et maritime) et opérateurs de voyage de transmettre les données de leurs passagers à une banque de données gérée par le SPF Intérieur » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 6) :

« Le traitement des données de passagers, leur comparaison avec des banques de données et leur soumission à des critères prédéterminés sont nécessaires pour révéler ces modes opératoires, découvrir de nouvelles tendances et de nouveaux phénomènes, mais aussi déterminer les passagers à soumettre à un examen approfondi car ceux-ci, sur la base des résultats du traitement, peuvent être impliqués dans une infraction terroriste, dans des formes de criminalité grave, dans des atteintes à l'ordre public dans le cadre de la radicalisation violente et dans des activités pouvant menacer les intérêts fondamentaux de l'État.

[…]

Transposant la directive européenne 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'avant-projet de loi prend au maximum en compte les dispositions prévues au niveau européen. Cela est essentiel pour créer un mécanisme efficace pour le traitement des données relatives aux passagers, de manière à tendre vers une interopérabilité maximale entre les Unités d'information des passagers des États membres.

[…]

L'analyse des données des passagers sera exclusivement confiée à une Unité d'Information des Passagers (UIP) créée au sein du SPF Intérieur et notamment composée, placés sous l'autorité fonctionnelle d'un fonctionnaire dirigeant de l'UIP des membres détachés issus des services de police, de la Sûreté de l'État, du Service général de Renseignement et de Sécurité et des Douanes (en ce qui concerne les Douanes, le traitement des données de passagers est nécessaire à la recherche et à la poursuite de fraudes, comme prévu dans l'Annexe 2, point 7 de la Directive 2016/681) » (*ibid.*, pp. 5-6).

COPIE NON CORRIGÉE

B.3.2. Le système de collecte des données mis en place par la directive « PNR » complète le système de collecte des données créé par la directive « API », les données « PNR » étant plus larges que les données « API » :

« Les données API (*Advanced Passenger Information*) sont des données authentiques. Elles proviennent de documents authentiques (en[tre] autre[s] des cartes d'identités) et sont suffisamment précises pour identifier une personne. Il s'agit des données transmises dans le cadre du check-in et l'embarquement. Dans le cadre de la lutte contre le terrorisme et la criminalité grave, l'information qui est contenue dans les données API est suffisante pour identifier les terroristes et les criminels connus à l'aide de systèmes d'avertissement.

Les données PNR, c'est-à-dire les données de réservation, contiennent davantage d'éléments et sont plus rapidement disponibles que les données API. Ces éléments constituent un instrument très important pour la réalisation d'évaluations de risque concernant des personnes et l'établissement de liens entre des personnes connues et des personnes inconnues. De même pour les recherches ponctuelles, les données PNR représentent une plus-value importante » (*ibid.*, pp. 6-7).

B.3.3. L'obligation de transmission des données des passagers s'applique « tant aux vols internationaux, aux trains internationaux à grande vitesse, au transport international affrété par cars et au transport maritime à destination et à partir de l'Union européenne, qu'au transport entrant et sortant de l'Union européenne » (*ibid.*, p. 7), en vertu de la possibilité prévue par l'article 2 de la directive « PNR ».

Par ailleurs, l'obligation légale de transmission des données des passagers s'applique non seulement aux transporteurs, visés par la directive « PNR », mais également aux opérateurs de voyage, en vertu de la possibilité, offerte par la directive « PNR », d'imposer cette obligation à d'autres acteurs économiques que les transporteurs (*ibid.*, p. 8).

Quant à l'étendue du recours

B.4.1. La Cour doit déterminer l'étendue du recours en annulation en se basant sur le contenu de la requête.

COPIE NON CORRIGÉE

La Cour peut uniquement annuler des dispositions législatives explicitement attaquées contre lesquelles des moyens sont invoqués et, le cas échéant, des dispositions qui ne sont pas attaquées mais qui sont indissociablement liées aux dispositions qui doivent être annulées.

B.4.2. Bien que la partie requérante demande, par son premier moyen, l'annulation de l'intégralité de la loi du 25 décembre 2016, il ressort de l'exposé du moyen que les griefs sont uniquement dirigés contre les articles 3, § 2, 4, 9° et 10°, 7 à 9, 12 à 16, 18, 24 à 27, 50 et 51 de la loi du 25 décembre 2016. En conséquence, le recours en annulation n'est recevable que dans cette mesure.

Le second moyen, formulé à titre subsidiaire, est dirigé contre les articles 3, § 1er, 8, § 2, et contre le chapitre 11, qui comporte les articles 28 à 31, de la loi du 25 décembre 2016.

B.4.3. S'il devait apparaître de l'examen plus approfondi des moyens que seules certaines parties des dispositions attaquées sont critiquées, l'examen sera, le cas échéant, limité auxdites parties.

B.5. Les articles attaqués disposent :

« CHAPITRE 2. – *Champ d'application*

Art. 3. § 1er. La présente loi détermine les obligations des transporteurs et des opérateurs de voyage relatives à la transmission des données des passagers à destination du, en provenance du et transitant par le territoire national.

§ 2. Le Roi détermine par arrêté délibéré en Conseil des ministres par secteur de transport et pour les opérateurs de voyage, les données des passagers à transmettre et leurs modalités de transmission, après avis de la Commission de la protection de la vie privée.

CHAPITRE 3. – *Définitions*

Art. 4. Pour l'application de la présente loi et de ses arrêtés d'exécution, l'on entend par :

[…]

COPIE NON CORRIGÉE

9° ‘ PNR ’ : le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations visées à l’article 9, nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs et les opérateurs de voyage concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs (utilisés pour contrôler les passagers lors de l’embarquement) ou des systèmes équivalents offrant les mêmes fonctionnalités;

10° ‘ passager ’ : toute personne, y compris une personne en correspondance ou en transit et à l’exception du personnel d’équipage, transportée ou devant être transportée par le transporteur, avec le consentement de ce dernier, lequel se traduit par l’inscription de cette personne sur la liste des passagers;

[…]

CHAPITRE 4. – *Obligations des transporteurs et opérateurs de voyage*

[…]

Art. 7. § 1er. Les transporteurs transmettent les données des passagers visées à l’article 9, § 1er, dont ils disposent, et s’assurent que les données de passagers visées à l’article 9, § 1er, 18°, dont ils disposent, sont complètes, exactes et actuelles. A cette fin, ils vérifient la correspondance entre les documents de voyage et l’identité du passager concerné.

§ 2. Les opérateurs de voyage transmettent les données des passagers visées à l’article 9, § 1er, dont ils disposent, et s’assurent que les données des passagers visées à l’article 9, § 1er, 18°, dont ils disposent, sont complètes, exactes et actuelles. A cette fin, ils prennent toutes les mesures nécessaires afin de vérifier la correspondance entre les documents de voyage et l’identité du passager concerné.

§ 3. Le Roi détermine par arrêté délibéré en Conseil des ministres par secteur de transport et pour les opérateurs de voyage, les modalités relatives à l’obligation prévue aux §§ 1er et 2.

CHAPITRE 5. – *Finalités du traitement des données*

Art. 8. § 1er. Les données des passagers sont traitées aux fins :

1° de la recherche et la poursuite, en ce compris l’exécution des peines ou des mesures limitatives de liberté, relatives aux infractions visées à l’article 90*ter*, § 2, 1°*bis*, 1°*ter*, 1°*quater*, 1°*quinquies*, 1°*octies*, 4°, 5°, 6°, 7°, 7°*bis*, 7°*ter*, 8°, 9°, 10°, 10°*bis*, 10°*ter*, 11°, 13°, 13°*bis*, 14°, 16°, 17°, 18°, 19° et § 3, du Code d’instruction criminelle;

2° de la recherche et la poursuite, en ce compris l’exécution des peines ou des mesures limitatives de liberté, relatives aux infractions visées aux articles 196, en ce qui concerne les infractions de faux en écritures authentiques et publiques, 198, 199, 199*bis*, 207, 213, 375 et 505 du Code pénal;

COPIE NON CORRIGÉE

3° de la prévention des troubles graves à la sécurité publique dans le cadre de la radicalisation violente par le suivi des phénomènes et groupements conformément à l'article 44/5, § 1er, 2° et 3° et § 2, de la loi du 5 août 1992 sur la fonction de police;

4° du suivi des activités visées aux articles 7, 1° et 3°/1, et 11, § 1er, 1° à 3° et 5°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

5° de la recherche et la poursuite des infractions visées à l'article 220, § 2, de la loi générale sur les douanes et accises du 18 juillet 1977 et l'article 45, alinéa 3, de la loi du 22 décembre 2009 relative au régime général d'accise.

§ 2. Sous les conditions prévues au chapitre 11, les données des passagers sont également traitées en vue de l'amélioration des contrôles de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale.

CHAPITRE 6. – *Données des passagers*

Art. 9. § 1er. En ce qui concerne les données de réservation, les données des passagers comprennent au maximum :

1° le code repère du PNR;

2° la date de réservation et d'émission du billet;

3° les dates prévues du voyage;

4° les noms, prénoms et la date de naissance;

5° l'adresse et les coordonnées (numéro de téléphone, adresse électronique);

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

7° l'itinéraire complet pour le passager concerné;

8° les informations relatives aux ' voyageurs enregistrés ', c'est-à-dire les grands voyageurs;

9° l'agence de voyage ou l'agent de voyage;

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

11° les indications concernant la scission ou la division du PNR;

COPIE NON CORRIGÉE

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

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

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

15° les informations sur le partage de code;

16° toutes les informations relatives aux bagages;

17° le nombre et les noms des autres voyageurs figurant dans le PNR;

18° toutes les données préalables sur les passagers (données API) qui ont été collectées et sont énumérées au § 2;

19° l'historique complet des modifications des données énumérées aux 1° à 18°;

§ 2. En ce qui concerne les données d'enregistrement et d'embarquement, les données préalables visées au § 1er, 18°, sont :

1° le type de document de voyage;

2° le numéro de document;

3° la nationalité;

4° le pays de délivrance du document;

5° la date d'expiration du document;

6° le nom de famille, le prénom, le sexe, la date de naissance;

7° le transporteur/opérateur de voyage;

8° le numéro du transport;

9° la date de départ, la date d'arrivée;

10° le lieu de départ, le lieu d'arrivée;

11° l'heure de départ, l'heure d'arrivée;

COPIE NON CORRIGÉE

12° le nombre total de personnes transportées;

13° le numéro de siège;

14° le code repère du PNR;

15° le nombre, le poids et l'identification des bagages;

16° le point de passage frontalier utilisé pour entrer sur le territoire national.

[…]

CHAPITRE 7. – *L'Unité d'information des passagers*

Art. 12. Il est créé, au sein du Service Public Fédéral Intérieur une Unité d'information des passagers.

Art. 13. § 1er. L'UIP est chargée de :

1° la collecte, de la conservation et du traitement des données des passagers transmises par les transporteurs et les opérateurs de voyage, ainsi que de la gestion de la banque de données des passagers;

2° l'échange, à la fois des données des passagers et des résultats de leur traitement, avec les UIP d'autres États membres de l'Union européenne, avec Europol, et avec les pays tiers, conformément au chapitre 12.

§ 2. Sans préjudice d'autres dispositions légales, l'UIP ne peut utiliser les données conservées en vertu du chapitre 9 pour d'autres finalités que celles visées à l'article 8.

Art. 14. § 1er. L'UIP est composée :

1° d'un fonctionnaire dirigeant, assisté par un service d'appui, responsable :

a) de l'organisation et du fonctionnement de l'UIP;

b) du contrôle du respect par les transporteurs et les opérateurs de voyage de leurs obligations prévues au chapitre 4;

c) de la gestion et de l'exploitation de la banque de données des passagers;

d) du traitement des données de passagers;

e) du respect de la légalité et de la régularité des traitements visés au chapitre 10;

f) du soutien des services compétents pour l'exécution de leurs compétences au sein de l'UIP.

COPIE NON CORRIGÉE

2° de membres détachés issus des services compétents suivants :

a) des Services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

b) de la Sûreté de l'État visée par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

c) du Service général de Renseignement et de Sécurité visé par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

d) de l'Administration Enquête et Recherche et de l'Administration Surveillance, Contrôle et Constatation de l'Administration générale des Douanes et Accises visée par l'arrêté du Président du Comité de direction du 16 octobre 2014 portant création des nouveaux services de l'Administration générale des Douanes et Accises.

Durant la période de leur détachement, les membres des services compétents sont placés sous l'autorité fonctionnelle et hiérarchique du fonctionnaire dirigeant de l'UIP. Toutefois, ceux-ci gardent le statut de leur service d'origine.

§ 2. Après concertation avec le délégué à la protection des données et après avis de la Commission de la protection de la vie privée, le fonctionnaire dirigeant de l'UIP et les services compétents concluent le protocole d'accord visé à l'article 17 afin de déterminer les modalités relatives à la transmission des données. Le protocole prévoit au minimum les garanties suivantes :

- les modalités relatives à l'échange des données;

- les délais maximaux déterminés par la loi pour le traitement des données;

- l'information de l'UIP par les services compétents de la suite donnée aux correspondances positives validées.

§ 3. Conformément aux obligations légales de chaque service compétent, l'Autorité Nationale de Sécurité homologue un système de communication et d'informations sécurisé et crypté en vue de l'envoi automatisé des correspondances positives.

§ 4. Le Roi détermine par arrêté délibéré en Conseil des ministres et après avis de la Commission de la protection de la vie privée, les modalités de composition et d'organisation de l'UIP, le statut du fonctionnaire dirigeant et des membres de l'UIP ainsi que les directions ou sections au sein des services compétents chargées du traitement des données des passagers.

CHAPITRE 8. – *La banque de données des passagers*

Art. 15. § 1er. Il est créé une banque de données des passagers gérée par le Service Public Fédéral Intérieur dans laquelle sont enregistrées les données de passagers.

COPIE NON CORRIGÉE

§ 2. Le fonctionnaire dirigeant de l'UIP est le responsable du traitement de la banque de données des passagers au sens de l'article 1er, § 4, de la loi relative à la protection de la vie privée.

§ 3. Les droits d'accès et de rectification prévus respectivement aux articles 10 et 12 de la loi relative à la protection de la vie privée, concernant les données des passagers s'exercent directement auprès du délégué à la protection des données.

Par dérogation à l'alinéa 1er, ces droits s'exercent auprès de la Commission de la protection de la vie privée en ce qui concerne les correspondances positives et les résultats des recherches ponctuelles visées aux articles 24 à 27.

§ 4. Les traitements des données des passagers effectués en vertu de la présente loi sont soumis à la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. La Commission de la protection de la vie privée exerce les compétences prévues dans la loi relative à la protection de la vie privée.

Art. 16. Dans le cadre des finalités visées à l'article 8, § 1er, la banque de données des passagers est directement accessible par l'UIP pour les traitements visés aux articles 24 à 27, conformément aux dispositions prévues au chapitre 9.

[…]

CHAPITRE 9. – *Des délais de conservation*

Art. 18. Les données des passagers sont conservées dans la banque de données des passagers pour une durée maximale de cinq ans à compter de leur enregistrement. À l'issue de ce délai, elles sont détruites.

[…]

CHAPITRE 10. – *Le traitement des données*

Section 1re. – Le traitement des données de passagers dans le cadre de l'évaluation préalable des passagers

Art. 24. § 1er. Les données des passagers sont traitées en vue de la réalisation d'une évaluation préalable des passagers avant leur arrivée, leur départ ou leur transit prévu sur le territoire national afin de déterminer quelles personnes doivent être soumises à un examen plus approfondi.

§ 2. Dans le cadre des finalités visées à l'article 8, § 1er, 1°, 4° et 5°, ou relatives aux menaces mentionnées aux articles 8, 1°, a), b), c), d), f), g) et 11, § 2, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, l'évaluation préalable des passagers repose sur une correspondance positive, résultant d'une corrélation des données des passagers avec :

COPIE NON CORRIGÉE

1° les banques de données gérées par les services compétents ou qui leur sont directement disponibles ou accessibles dans le cadre de leurs missions ou avec des listes de personnes élaborées par les services compétents dans le cadre de leurs missions.

2° les critères d'évaluation préétablis par l'UIP, visés à l'article 25.

§ 3. Dans le cadre des finalités visées à l'article 8, § 1er, 3°, l'évaluation préalable des passagers repose sur une correspondance positive, résultant d'une corrélation des données des passagers avec les banques de données visées au § 2, 1°.

§ 4. La correspondance positive est validée par l'UIP dans les vingt-quatre heures après réception de la notification automatisée de la correspondance positive.

§ 5. Dès le moment de cette validation, le service compétent, qui est à l'origine de cette correspondance positive, donne une suite utile le plus rapidement possible.

Art. 25. § 1er. Les données des passagers peuvent être exploitées par l'UIP pour mettre à jour ou définir de nouveaux critères destinés à cibler des individus lors des évaluations préalables des passagers, visées à l'article 24, § 2, 2°.

§ 2. L'évaluation des passagers avant leur arrivée, leur transit ou leur départ au regard des critères préétablis est réalisée de façon non-discriminatoire. Ces critères ne peuvent viser l'identification d'un individu et doivent être ciblés, proportionnés et spécifiques.

§ 3. Ces critères ne peuvent pas être fondés sur des données qui révèlent l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à une organisation syndicale, son état de santé, sa vie sexuelle ou son orientation sexuelle.

Art. 26. § 1er. Pour la finalité visée à l'article 8, § 1er, 3°, seules les données des passagers visées à l'article 9, § 1er, 18°, relatives à la ou les personnes pour lesquelles une correspondance positive est générée sont accessibles.

§ 2. Pour la finalité visée à l'article 8, § 1er, 1°, 4° et 5°, ou relatives aux menaces mentionnées aux articles 8, 1°, a), b), c), d), f), g), et 11, § 2, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, toutes les données des passagers visées à l'article 9 sont accessibles.

Section 2. – Le traitement des données dans le cadre des recherches ponctuelles

Art. 27. Les données des passagers sont exploitées en vue de procéder à des recherches ponctuelles aux fins visées à l'article 8, § 1er, 1°, 2°, 4° et 5°, et aux conditions prévues à l'article 46*septies* du Code d'instruction criminelle ou à l'article 16/3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

COPIE NON CORRIGÉE

CHAPITRE 11. – *Le traitement des données des passagers en vue de l'amélioration du contrôle aux frontières et de la lutte contre l'immigration illégale*

Art. 28. § 1er. Le présent chapitre s'applique au traitement des données des passagers par les services de police chargés du contrôle aux frontières et par l'Office des étrangers en vue de l'amélioration des contrôles de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale.

§ 2. Il s'applique sans préjudice des obligations qui incombent aux services de police chargés du contrôle aux frontières et à l'Office des étrangers de transmettre des données à caractère personnel ou d'informations en vertu de dispositions légales ou réglementaires.

Art. 29. § 1er. Aux fins visées à l'article 28, § 1er, les données de passagers sont transmises aux services de police chargés du contrôle aux frontières et à l'Office des étrangers pour leur permettre d'exercer leurs missions légales, dans les limites prévues au présent article.

§ 2. Seules les données de passagers visées à l'article 9, § 1er, 18°, concernant les catégories de passagers suivantes sont transmises :

1° les passagers qui envisagent d'entrer ou sont entrés sur le territoire par les frontières extérieures de la Belgique;

2° les passagers qui envisagent de quitter ou ont quitté le territoire par les frontières extérieures de la Belgique;

3° les passagers qui envisagent de passer par, se trouvent dans ou sont passés par une zone internationale de transit située en Belgique.

§ 3. Les données de passagers visées au § 2 sont transmises aux services de police chargés du contrôle aux frontières extérieures de la Belgique immédiatement après leur enregistrement dans la banque de données de passagers. Ceux-ci conservent ces données dans un fichier temporaire et les détruisent dans les vingt-quatre heures qui suivent la transmission.

§ 4. Lorsqu'il en a besoin pour l'exercice de ses missions légales, les données de passagers visées au § 2 sont transmises à l'Office des étrangers immédiatement après leur enregistrement dans la banque de données de passagers. Celui-ci conserve ces données dans un fichier temporaire et les détruit dans les vingt-quatre heures qui suivent la transmission.

Si à l'expiration de ce délai, l'accès aux données des passagers visées au § 2 est nécessaire dans le cadre de l'exercice de ses missions légales, l'Office des étrangers adresse une requête dûment motivée à l'UIP.

L'Office des étrangers transmet mensuellement un rapport à la Commission de la protection de la vie privée concernant l'application de l'alinéa 2.

COPIE NON CORRIGÉE

Le Roi détermine par arrêté délibéré en Conseil des ministres et après avis de la Commission de la protection de la vie privée les conditions d'accès visées à l'alinéa 2.

Art. 30. § 1er. Les modalités techniques de sécurisation et d'accès, ainsi que les modalités de transmission des données des passagers aux services de police chargés du contrôle aux frontières et à l'Office des étrangers sont précisées dans un protocole conclu en concertation avec le délégué à la protection des données et après avis de la Commission de la protection de la vie privée entre le fonctionnaire dirigeant de l'UIP, d'une part, et le Commissaire général de la police fédérale et le fonctionnaire dirigeant de l'Office des étrangers, chacun en ce qui le concerne, d'autre part.

§ 2. Ces modalités portent au moins sur :

1° le besoin de l'Office des étrangers de connaître les données;

2° les catégories des membres du personnel qui sur la base de l'exécution de leurs missions disposent d'un accès direct aux données transmises;

3° l'obligation du respect du secret professionnel par toutes les personnes qui prennent directement ou indirectement connaissance des données de passagers;

4° les mesures de sécurité en relation avec leur transmission.

Art. 31. Dans les vingt-quatre heures après la fin du transport, visé à l'article 4, 3° à 6°, les transporteurs et les opérateurs de voyage détruisent toutes les données des passagers visées à l'article 9, § 2, qu'ils transfèrent conformément à l'article 7.

[…]

CHAPITRE 15. – *Dispositions modificatives*

Section 1re. – Modification du Code d'instruction criminelle

Art. 50. Dans le Code d'instruction criminelle, il est inséré un article 46*septies* rédigé comme suit :

‘ Art. 46*septies*. En recherchant les crimes et délits visés à l'article 8, § 1er, 1°, 2° et 5°, de la loi du 25 décembre 2016 relative au traitement des données des passagers, le procureur du Roi peut, par une décision écrite et motivée, charger l'officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.

COPIE NON CORRIGÉE

La mesure peut porter sur un ensemble de données relatives à une enquête spécifique. Dans ce cas, le procureur du Roi précise la durée de la mesure qui ne peut excéder un mois à dater de la décision, sans préjudice de renouvellement.

En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et, par une décision motivée et écrite, requérir du fonctionnaire dirigeant de l'UIP la communication des données des passagers. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence '.

Section 2. – Modification de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 51. Dans le chapitre III, section 1re, sous-section 2, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, il est inséré un article 16/3 rédigé comme suit :

' Art. 16/3. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, décider de façon dûment motivée d'accéder aux données des passagers visées à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

§ 2. La décision visée au § 1er est prise par le dirigeant du service et communiquée par écrit à l'Unité d'information des passagers visée au chapitre 7 de la loi précitée. La décision est notifiée au Comité permanent R avec la motivation de celle-ci.

Le Comite permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales.

La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, la liste des consultations des données des passagers est communiquée une fois par mois au Comité permanent R. ' ».

Quant à l'entrée en vigueur et au champ d'application de la loi du 25 décembre 2016

B.6. En vertu de l'article 54 de la loi du 25 décembre 2016, le Roi détermine par arrêté délibéré en Conseil des ministres, par secteur de transport et pour les opérateurs de voyage, la date d'entrée en vigueur de cette loi.

COPIE NON CORRIGÉE

B.7. L'arrêté royal du 18 juillet 2017 « relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les compagnies aériennes » (ci-après : l'arrêté royal du 18 juillet 2017) définit notamment les obligations des compagnies aériennes et les modalités de transmission des données des passagers.

En vertu de l'article 12 de l'arrêté royal du 18 juillet 2017, la loi du 25 décembre 2016 est, en ce qui concerne les compagnies aériennes, entrée en vigueur le même jour que cet arrêté royal, soit le 7 août 2017.

B.8. De même, l'arrêté royal du 3 février 2019 « relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les transporteurs « HST » et les distributeurs de tickets « HST » définit les obligations des transporteurs « HST » (*High speed train* – service international de transport de voyageurs par voie ferroviaire) et des distributeurs de tickets « HST », ainsi que les modalités de transmission des données des passagers.

En vertu de l'article 10 de l'arrêté royal du 3 février 2019 précité, la loi du 25 décembre 2016 est entrée en vigueur, en ce qui concerne les transporteurs « HST » et les distributeurs de tickets « HST », le même jour que cet arrêté royal, soit le 22 février 2019.

B.9. Enfin, l'arrêté royal du 3 février 2019 « relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les transporteurs par bus » définit les obligations des transporteurs par bus ainsi que les modalités de transmission des données des passagers.

En vertu de l'article 10 de l'arrêté royal du 3 février 2019 précité, la loi du 25 décembre 2016 est entrée en vigueur, en ce qui concerne les transporteurs par bus, le même jour que cet arrêté royal, soit le 22 février 2019.

B.10. Il résulte de ce qui précède que la loi du 25 décembre 2016 est en vigueur en ce qui concerne (1) les compagnies aériennes, (2) les transporteurs « HST » et les distributeurs de tickets « HST » et (3) les transporteurs par bus.

COPIE NON CORRIGÉE

Quant aux modifications apportées à la loi du 25 décembre 2016

B.11.1. L'article 280, alinéa 4, de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » (ci-après : la loi du 30 juillet 2018) a abrogé l'article 15, § 3, de la loi du 25 décembre 2016.

Conformément à l'article 281, alinéa 1er, de la loi du 30 juillet 2018, cette abrogation est entrée en vigueur le jour de la publication de la loi du 30 juillet 2018 au *Moniteur belge*, soit le 5 septembre 2018.

B.11.2. Les travaux préparatoires de la loi du 30 juillet 2018 exposent, en ce qui concerne l'abrogation de l'article 15, § 3, de la loi du 25 décembre 2016 :

« Dans le dernier alinéa le système d'accès direct et indirect des personnes concernées à leurs données prévu par l'article 15 de la loi PNR est supprimé. En effet, ce système ne convenait pas à la nature confidentielle des données traitées, et souffre d'une faille. Le caractère binaire de ce système aurait pu permettre à un passager de savoir, en fonction de l'entité auprès de laquelle il aurait pu exercer l'accès à ses données, si celles-ci ont fait l'objet d'une correspondance positive ou d'une recherche ponctuelle, et ainsi savoir s'il était recherché ou suivi par les services compétents. Le système susmentionné ainsi supprimé, ce sont les dispositions présentes dans la loi relative à la protection à l'égard des données à caractère personnel qui s'appliquent et qui prévoient un accès direct ou indirect en fonction du Titre de la présente loi qui s'applique. Cela permet également de répondre au point 247 de l'avis de la Commission vie privée qui s'interroge sur la conformité d'un tel système avec les dispositions de la présente loi » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3126/001, pp. 254-255).

B.11.3. Aucun recours en annulation n'a été introduit contre l'article 280, alinéa 4, de la loi du 30 juillet 2018.

Il en résulte que le présent recours en annulation, en ce qu'il porte sur l'article 15, § 3, de la loi du 25 décembre 2016, est définitivement devenu sans objet.

B.11.4. La loi du 30 juillet 2018 encadre par ailleurs les traitements de données à caractère personnel, notamment en ce qui concerne les finalités énumérées à l'article 8 de la loi du 25 décembre 2016.

COPIE NON CORRIGÉE

B.11.5. Les travaux préparatoires de la loi du 30 juillet 2018 exposent à ce sujet :

« Les traitements en vue de l'amélioration des contrôles de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale, visés à l'article 8, § 2, de la loi précitée du 25 décembre 2016, qui constitue une transposition de la Directive API, sont classés sous le titre 1er de la présente loi.

Les traitements dans le cadre des finalités visées à l'article 8, § 1er, 1°, 2°, 3° et 5°, de la loi précitée du 25 décembre 2016 sont classés sous le titre 2 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Les traitements dans le cadre de la finalité visée à l'article 8, § 1er, 4°, de la loi précitée du 25 décembre 2016 sont classés sous le titre 3 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) dans le cadre des missions des services de renseignement et de sécurité visés aux articles 7 et 11 de la loi du 30 novembre 1998.

La loi du 25 décembre 2016 précitée contient plusieurs dispositions concernant la protection des données telles que la désignation d'un délégué à la protection des données, la prévision d'une validation manuelle ou encore l'interdiction de traiter des données sensibles. Certains points déjà repris dans la loi du 25 décembre 2016 ne doivent par conséquent plus être repris dans la présente loi » (*ibid.*, pp. 188-189).

B.11.6. Il en résulte que, pour apprécier la portée de l'article 8, attaqué, de la loi du 25 décembre 2016, la Cour doit tenir compte de la loi du 30 juillet 2018.

B.12.1. Les articles 62 à 70 de la loi du 15 juillet 2018 « portant des dispositions diverses Intérieur » (ci-après : la loi du 15 juillet 2018), publiée au *Moniteur belge* le 25 septembre 2018, ont également modifié la loi du 25 décembre 2016.

Les articles 62 à 68 modifient plusieurs articles, attaqués, de la loi du 25 décembre 2016, comme suit :

« Art. 62. À l'article 8 de la loi du 25 décembre 2016 relative au traitement des données des passagers, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, le 1° est remplacé par ce qui suit :

COPIE NON CORRIGÉE

‘ 1° de la recherche et la poursuite, en ce compris l’exécution des peines ou des mesures limitatives de liberté, relatives aux infractions visées à l’article 90*ter*, § 2, 2°, 3°, 7°, 8°, 11°, 14°, 17° à 20°, 22°, 24° à 28°, 30°, 32°, 33°, 34°, 36° à 39°, 43° à 45° et § 3, du Code d’instruction criminelle; ’

2° dans le paragraphe 1er, le 5° est remplacé par ce qui suit :

‘ 5° de la recherche et la poursuite des infractions visées à l’article 220, § 2, de la loi générale sur les douanes et accises du 18 juillet 1977, à l’article 45, alinéa 3, de la loi du 22 décembre 2009 relative au régime général d’accise, à l’article 5 de la loi du 15 mai 2007 relative à la répression de la contrefaçon et de la piraterie de droits de la propriété intellectuelle, à l’article 26 du décret de la Communauté germanophone du 20 février 2017 visant la protection des biens culturels mobiliers particulièrement remarquables ainsi qu’à l’article 24 du décret de la Communauté flamande du 24 janvier 2003 portant protection du patrimoine culturel mobilier présentant un intérêt exceptionnel, l’arrêté ministériel du 7 février 2012 soumettant à licence l’importation des marchandises originaires ou en provenance de Syrie modifié par l’arrêté ministériel du 1er juillet 2014, l’arrêté ministériel du 23 mars 2004 abrogeant l’arrêté ministériel du 17 janvier 2003 soumettant à une autorisation préalable l’importation, l’exportation et le transit des marchandises originaires, en provenance ou à destination de l’Iraq et soumettant à une licence l’importation, l’exportation et le transit de certaines marchandises originaires, en provenance ou à destination de l’Iraq ainsi que la recherche des infractions visées à l’article 5 de la loi du 28 juillet 1981 portant approbation de la Convention sur le commerce international des espèces de faune et de flore sauvages menacées d’extinction, et des Annexes, faites à Washington le 3 mars 1973, ainsi que l’Amendement à la Convention, adopté à Bonn le 22 juin 1979 ’.

Art. 63. Dans l’article 14 de la même loi, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, 2°, le *d)* est remplacé par ce qui suit :

‘ *d)* Les services d’enquête, les services de recherche et les services chargés de la surveillance, du contrôle et de la constatation de l’Administration générale des Douanes et Accises. ’;

2° le paragraphe 4 est remplacé par ce qui suit :

‘ § 4. Le Roi détermine par arrêté délibéré en Conseil des ministres et après avis de l’autorité compétente de contrôle des traitements de données à caractère personnel, les modalités de composition et d’organisation de l’UIP ainsi que le statut du fonctionnaire dirigeant et des membres de l’UIP. ’.

Art. 64. Dans l’article 15, § 2, de la même loi, les mots ‘ banque de données des passagers ’ sont remplacés par les mots ‘ données des passagers ’.

Art. 65. L’article 17 de la même loi est remplacé par ce qui suit :

COPIE NON CORRIGÉE

‘ Art. 17. Après concertation avec le délégué à la protection des données et après avis de l’autorité compétente de contrôle des traitements de données à caractère personnel, le fonctionnaire dirigeant de l’UIP et les services compétents concluent un protocole d’accord mettant en oeuvre les modalités techniques de sécurisation et d’accès.

Ce protocole :

1° garantit que les données traitées sont soumises aux mêmes exigences de sécurité et de protection;

2° veille à ce que les mesures de protection nécessaires soient prises afin :

- de respecter les obligations qui découlent des règles concernant les délais définis dans la présente loi, la conservation et la destruction des données conservées dans la banque de données des passagers;

- de rendre les données inaccessibles pour toute personne qui n’est pas autorisée à y avoir accès;

- d’assurer que les traitements effectués par les membres de l’UIP soient conformes à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

3° prévoit que des autorisations d’accès aux données des passagers et des profils d’utilisateurs communs et spécifiques sont attribuées à toute personne susceptible d’accéder aux données des passagers;

4° garantit que les données sont conservées sur le territoire de l’Union européenne. ’.

Art. 66. Dans l’article 24, § 2, de la même loi, la phrase liminaire de l’alinéa 1er est remplacée par ce qui suit :

‘ Dans le cadre des finalités visées à l’article 8, § 1er, 1°, 2°, 4° et 5°, ou relatives aux menaces mentionnées aux articles 8, 1°, *a), b), c), d), f), g),* et 11, § 2, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, l’évaluation préalable des passagers repose sur une correspondance positive, résultant d’une corrélation des données des passagers avec : ’.

Art. 67. Dans l’article 26 de la même loi, le paragraphe 2 est remplacé par ce qui suit :

‘ § 2. Pour la finalité visée à l’article 8, § 1er, 1°, 2°, 4° et 5°, ou relatives aux menaces mentionnées aux articles 8, 1°, *a), b), c), d), f), g),* et 11, § 2, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, toutes les données des passagers visées à l’article 9 sont accessibles. ’.

Art. 68. Dans l’article 31 de la même loi, les mots ‘ à l’article 9, § 2 ’ sont remplacés par les mots ‘ à l’article 9, § 1er, 18° ’ ».

COPIE NON CORRIGÉE

B.12.2. Ces modifications sont entrées en vigueur le 5 octobre 2018.

B.12.3. La Cour doit examiner dans quelle mesure ces modifications ont une incidence sur l'objet du recours.

B.12.4.1. L'article 62 de la loi du 15 juillet 2018 remplace l'article 8, § 1er, 1° et 5°, de la loi du 25 décembre 2016.

L'article 63 de la loi du 15 juillet 2018 remplace l'article 14, § 1er, 2°, *d)*, et § 4, de la loi du 25 décembre 2016.

L'article 65 de la loi du 15 juillet 2018 remplace l'article 17 de la loi du 25 décembre 2016.

L'article 66 de la loi du 15 juillet 2018 remplace l'article 24, § 2, alinéa 1er, phrase liminaire, de la loi du 25 décembre 2016.

L'article 67 de la loi du 15 juillet 2018 remplace l'article 26, § 2, de la loi du 25 décembre 2016.

B.12.4.2. Du fait de ces modifications, le recours devient en principe sans objet en ce qu'il est dirigé contre les articles 8, § 1er, 1° et 5°, 14, § 1er, 2°, *d)*, et § 4, 17, 24, § 2, alinéa 1er, phrase liminaire, et 26, § 2, de la loi du 25 décembre 2016.

B.12.4.3. Aucun recours en annulation n'a été introduit contre les articles précités de la loi du 15 juillet 2018, qui modifient la loi du 25 décembre 2016.

COPIE NON CORRIGÉE

B.12.4.4. Le présent recours en annulation est dirigé contre la loi du 25 décembre 2016 dans sa version initiale. Même si les articles 8, § 1er, 1° et 5°, 14, § 1er, 2°, *d)*, et § 4, 17, 24, § 2, alinéa 1er, phrase liminaire, et 26, § 2, de la loi du 25 décembre 2016 ont été remplacés par les articles précités de la loi du 15 juillet 2018, le recours en annulation, en ce qu'il est dirigé contre les articles 8, § 1er, 1° et 5°, 14, § 1er, 2°, *d)*, et § 4, 17, 24, § 2, alinéa 1er, phrase liminaire, et 26, § 2, de la loi du 25 décembre 2016, conserve un objet dans la mesure où la loi du 15 juillet 2018 ne modifie pas substantiellement ces articles, attaqués, de la loi du 25 décembre 2016.

La Cour examine en conséquence, à l'égard de chacune de ces dispositions et au regard de chaque grief, dans quelle mesure le recours en annulation a conservé ou non un objet.

B.12.5.1. L'article 64 de la loi du 15 juillet 2018 remplace, dans l'article 15, § 2, de la loi du 25 décembre 2016, les mots « banque de données des passagers » par les mots « données des passagers ».

L'article 68 de la loi du 15 juillet 2018 remplace, dans l'article 31 de la loi du 25 décembre 2016, les mots « à l'article 9, § 2 » par les mots « à l'article 9, § 1er, 18° ».

B.12.5.2. Ces modifications ne constituent que des corrections techniques des articles 15, § 2, et 31, de la loi du 25 décembre 2016, sans remplacer ces dispositions, de sorte qu'elles ne peuvent être considérées comme ayant une incidence sur l'objet du présent recours.

B.12.6. Pour le surplus, la Cour tient compte des modifications précitées, afin, notamment, de déterminer la portée des dispositions attaquées.

B.13.1. Les articles 2 à 11 de la loi du 2 mai 2019 « modifiant diverses dispositions relatives au traitement des données des passagers » (ci-après : la loi du 2 mai 2019), publiée au *Moniteur belge* du 24 mai 2019, ont également modifié la loi du 25 décembre 2016.

Les articles 2 et 4 à 7 de la loi du 2 mai 2019 modifient plusieurs articles, attaqués, de la loi du 25 décembre 2016, comme suit :

COPIE NON CORRIGÉE

« Art. 2. Aux articles 3, § 2, 14, § 2, 15, § 4, 23, § 2, alinéa 2, 29, § 4, 30, § 1er, 44, § 2, 7° et 9°, et § 4, de la loi du 25 décembre 2016 relative au traitement des données des passagers, les mots ‘ la Commission de la protection de la vie privée ’ sont chaque fois remplacés par les mots ‘ l’autorité compétente de contrôle des traitements de données à caractère personnel ’ ».

« Art. 4. A l’article 15 de la même loi, modifié par les lois du 15 juillet 2018 et du 30 juillet 2018, les modifications suivantes sont apportées :

1° Aux paragraphes 2 et 4, les mots ‘ loi relative à la protection de la vie privée ’ sont chaque fois remplacés par les mots ‘ loi relative à la protection des données ’

2° Au paragraphe 2, les mots ‘ l’article 1er, § 4 ’ sont remplacés par ‘ l’article 26, 8° ’.

Art. 5. L’article 24, § 2, de la même loi, modifié par la loi du 15 juillet 2018 est complété par un alinéa rédigé comme suit :

‘ Dans le cadre de la finalité visée à l’alinéa 1er pour laquelle la correspondance positive a été obtenue, l’exploitation des données des passagers dans le cadre de l’évaluation préalable repose, pendant une période de vingt-quatre heures à partir de la validation visée au paragraphe 4, sur :

1° les données des passagers pertinentes du même transport que celui dont est issu la correspondance positive, pour autant que ces données soient corrélées avec les données reprises dans la correspondance positive.

2° les autres données des passagers enregistrées dans la banque de données des passagers de la personne ayant fait l’objet de la correspondance positive, sans préjudice de l’application des articles 19 et 20 ’.

Art. 6. L’article 27 de la même loi est remplacé par ce qui suit :

‘ Art. 27. Les données des passagers sont exploitées en vue de procéder à des recherches ponctuelles aux fins visées à l’article 8, § 1er, 1°, 2°, 4° et 5°, et aux conditions prévues à l’article 46*septies* du Code d’instruction criminelle, à l’article 16/3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ou à l’article 281, § 4 de la loi générale sur les douanes et accises, coordonnée le 18 juillet 1977 ’.

Art. 7. A l’article 29 de la même loi, les modifications suivantes sont apportées :

1° au paragraphe 1er, les mots ‘ chargés du contrôle aux frontières ’ sont remplacés par les mots ‘ visés à l’article 14, § 1er, 2°, a) ’;

2° au paragraphe 3, les mots ‘ chargés du contrôle aux frontières extérieures de la Belgique ’ sont remplacés par ‘ visés à l’article 14, § 1er, 2°, a) ’».

COPIE NON CORRIGÉE

B.13.2. Ces modifications sont entrées en vigueur le 3 juin 2019.

B.13.3. Comme il est dit en B.12.5.2, les articles 2, 4 et 7 de la loi du 2 mai 2019 ne constituent que des corrections techniques des articles 3, § 2, 14, § 2, 15, § 4, 29 et 30, § 1er, de la loi du 25 décembre 2016, de sorte que ces modifications n'ont pas d'incidence sur l'objet du présent recours.

B.13.4. Comme il est dit en B.12.4.4, même si l'article 6 de la loi du 2 mai 2019 remplace l'article 27, attaqué, de la loi du 25 décembre 2016, le recours en annulation, en ce qu'il est dirigé contre cette disposition, conserve un objet dans la mesure où le contenu de l'article 6 de la loi du 2 mai 2019 est identique à la version initiale de cet article 27.

B.13.5. Pour le surplus, la Cour tient compte de la modification apportée par l'article 5 de la loi du 2 mai 2019 à l'article 24, § 2, de la loi du 25 décembre 2016, afin, notamment, de déterminer la portée de la disposition attaquée.

Quant au fond

Quant au premier moyen

B.14. Le premier moyen, formulé à titre principal, est pris de la violation de l'article 22 de la Constitution, lu ou non en combinaison avec l'article 23 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 de ces données, et abrogeant la directive 95/46/CE » (règlement général sur la protection des données – ci-après : le RGPD), avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et avec l'article 8 de la Convention européenne des droits de l'homme.

COPIE NON CORRIGÉE

Selon la partie requérante, la loi du 25 décembre 2016 porterait atteinte au droit au respect de la vie privée et à la protection des données à caractère personnel, garantis par ces dispositions. La loi du 25 décembre 2016 ne respecterait pas le principe de légalité. La collecte, le transfert et le traitement systématiques et indifférenciés des données « PNR » selon une méthode de « *pre-screening* » ne seraient ni nécessaires, ni justifiés par un objectif d'intérêt général et plusieurs mesures instaurées seraient disproportionnées.

En ce qui concerne les normes de référence

B.15.1. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

B.15.2. L'article 8 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

B.15.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (*Doc. parl*., Chambre, 1992-1993, n° 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un tout indissociable.

COPIE NON CORRIGÉE

B.16.1. Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelle et conventionnelle précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée.

Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles. La jurisprudence de la Cour européenne des droits de l'homme fait apparaître que de la protection de ce droit relèvent notamment les données et informations personnelles suivantes : le nom, l'adresse, les activités professionnelles, les relations personnelles, les empreintes digitales, les images filmées, les photographies, les communications, les données ADN, les données judiciaires (condamnations ou inculpations), les données financières et les informations concernant des biens (voy. notamment CEDH, 26 mars 1987, *Leander c. Suède*, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 66-68; 17 décembre 2009, *B.B. c. France*, § 57; 10 février 2011, *Dimitrov-Kazakov c. Bulgarie*, §§ 29-31; 18 octobre 2011, *Khelili c. Suisse*, §§ 55-57; 9 octobre 2012, *Alkaya c. Turquie*, § 29; 18 avril 2013, *M.K. c. France*, § 26; 18 septembre 2014, *Brunet c. France*, § 31).

La Cour de justice considère également que le respect du droit à la vie privée à l'égard du traitement de données à caractère personnel se rapporte à toute information concernant une personne identifiée ou identifiable (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke et Eifert*, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, point 54).

B.16.2. Les droits que garantissent l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme ne sont toutefois pas absolus.

Ils n'excluent pas une ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée, mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, aussi dans la sphère des relations entre les individus (CEDH, 27 octobre 1994, *Kroon et autres c. Pays-Bas*, § 31; grande chambre, 12 novembre 2013, *Söderman c. Suède*, § 78).

COPIE NON CORRIGÉE

B.17.1. L'article 7 de la Charte des droits fondamentaux de l'Union européenne dispose :

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

B.17.2. L'article 8 de la Charte des droits fondamentaux de l'Union européenne dispose :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

B.17.3. L'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, dispose :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

B.17.4.1. L'article 52, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne, dispose :

« Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ».

COPIE NON CORRIGÉE

B.17.4.2. Lorsque la Charte contient des droits correspondant à des droits garantis par la Convention européenne des droits de l'homme, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». Cette disposition aligne le sens et la portée des droits qui sont garantis par la Charte sur les droits correspondants qui sont garantis par la Convention européenne des droits de l'homme.

Les explications de la Charte (2007/C 303/02), publiées au *Journal officiel* du 14 décembre 2007, indiquent que, parmi les articles « dont le sens et la portée sont les mêmes que ceux des articles correspondants dans la CEDH », l'article 7 de la Charte correspond à l'article 8 de la Convention européenne des droits de l'homme.

La Cour de justice rappelle à cet égard que « l'article 7 de la Charte, relatif au droit au respect de la vie privée et familiale, contient des droits correspondant à ceux garantis par l'article 8, paragraphe 1, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après : la « CEDH »), et qu'il convient donc, conformément à l'article 52, paragraphe 3, de la Charte, de donner audit article 7 le même sens et la même portée que ceux conférés à l'article 8, paragraphe 1, de la CEDH, tel qu'interprété par la jurisprudence de la Cour européenne des droits de l'homme » (CJUE, 17 décembre 2015, C-419/14, *WebMindLicenses*, point 70; 14 février 2019, C-345/17, *Buivids*, point 65).

B.17.4.3. En ce qui concerne l'article 8 de la Charte, la Cour de justice considère qu' « ainsi que le prévoit expressément l'article 52, paragraphe 3, seconde phrase, de la Charte, l'article 52, paragraphe 3, première phrase, de celle-ci ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue que la CEDH », et que « l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci et qui n'a pas d'équivalent dans la CEDH » (CJUE, grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige*, point 129).

B.17.4.4. Comme il est dit en B.16.1, la Cour de justice considère également que le respect du droit à la vie privée à l'égard du traitement de données à caractère personnel se rapporte à toute information concernant une personne identifiée ou identifiable (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke et Eifert*, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, point 54).

Dans son avis n° 1/15 du 26 juillet 2017 « relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers », la Cour de justice constate que les données « PNR » comportent des informations sur des personnes identifiées ou identifiables, et que leurs collecte et traitements et l'accès à ces données sont dès lors susceptibles d'affecter le droit au respect de la vie privée, garanti par l'article 7 de la Charte, et le droit à la protection des données à caractère personnel, garanti par l'article 8 de la Charte (CJUE, grande chambre, 26 juillet 2017, avis n° 1/15, *Accord PNR UE-Canada*, points 122-126).

À l'égard des limitations pouvant être apportées aux articles 7 et 8 de la Charte, la Cour de justice considère que les « droits consacrés aux articles 7 et 8 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société » (*ibid.*, point 136) :

« 137. À cet égard, il convient de relever également que, aux termes de l'article 8, paragraphe 2, de la Charte, les données à caractère personnel doivent, notamment, être traitées ' à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi '.

138. En outre, conformément à l'article 52, paragraphe 1, première phrase, de la Charte, toute limitation de l'exercice des droits et des libertés reconnus par celle-ci doit être prévue par la loi et respecter leur contenu essentiel. Selon l'article 52, paragraphe 1, seconde phrase, de la Charte, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui » (*ibid.*).

COPIE NON CORRIGÉE

B.18. L’article 23 du RGPD dispose :

« 1. Le droit de l’Union ou le droit de l’État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l’article 34, ainsi qu’à l’article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu’une telle limitation respecte l’essence des libertés et droits fondamentaux et qu’elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :

a) la sécurité nationale;

b) la défense nationale;

c) la sécurité publique;

d) la prévention et la détection d’infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

e) d’autres objectifs importants d’intérêt public général de l’Union ou d’un État membre, notamment un intérêt économique ou financier important de l’Union ou d’un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

f) la protection de l’indépendance de la justice et des procédures judiciaires;

g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière;

h) une mission de contrôle, d’inspection ou de réglementation liée, même occasionnellement, à l’exercice de l’autorité publique, dans les cas visés aux points a) à e) et g);

i) la protection de la personne concernée ou des droits et libertés d’autrui;

j) l’exécution des demandes de droit civil.

2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant :

a) aux finalités du traitement ou des catégories de traitement;

b) aux catégories de données à caractère personnel;

c) à l’étendue des limitations introduites;

d) aux garanties destinées à prévenir les abus ou l’accès ou le transfert illicites;

COPIE NON CORRIGÉE

e) à la détermination du responsable du traitement ou des catégories de responsables du traitement;

f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement;

g) aux risques pour les droits et libertés des personnes concernées; et

h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation ».

B.19.1. Le Conseil des ministres soulève à titre principal une exception d'irrecevabilité du premier moyen, en ce qu'il est pris de la violation de l'article 23 du RGPD, qui ne s'appliquerait pas à la loi du 25 décembre 2016.

B.19.2.1. L'article 2 du RGPD dispose :

« 1. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :

[…]

d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

[…] ».

B.19.2.2. Le considérant 12 du RGPD indique :

« L'article 16, paragraphe 2, du traité sur le fonctionnement de l'Union européenne donne mandat au Parlement européen et au Conseil pour fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ainsi que les règles relatives à la libre circulation des données à caractère personnel ».

La protection qu'offre le RGPD est fondée sur l'article 16, paragraphe 2, du Traité sur le fonctionnement de l'Union européenne (ci-après : le TFUE).

COPIE NON CORRIGÉE

B.19.2.3. Le considérant 19 du RGPD dispose :

« La protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données, fait l'objet d'un acte juridique spécifique de l'Union. Le présent règlement ne devrait dès lors pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, les données à caractère personnel traitées par des autorités publiques en vertu du présent règlement devraient, lorsqu'elles sont utilisées à ces fins, être régies par un acte juridique de l'Union plus spécifique, à savoir la directive (UE) 2016/680 du Parlement européen et du Conseil. Les États membres peuvent confier à des autorités compétentes au sens de la directive (UE) 2016/680 des missions qui ne sont pas nécessairement effectuées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, de manière à ce que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du présent règlement.

En ce qui concerne le traitement de données à caractère personnel par ces autorités compétentes à des fins relevant du champ d'application du présent règlement, les États membres devraient pouvoir maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement. Ces dispositions peuvent déterminer plus précisément les exigences spécifiques au traitement de données à caractère personnel par ces autorités compétentes à ces autres fins, compte tenu de la structure constitutionnelle, organisationnelle et administrative de l'État membre concerné. Lorsque le traitement de données à caractère personnel par des organismes privés relève du champ d'application du présent règlement, celui-ci devrait prévoir la possibilité pour les États membres, sous certaines conditions, de limiter par la loi certaines obligations et certains droits lorsque cette limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir des intérêts spécifiques importants tels que la sécurité publique, ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cela est pertinent, par exemple, dans le cadre de la lutte contre le blanchiment d'argent ou des activités des laboratoires de police scientifique ».

COPIE NON CORRIGÉE

Comme il ressort de ce considérant, le traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales ne relève en principe pas du RGPD, mais de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive « police »).

B.19.2.4. La directive « police » fixe, dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière, des règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris à la protection contre les menaces pour la sécurité publique et à la prévention de telles menaces, en respectant la nature spécifique de ces activités.

L'article 1er, paragraphe 1, de la directive « police » dispose :

« La présente directive établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ».

L'article 9, paragraphes 1 et 2, de la même directive dispose :

« 1. Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1er, paragraphe 1, ne peuvent être traitées à des fins autres que celles énoncées à l'article 1er, paragraphe 1, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union ou le droit d'un État membre. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

2. Lorsque les autorités compétentes sont chargées par le droit d'un État membre d'exécuter des missions autres que celles exécutées pour les finalités énoncées à l'article 1er, paragraphe 1, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union ».

Le considérant 11 de la directive « police » précise à cet égard :

« […] Les autorités compétentes en question peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive. Lorsqu'un tel organisme ou une telle entité traite des données à caractère personnel à des fins autres que celles prévues dans la présente directive, le règlement (UE) 2016/679 s'applique. Par conséquent, le règlement (UE) 2016/679 s'applique lorsqu'un organisme ou une entité recueille des données à caractère personnel à d'autres fins et les traite ultérieurement pour respecter une obligation légale à laquelle il est soumis. Par exemple, les établissements financiers conservent, à des fins de détection ou de poursuites d'infractions pénales ou d'enquêtes en la matière, certaines données à caractère personnel qu'ils traitent et qu'ils ne transmettent aux autorités nationales compétentes que dans des cas spécifiques et conformément au droit des États membres. Un organisme ou une entité qui traite des données à caractère personnel pour le compte de ces autorités dans le cadre du champ d'application de la présente directive devrait être lié par un contrat ou un autre acte juridique et par les dispositions applicables aux sous-traitants en vertu de la présente directive, le règlement (UE) 2016/679 continuant de s'appliquer aux traitements de données à caractère personnel par le sous-traitant en dehors du champ d'application de la présente directive ».

Le considérant 34 de la directive « police » précise aussi :

« […] Lorsque des données à caractère personnel ont été initialement collectées par une autorité compétente pour l'une des finalités prévues par la présente directive, le règlement (UE) 2016/679 devrait s'appliquer au traitement de ces données à des fins autres que celles prévues par la présente directive lorsqu'un tel traitement est autorisé par le droit de l'Union ou le droit d'un État membre. En particulier, les règles fixées dans le règlement (UE) 2016/679 devraient s'appliquer au transfert de données à caractère personnel à des fins ne relevant pas du champ d'application de la présente directive. Le règlement (UE) 2016/679 devrait s'appliquer au traitement de données à caractère personnel par un destinataire qui n'est pas une autorité compétente ou qui n'agit pas en cette qualité au sens de la présente directive et auquel une autorité compétente communique de manière licite des données à caractère personnel […] ».

B.19.3.1. La loi du 25 décembre 2016 organise la collecte et le transfert des données « PNR », la création d'une banque de données des passagers, gérée par l' « Unité d'information des passagers » (ci-après : l'UIP), les finalités du traitement de cette banque de données et l'accès à cette dernière.

La loi du 25 décembre 2016 transpose essentiellement la directive « PNR », mais elle a aussi, comme l'indique son article 2, un contenu qui va au-delà de la transposition de cette directive.

B.19.3.2. Dans son avis n° 1/15 du 26 juillet 2017 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, la Cour de justice a considéré que les dispositions de cet accord poursuivaient deux finalités, de sorte que l'accord projeté possédait « une double composante, l'une concernant la nécessité d'assurer la sécurité publique et l'autre concernant la protection des données PNR » (CJUE, grande chambre, 26 juillet 2017, avis n° 1/15, point 90). Au regard de ces deux composantes, qui sont liées de façon indissociable et qui doivent être considérées toutes les deux comme présentant un caractère essentiel (*ibid.*, point 94), la Cour de justice a considéré que la décision du Conseil relative à la conclusion de l'accord envisagé devrait être fondée tant sur l'article 16, paragraphe 2, que sur l'article 87, paragraphe 2, sous a), du TFUE, « à moins qu'une telle combinaison de bases juridiques ne soit exclue » parce que les procédures prévues pour l'une et l'autre de ces bases sont incompatibles (*ibid.*, point 104).

Des dispositions organisant la collecte, le transfert et le traitement de données « PNR » peuvent dès lors relever tant de la protection des données (article 16 du TFUE) que de la coopération policière (article 87 du TFUE).

B.19.3.3. Le considérant 5 de la directive « PNR » indique que les objectifs de cette directive sont « entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes ».

Le considérant 38 de la directive « PNR » indique toutefois que les objectifs de la directive sont « le transfert de données PNR par les transporteurs aériens et leur traitement aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière », ce qui pourrait conférer à ces objectifs un caractère prépondérant sur celui de la protection des données.

B.19.4. La Cour constate par ailleurs que l'article 15, alinéa 1er, de la loi du 30 juillet 2018 dispose :

« En application de l'article 23 du Règlement, les articles 12 à 22 et 34 du Règlement, ainsi que le principe de transparence du traitement visé à l'article 5 du Règlement, ne s'appliquent pas aux traitements de données à caractère personnel par l'Unité d'information des passagers, tels que visés au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers ».

Cette disposition n'exclut donc pas l'intégralité de la loi du 25 décembre 2016 du champ d'application de l'article 23 du RGPD.

B.19.5. Afin, dès lors, de déterminer si les exigences contenues dans l'article 23 du RGPD s'appliquent à la loi du 25 décembre 2016, qui, comme il est dit en B.2.2, transpose, entre autres et principalement, la directive « PNR », il convient de poser à la Cour de justice de l'Union européenne la première question préjudicielle formulée dans le dispositif.

B.19.6. Pour le surplus, l'exception d'irrecevabilité soulevée par le Conseil des ministres est liée à la portée de la loi du 25 décembre 2016, de sorte que son examen se confond avec celui du fond.

En ce qui concerne l'ordre d'examen des griefs

B.20. Il ressort de l'examen du premier moyen et des dispositions attaquées que la partie requérante critique plusieurs aspects de la loi du 25 décembre 2016, que la Cour examine dans l'ordre suivant :

1. les modalités d'exécution de la loi du 25 décembre 2016 (articles 3, § 2 et 7, § 3);

COPIE NON CORRIGÉE

2. les notions de « documents d'identité » et de « documents de voyage » (article 7, §§ 1er et 2);

3. les données visées (articles 4, 9°, et 9);

4. la notion de « passager » (article 4, 10°);

5. les finalités du traitement des données « PNR » (article 8);

6. la gestion de la banque de données des passagers et le traitement des données dans le cadre de l'évaluation préalable des passagers et des recherches ponctuelles (articles 12 à 16 et 24 à 27 et articles 50 et 51);

7. la durée de conservation des données PNR (article 18).

1. *Les modalités d'exécution de la loi du 25 décembre 2016 (articles 3, § 2 et 7, § 3)*

B.21. La partie requérante estime tout d'abord qu'en confiant au Roi le soin de déterminer des éléments essentiels, les articles 3, § 2, et 7, § 3, de la loi du 25 décembre 2016 violent le principe de légalité garanti par les dispositions visées au moyen.

B.22.1. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout justiciable qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

COPIE NON CORRIGÉE

B.22.2. Outre l'exigence de légalité formelle, l'article 22 de la Constitution impose également que l'ingérence dans l'exercice du droit au respect de la vie privée soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la Convention européenne des droits de l'homme implique que sa formulation soit assez précise pour que chacun puisse - en s'entourant au besoin de conseils éclairés - prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 55; grande chambre, 17 février 2004, *Maestri c. Italie*, § 30). La législation doit donner à chacun une indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention (CEDH, grande chambre, 12 juin 2014, *Fernández Martínez c. Espagne*, § 117).

B.22.3. Il découle dès lors de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution qu'il doit être prévu de manière suffisamment précise dans quelles circonstances un traitement de données à caractère personnel est autorisé (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 57; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 99).

Le niveau requis de précision de la législation concernée - laquelle ne peut du reste parer à toute éventualité - dépend notamment, selon la Cour européenne des droits de l'homme, du domaine qu'elle est censée couvrir et du nombre et de la qualité de ses destinataires (CEDH, grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 95 et 96). Ainsi, la Cour européenne des droits de l'homme a jugé que l'exigence de prévisibilité dans des domaines liés à la sécurité nationale ne pouvait avoir la même portée que dans d'autres domaines (CEDH, 26 mars 1987, *Leander c. Suède*, § 51; 8 juin 2006, *Lupsa c. Roumanie*, § 33).

COPIE NON CORRIGÉE

B.22.4. La Cour de justice considère également que « l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné » (CJUE, 17 décembre 2015, C-419/14, *WebMindLicenses*, point 81; grande chambre, 26 juillet 2017, avis 1/15, point 139).

B.23.1. Les dispositions attaquées habilitent le Roi à déterminer par arrêté délibéré en Conseil des ministres, par secteur de transport et pour les opérateurs de voyage, d'une part, les données des passagers à transmettre et leurs modalités de transmission, après avis de la Commission de la protection de la vie privée, devenue l'Autorité de protection des données (article 3, § 2) et, d'autre part, les modalités relatives à l'obligation, pour les transporteurs et opérateurs de voyage, de s'assurer que ces données, dont ils disposent, sont complètes, exactes et actuelles, en vérifiant la correspondance entre les documents de voyage et l'identité du passager concerné (article 7, § 3).

Ces mesures constituent, comme il est dit en B.17.4.4, une ingérence dans le droit au respect de la vie privée et familiale.

B.23.2. Toute personne doit savoir de manière suffisamment précise les circonstances et conditions dans lesquelles une ingérence dans sa vie privée est autorisée, en particulier en ce qui concerne le traitement automatisé de données à caractère personnel. Toute personne doit dès lors avoir une idée suffisamment claire des données traitées, des personnes concernées par ce traitement de données et des conditions et finalités dudit traitement.

B.23.3. Il convient d'examiner si, eu égard aux différents éléments contenus dans la loi du 25 décembre 2016, toute personne concernée par la collecte, le transfert et le traitement des données « PNR » peut savoir de manière suffisamment précise quand et dans quelles conditions cette collecte, ce transfert et ce traitement sont autorisés, le cas échéant, selon des modalités techniques déterminées par le Roi.

COPIE NON CORRIGÉE

B.24.1. L'article 4, 9°, de la loi du 25 décembre 2016 définit le « PNR » comme étant « le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations visées à l'article 9, nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs et les opérateurs de voyage concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs (utilisés pour contrôler les passagers lors de l'embarquement) ou des systèmes équivalents offrant les mêmes fonctionnalités ».

En ce qui concerne les données d'enregistrement et d'embarquement, les données préalables (données « API » – *Advanced Passenger Information*) visées à l'article 9, § 1er, 18°, sont exhaustivement énumérées aux seize points de l'article 9, § 2, de la loi du 25 décembre 2016.

En ce qui concerne les données de réservation, les données des passagers (données « PNR » – *Passenger Name Record*) comprennent au maximum les dix-neuf éléments exhaustivement énumérés à l'article 9, § 1er, de la loi du 25 décembre 2016, parmi lesquels les données « API » visées à l'article 9, § 1er, 18°.

B.24.2. En vertu de l'article 5 de la loi du 25 décembre 2016, les données « PNR » sont collectées par les transporteurs et opérateurs de voyage et transmises en vue de leur enregistrement dans la banque de données des passagers visée à l'article 15 et gérée par l'UIP créée au sein du Service public fédéral Intérieur (articles 12 et suivants). Les passagers sont informés que leurs données sont transmises à l'UIP et que ces données peuvent être traitées ultérieurement pour les finalités visées à l'article 8 (article 6).

Les finalités du traitement des données « PNR » sont énumérées dans l'article 8 de la loi du 25 décembre 2016 : il s'agit, d'une part, de la recherche et de la poursuite d'infractions (article 8, § 1er) et, d'autre part, aux conditions prévues au chapitre 11, de l'amélioration des contrôles des personnes aux frontières extérieures et de la lutte contre l'immigration illégale (article 8, § 2).

COPIE NON CORRIGÉE

Dans le cadre des finalités visées à l'article 8, § 1er, l'article 16 de la loi du 25 décembre 2016 prévoit l'accès direct de l'UIP à la banque de données des passagers pour les traitements visés aux articles 24 à 27, conformément aux dispositions prévues au chapitre 9.

Dans le cadre des finalités visées à l'article 8, § 2, seules sont transmises les données des passagers visées à l'article 9, § 1er, 18° (données « API ») qui concernent les catégories de passagers visées à l'article 29, § 2, de la loi du 25 décembre 2016.

La durée de conservation des données est fixée par les articles 18 et suivants de la loi du 25 décembre 2016.

B.24.3. Compte tenu de ce qui précède, la loi du 25 décembre 2016 contient les éléments de définition des données traitées, des personnes concernées par ce traitement de données et des conditions et finalités dudit traitement.

Il convient maintenant d'examiner les délégations contenues dans les articles 3, § 2, et 7, § 3, de la loi du 25 décembre 2016.

a) Article 3, § 2, de la loi du 25 décembre 2016

B.25.1. En ce qui concerne le champ d'application de la loi du 25 décembre 2016, les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« La directive européenne PNR prévoit la collecte de données des passagers en premier lieu pour le trafic aérien. Elle laisse explicitement la possibilité aux États membres d'imposer cette obligation à d'autres transporteurs. Les États membres peuvent donc adopter une réglementation nationale visant d'autres modes de transport.

COPIE NON CORRIGÉE

La directive européenne PNR prévoit explicitement la possibilité pour les États membres d'établir, en vertu de leur droit national, et dans le respect des principes fondamentaux de l'Union, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des opérateurs de voyage qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne.

Le projet de loi prévoit dans ce sens l'obligation légale pour les opérateurs de voyage de transmettre les données des passagers à la banque de données des passagers » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 8).

B.25.2.1. L'article 3, § 2, de la loi du 25 décembre 2016, tel qu'il a été modifié par l'article 2 de la loi du 2 mai 2019, dispose :

« Le Roi détermine par arrêté délibéré en Conseil des ministres par secteur de transport et pour les opérateurs de voyage, les données des passagers à transmettre et leurs modalités de transmission, après avis de l'autorité compétente de contrôle des traitements de données à caractère personnel ».

B.25.2.2. En ce qui concerne cette disposition, les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« L'article trois a pour seule ambition de définir d'emblée le champ d'application de la loi vis-à-vis des transporteurs professionnels de passagers et des opérateurs de voyage. Les transporteurs et les opérateurs de voyage ne doivent pas recueillir plus de données que celles dont ils disposent.

Afin de tenir compte au maximum de la spécificité de chaque secteur de transport ainsi que des opérateurs, un arrêté royal déterminera, après avis de la Commission pour la protection de la vie privée, pour chaque secteur quelles données des passagers précisément (mentionnées à l'article 9) devront être transmises et selon quelles modalités.

La délégation importante faite au Roi s'explique par les spécificités des divers secteurs de transport. La rédaction des AR veillera à répondre au respect des principes de pertinence, de proportionnalité par rapport aux objectifs de la loi et d'égalité de traitement entre les agents économiques des différents secteurs de transport, souligné par le CE » (*ibid.*, p. 15).

B.25.2.3. En ce qui concerne l'habilitation contenue dans l'article 3, § 2, de la loi du 25 décembre 2016, la section de législation du Conseil d'État a émis les observations suivantes :

COPIE NON CORRIGÉE

« L'habilitation conférée au Roi ne concerne donc, dans la mise en œuvre de l'article 3, que la détermination des données qui, parmi celles prévues à l'article 9 de l'avant-projet, doivent être transmises par les transporteurs en fonction du secteur dont ils relèvent.

Il en résulte que ce n'est qu'au moment où le ou les projets d'arrêté royal auront été élaborés que pourra être opéré un contrôle du caractère nécessaire, adéquat, pertinent et proportionnel au regard des finalités, des données personnelles des passagers que le transporteur devra collecter et transmettre. En l'état actuel du dispositif, la section de législation n'est pas en mesure de se livrer à un tel contrôle.

Il en va de même en ce qui concerne le respect du principe d'égalité qui devra être assuré entre les agents économiques actifs dans les différents secteurs du transport ainsi qu'entre les passagers lors de l'adoption de cet ou ces arrêtés royaux. Sur ce point également, la section de législation ne dispose pas, à ce moment, d'éléments suffisants pour se prononcer en connaissance de cause » (*ibid.*, p. 92).

B.26.1. L'article 3, § 2, de la loi du 25 décembre 2016 habilite le Roi à déterminer, par secteur de transport et pour les opérateurs de voyage, les données des passagers à transmettre et les modalités de leur transmission.

Conformément à l'article 3, § 2, de la loi du 25 décembre 2016, l'avis de la Commission de la protection de la vie privée, devenue l'Autorité de protection des données, est requis pour l'adoption de l'arrêté royal déterminant, par secteur de transport et pour les opérateurs de voyage, les données des passagers à transmettre et les modalités de leur transmission.

B.26.2. L'habilitation contenue dans l'article 3, § 2, de la loi du 25 décembre 2016 permet tout d'abord d'adapter les obligations prévues par la loi du 25 décembre 2016 par secteur de transport et pour les opérateurs de voyage, auxquels la loi du 25 décembre 2016 est rendue applicable.

Comme il est dit en B.2.2 et B.25.1, la directive « PNR » vise essentiellement le secteur aérien, mais les États membres sont libres d'étendre le système « PNR » à d'autres secteurs de transport. Comme il est dit en B.7 à B.10, les arrêtés royaux des 18 juillet 2017 et 3 février 2019 ont respectivement rendu la loi du 25 décembre 2016 applicable aux compagnies aériennes, aux transporteurs par bus et aux transporteurs « HST » et distributeurs de tickets « HST.

COPIE NON CORRIGÉE

Le chapitre 1er de l'arrêté royal du 18 juillet 2017 précise qu'il transpose partiellement la directive « API » et la directive « PNR ». Après une définition des termes utilisés dans celui-ci (chapitre 2 de l'arrêté royal du 18 juillet 2017 et chapitre 1er des arrêtés royaux du 3 février 2019), sont définies les modalités relatives aux obligations respectives des compagnies aériennes, des transporteurs par bus et des transporteurs « HST » et distributeurs de tickets « HST » (chapitre 3 de l'arrêté royal du 18 juillet 2017 et chapitre 2 des arrêtés royaux du 3 février 2019), les modalités de transmission des données des passagers (chapitre 4 de l'arrêté royal du 18 juillet 2017 et chapitre 3 des arrêtés royaux du 3 février 2019), et la date de l'entrée en vigueur de la loi du 25 décembre 2016 à l'égard du secteur de transport visé (chapitre 5 de l'arrêté royal du 18 juillet 2017 et chapitre 4 des arrêtés royaux du 3 février 2019).

B.26.3. La partie requérante ne critique pas le fait que l'habilitation contenue dans l'article 3, § 2, de la loi du 25 décembre 2016 permette au Roi de viser différents secteurs de transport, mais uniquement le fait que cette habilitation porte sur les données des passagers et sur les modalités de leur transmission.

B.26.4.1. En ce qui concerne la critique portant sur les données concernées, l'habilitation contenue dans l'article 3, § 2, de la loi du 25 décembre 2016 ne porte toutefois que sur la sélection des données des passagers à transmettre, par secteur de transport et pour les opérateurs de voyage, parmi les données des passagers qui sont légalement et exhaustivement énumérées à l'article 9 de la loi du 25 décembre 2016.

C'est d'ailleurs ce que la section de législation du Conseil d'État a considéré :

« L'habilitation conférée au Roi ne concerne donc, dans la mise en œuvre de l'article 3, que la détermination des données qui, parmi celles prévues à l'article 9 de l'avant-projet, doivent être transmises par les transporteurs en fonction du secteur dont ils relèvent » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 92).

De même, la Commission de la protection de la vie privée a considéré :

COPIE NON CORRIGÉE

« La Commission fait remarquer par ailleurs que si l'article 3, § 2 de la loi PNR prévoit que les données des passagers à transmettre sont déterminées par arrêté royal, ces données sont établies – à juste titre – directement dans la loi, à l'article 9 de la loi PNR. Ces données sont d'ailleurs issues de l'annexe 1 de la directive PNR à laquelle renvoient les articles 6 et 8 de cette directive » (Commission de la protection de la vie privée, avis n° 23/2017 du 24 mai 2017, point 10; voy. aussi Autorité de protection des données, avis n° 85/2018 du 26 septembre 2018, point 12).

Le Roi ne pourrait donc pas prévoir la transmission de données nouvelles, non reprises à l'article 9 de la loi du 25 décembre 2016 (voy., en ce sens, Autorité de protection des données, avis n° 85/2018 du 26 septembre 2018, point 15).

B.26.4.2. L'habilitation contenue dans l'article 3, § 2, de la loi du 25 décembre 2016 permet par ailleurs au Roi de déterminer, par secteur de transport et pour les opérateurs de voyage, les modalités de transmission des données des passagers.

Cette habilitation ne concerne donc que des aspects purement techniques de la transmission des données des passagers.

L'arrêté royal du 18 juillet 2017 précise la méthode et les moments de transfert des données des passagers par les compagnies aériennes. Cet arrêté royal organise la méthode « *push* » – méthode retenue dans l'article 8 de la directive « PNR », selon laquelle les compagnies aériennes transmettent les données « PNR » à l'autorité compétente sans que, comme dans la méthode « *pull* », celle-ci doive les extraire du système de réservation –, qui est prévue pour le transfert des données des passagers vers la banque de données des passagers. Les travaux préparatoires de la loi du 25 décembre 2016 avaient d'ailleurs indiqué que cette méthode « *push* » « offre un meilleur niveau de protection des données » et « doit donc être préférée » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 16). Pour le surplus, les formats de données et les protocoles de transmission devant être utilisés par les transporteurs aériens sont fixés dans la décision d'exécution (UE) 2017/759 de la Commission du 28 avril 2017 « sur les protocoles communs et formats de données devant être utilisés par les transporteurs aériens lors d'un transfert de données PNR aux unités d'information passagers ».

COPIE NON CORRIGÉE

Les arrêtés royaux du 3 février 2019 prévoient la méthode et les moments de transfert des données respectivement par les transporteurs par bus et par les transporteurs « HST » et distributeurs de tickets « HST ». Ces arrêtés royaux prévoient que le format des données, le protocole de transmission et l'organisation technique de la transmission seront définis dans le protocole d'accord conclu entre le fonctionnaire dirigeant de l'UIP et le transporteur/opérateur de voyage concerné.

Enfin, les arrêtés royaux des 18 juillet 2017 et 3 février 2019 prévoient que les données sont transférées 48 heures avant l'heure de départ programmée et dès que les passagers ont embarqué à bord de l'avion, du bus ou du train à grande vitesse prêt à partir, dans des conditions de sécurisation des données. Le rapport au Roi qui a précédé l'arrêté royal du 18 juillet 2017 précise que cela « n'empêche d'aucune manière les réservations de dernière minute et les changements de dernière minute, puisque l'information la plus actuelle est envoyée lors du deuxième transfert » (*Moniteur belge* du 28 juillet 2017, p. 75934).

B.26.5. L'habilitation contenue dans l'article 3, § 2, de la loi du 25 décembre 2016 permet donc d'identifier les données des passagers parmi les données légalement fixées dans l'article 9 de la loi du 25 décembre 2016 et de déterminer les modalités de transmission des données « PNR » en fonction des spécificités de chaque secteur de transport auquel la loi du 25 décembre 2016 est rendue applicable.

Comme il est dit en B.22.1, pareille délégation n'est pas contraire au principe de légalité contenu dans l'article 22 de la Constitution, dès lors que cette habilitation porte uniquement sur l'exécution de mesures dont les éléments essentiels ont été déterminés par le législateur, ainsi qu'il a été exposé en B.24.

Le cas échéant, il appartient au juge compétent d'examiner si l'utilisation, faite par le Roi, de cette habilitation est conforme aux dispositions constitutionnelle et conventionnelles invoquées au moyen, telles qu'elles ont été précisées en B.22.

COPIE NON CORRIGÉE

b) Article 7, § 3, de la loi du 25 décembre 2016

B.27.1. L'article 7 de la loi du 25 décembre 2016 dispose :

« § 1er. Les transporteurs transmettent les données des passagers visées à l'article 9, § 1er, dont ils disposent, et s'assurent que les données de passagers visées à l'article 9, § 1er, 18°, dont ils disposent, sont complètes, exactes et actuelles. À cette fin, ils vérifient la correspondance entre les documents de voyage et l'identité du passager concerné.

§ 2. Les opérateurs de voyage transmettent les données des passagers visées à l'article 9, § 1er, dont ils disposent, et s'assurent que les données des passagers visées à l'article 9, § 1er, 18°, dont ils disposent, sont complètes, exactes et actuelles. A cette fin, ils prennent toutes les mesures nécessaires afin de vérifier la correspondance entre les documents de voyage et l'identité du passager concerné.

§ 3. Le Roi détermine par arrêté délibéré en Conseil des ministres par secteur de transport et pour les opérateurs de voyage, les modalités relatives à l'obligation prévue aux §§ 1er et 2 ».

B.27.2.1. En ce qui concerne cette disposition, les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« L'incident dans le Thalys a à nouveau démontré à quel point il est important de pouvoir retracer les déplacements de certains individus. L'obligation d'émettre un titre de transport nominatif a peu de sens si les instances compétentes ne vérifient même pas que la bonne personne effectue son voyage au moyen de ce titre de transport. Ce manque de contrôle a également pour conséquence que nos services ne savent même pas si des individus suspects figurant sur une liste, prennent l'avion ou le train, le bus ou le bateau pour effectuer un voyage international.

Il n'existe aucune obligation européenne qui impose aux transporteurs de contrôler la correspondance entre l'identité et le titre de transport. Neuf États membres européens imposent néanmoins cette obligation légale, entre autres aux compagnies aériennes (entre autres le Portugal, l'Espagne, l'Italie, la Grèce, la Bulgarie, la Hongrie et la Roumanie).

La législation belge ne prévoyait pas jusqu'à présent cette obligation. Il va de soi que l'obligation de transmettre les données des passagers, dont disposent les transporteurs et les opérateurs de voyage, doit pouvoir s'appuyer sur une obligation de vérifier la conformité des documents.

Cette obligation tient compte des spécificités des transporteurs et opérateurs de voyage. Dans cette optique, les opérateurs de voyage seront soumis à une obligation de moyen.

COPIE NON CORRIGÉE

L'identité du passager peut être déterminée sur la base d'un document authentique qui est accepté dans le pays d'origine du passager concerné en tant que document d'identité valide. Ceci pour ne pas créer une limitation à la libre circulation des personnes au sein de l'espace Schengen » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, pp. 16-17).

Le ministre de la Sécurité et de l'Intérieur a également précisé que « le contrôle de la validité des documents d'identité ne relève pas de [la] responsabilité [des transporteurs et opérateurs de voyage] » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/003, p. 24).

B.27.2.2. En ce qui concerne l'habilitation contenue dans l'article 7, § 3, de la loi du 25 décembre 2016, la section de législation du Conseil d'État a émis les observations suivantes :

« Cette obligation nouvelle imposée aux transporteurs, en dehors de tout dispositif européen contraignant, *a fortiori* lorsqu'elle concerne également les opérateurs de voyage qui ne sont pas visés par la directive 2016/681/UE 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 ' (ci-après : ' la directive 2016/681/UE ') doit, dans son principe et ses modalités, respecter l'article 22 de la Constitution et la loi du 8 décembre 1992. En l'état actuel du dossier soumis à la section de législation, ce contrôle n'a pu être effectué quant aux modalités de l'obligation nouvelle prévue par l'article 6, § 3, de l'avant-projet pas plus que celui relatif au respect du principe d'égalité garanti par les articles 10 et 11 de la Constitution » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 93).

B.28.1. En vertu de l'article 7, § 3, de la loi du 25 décembre 2016, le Roi détermine par arrêté délibéré en Conseil des ministres, par secteur de transport et pour les opérateurs de voyage, les modalités relatives à l'obligation pour les transporteurs et opérateurs de voyage de transmettre les données « PNR » (article 9, § 1er) dont ils disposent, mais aussi de s'assurer que les données « API » (article 9, § 1er, 18°) sont « complètes, exactes et actuelles », en vérifiant « la correspondance entre les documents de voyage et l'identité du passager concerné ».

COPIE NON CORRIGÉE

Cette obligation vise à assurer l'efficacité du système de collecte et de transfert des données des passagers à la banque de données des passagers, dont le principe est posé par l'article 5 de la loi du 25 décembre 2016 pour les transporteurs et opérateurs de voyage.

B.28.2. Cette disposition habilite donc le Roi à organiser les modalités selon lesquelles les transporteurs et opérateurs de voyage vérifient l'exactitude des données préalables d'enregistrement et d'embarquement. Comme l'indiquent les travaux préparatoires, cette disposition ne crée qu'une obligation de moyen.

B.28.3. L'habilitation au Roi contenue dans l'article 7, § 3, de la loi du 25 décembre 2016 tend à adapter les modalités de cette vérification de l'exactitude des données en fonction des spécificités de chaque secteur de transport.

Le rapport au Roi qui a précédé l'arrêté royal du 18 juillet 2017 expose à ce sujet :

« Le contrôle de conformité, décrit à l'article 4 du présent arrêté royal, vise à vérifier si la personne qui dispose du document de voyage pour un transport précis est effectivement la personne qui monte à bord de l'avion. Ceci se fera en comparant le nom et le prénom mentionnés sur le document de voyage avec le nom et le prénom sur le document d'identité. Le transfert des données des passagers et le traitement de celles-ci n'ont aucun sens s'il n'existe aucune certitude que les passagers sont bien montés à bord de l'avion. L'exécution du contrôle de conformité contribue à l'exactitude des données.

Enfin, si les compagnies aériennes constatent que les données visées à l'article 9, § 1er, 18° de la loi dont elles disposent, ne sont pas actuelles, pas exactes ou incomplètes, elles prennent les mesures nécessaires afin de corriger ces données au plus tard au moment du deuxième transfert. Il faut entendre par données des passagers comme visées à l'article 9, § 1er, 18° de la loi, les données énumérées à l'article 9, § 2, de la loi, à savoir les données d'enregistrement et d'embarquement, transférées par les compagnies aériennes lorsqu'elles en disposent. Les données visées à l'article 9, § 1er, 18°, visent aussi les champs similaires repris dans le même paragraphe (comme le nom et le prénom à l'article 9, § 1er, 4° de la loi) » (*Moniteur belge* du 28 juillet 2017, pp. 75934-75935).

COPIE NON CORRIGÉE

En vertu de l'arrêté royal du 18 juillet 2017 et des arrêtés royaux du 3 février 2019, ce contrôle de conformité est effectué au moment où les passagers embarquent à bord de l'avion, du train à grande vitesse ou du bus. Si les transporteurs concernés constatent que les données « API » dont ils disposent ne sont pas actuelles, exactes ou complètes, ils prennent toutes les mesures nécessaires pour corriger ces données au plus tard au moment du second transfert qui a lieu dès que les passagers du vol ont embarqué à bord du bus ou du train à grande vitesse.

B.28.4. L'habilitation contenue dans l'article 7, § 3, de la loi du 25 décembre 2016 ne concerne donc que les aspects techniques d'une obligation qui avait été prévue dans la loi du 25 décembre 2016.

B.28.5. Comme il est dit en B.22.1, pareille délégation n'est pas contraire au principe de légalité contenu dans l'article 22 de la Constitution, dès lors que cette habilitation porte uniquement sur l'exécution de mesures dont les éléments essentiels ont été déterminés par le législateur, ainsi qu'il a été exposé en B.24.

Le cas échéant, il appartient au juge compétent d'examiner si l'utilisation, faite par le Roi, de cette habilitation est conforme aux dispositions constitutionnelle et conventionnelles invoquées au moyen, telles qu'elles ont été précisées en B.22.

B.29. En ce qu'il est dirigé contre les articles 3, § 2, et 7, § 3, de la loi du 25 décembre 2016, le moyen n'est pas fondé.

2. *Les notions de « documents d'identité » et de « documents de voyage » (article 7, §§ 1er et 2)*

B.30. La partie requérante critique également l'absence de définition légale des notions de « documents d'identité » et de « documents de voyage », visées à l'article 7, §§ 1er et 2, de la loi du 25 décembre 2016.

COPIE NON CORRIGÉE

B.31.1. Le fait que la loi du 25 décembre 2016 ne contient pas de définition légale des notions de « documents d'identité » et de « documents de voyage » ne signifie pas que le principe de légalité soit violé, pour autant que ces notions ne créent pas d'insécurité juridique.

B.31.2. Il ressort tout d'abord des travaux préparatoires de la loi du 25 décembre 2016 que le législateur envisageait les « documents d'identité » de manière large, considérant que l'identité du passager « peut être déterminée sur la base d'un document authentique qui est accepté dans le pays d'origine du passager concerné en tant que document d'identité valide » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 17).

Ces travaux préparatoires permettent donc d'éclairer la notion de « documents d'identité » comme une notion large, qui ne s'écarte pas de son acception usuelle dans le pays d'origine du passager.

B.31.3. Cette approche est d'ailleurs confirmée par les arrêtés royaux des 18 juillet 2017 et 3 février 2019, qui définissent de la même manière les « documents d'identité » comme étant les « documents, établis par une autorité officielle, sur base desquels l'identité des passagers peut être définie, à savoir les cartes d'identité nationales, les passeports internationalement reconnus ou les documents remplaçants légaux » (article 2, 3°, de l'arrêté royal du 18 juillet 2017 (transport aérien); article 1er, 6°, de l'arrêté royal du 3 février 2019 (transport HST) et article 1er, 4°, de l'arrêté royal du 3 février 2019 (transport par bus)).

B.32.1. En ce qui concerne les « documents de voyage », le législateur a pu considérer qu'une définition légale ne s'imposait pas, dès lors qu'il convenait, en l'espèce, de se référer à l'acception usuelle de cette notion, à savoir les documents conférant au passager un « titre de transport », qui lui permette d'emprunter le moyen de transport concerné conformément à la pratique propre à chaque secteur de transport concerné.

B.32.2. Les définitions contenues dans les arrêtés royaux des 18 juillet 2017 et 3 février 2019 confirment cette approche.

COPIE NON CORRIGÉE

Ainsi, l'article 2, 4°, de l'arrêté royal du 18 juillet 2017 définit les « documents de voyage » comme étant les « documents qui octroient au passager un titre pour le transport visé à l'article 4, 3° [,] de la loi », soit le transport par voie aérienne. De même, les arrêtés royaux du 3 février 2019 définissent les « documents de voyage » comme étant les documents qui octroient au passager un titre pour le transport visé, respectivement, aux 4° et 5° de l'article 4 de la loi du 25 décembre 2016, soit le transport par voie terrestre et le transport par voie ferroviaire.

B.33. En ce qu'il est dirigé contre l'article 7, §§ 1er et 2, le moyen n'est pas fondé.

3. *Les données visées (articles 4, 9°, et 9)*

B.34. La partie requérante estime tout d'abord que le champ d'application très large relatif aux données des passagers visées aux articles 4, 9°, et 9, de la loi du 25 décembre 2016 est manifestement disproportionné eu égard à l'objectif poursuivi. La partie requérante estime qu'il conviendrait, à tout le moins, de limiter la catégorie des données visées à l'article 9, § 1er, 12°, de la loi attaquée.

En outre, les données visées pourraient, selon la partie requérante, révéler des données sensibles, telles que l'appartenance à une organisation syndicale, les affinités personnelles et les relations personnelles ou professionnelles.

B.35.1. Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise, mais aussi répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause.

COPIE NON CORRIGÉE

B.35.2. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment de la Convention n° 108 (CEDH, 25 février 1997, *Z c. Finlande*, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103).

Cette Convention n° 108 contient, entre autres, les principes relatifs au traitement de données à caractère personnel : licéité, loyauté, transparence, limitation des finalités, proportionnalité, exactitude, limitation de la conservation, intégrité et confidentialité, et responsabilité.

La même Convention est actualisée par un protocole d'amendement ouvert à signature le 10 octobre 2018.

B.35.3. Une ingérence dans l'exercice du droit au respect de la vie privée par un traitement de données à caractère personnel, en l'occurrence par un accès et par l'utilisation par les services publics de certaines données personnelles au moyen de techniques particulières (CEDH, 26 mars 1987, *Leander c. Suède*, § 48; grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 46; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*) doit donc reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur.

B.35.4. En ce qui concerne la proportionnalité, la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne tiennent compte de l'existence ou non, dans la réglementation visée, des garanties matérielles et procédurales mentionnées en B.22.2.

Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient dès lors de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées, du caractère distinctif de la réglementation et de la présence ou de l'absence de garanties visant à éviter l'usage

COPIE NON CORRIGÉE

inapproprié et abusif, par les services publics, des données à caractère personnel traitées (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 59; décision, 29 juin 2006, *Weber et Saravia c. Allemagne*, § 135; 28 avril 2009, *K.H. e.a. c. Slovaquie*, §§ 60-69; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K. c. France*, §§ 37 et 42-44; 18 septembre 2014, *Brunet c. France*, §§ 35-37; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, § 68; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*, points 56-66).

B.35.5. Dans son avis n° 1/15 du 26 juillet 2017, la Cour de justice a également rappelé qu'une ingérence dans le droit à la protection des données à caractère personnel doit être limitée au « strict nécessaire » :

« 140. S'agissant du respect du principe de proportionnalité, la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (arrêts du 16 décembre 2008, *Satakunnan Markkinapörssi* et *Satamedia*, C-73/07, EU:C:2008:727, point 56; du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU:C:2014:238, points 51 et 52; du 6 octobre 2015, *Schrems*, C-362/14, EU:C:2015:650, point 92, ainsi que du 21 décembre 2016, *Tele2 Sverige* et *Watson e.a.*, C-203/15 et C-698/15, EU:C:2016:970, points 96 et 103).

141. Pour satisfaire à cette exigence, la réglementation en cause comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière des données à caractère personnel que sont les données sensibles (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, *Tele2 Sverige* et *Watson e.a.*, C-203/15 et C-698/15, EU:C:2016:970, points 109 et 117; voir, en ce sens, Cour EDH, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, CE:ECHR:2008:1204JUD003056204, § 103) ».

COPIE NON CORRIGÉE

B.36.1. L'article 4, 9°, de la loi du 25 décembre 2016 définit le « PNR » comme étant « le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations visées à l'article 9 ». Comme il est dit en B.24.1, l'article 9 de la loi du 25 décembre 2016 distingue, d'une part, les données préalables d'enregistrement et d'embarquement (données « API ») visées à l'article 9, § 1er, 18°, qui sont exhaustivement énumérées dans l'article 9, § 2, de la loi du 25 décembre 2016, et, d'autre part, les données de réservation (données « PNR »), qui comprennent au maximum les 19 éléments exhaustivement énumérés à l'article 9, § 1er, de la loi du 25 décembre 2016, dont les données « API » visées à l'article 9, § 1er, 18°.

La distinction entre les données « API » et les données « PNR » est explicitée dans les travaux préparatoires cités en B.3.1.

B.36.2.1. Les travaux préparatoires relatifs à l'article 9 de la loi du 25 décembre 2016 exposent :

« L'article 9 détermine les données des passagers qui devront être transmises. Ces données sont transmises par le biais d'un format de données imposé et uniforme par secteur de transport et opérateur de voyage pour lequel il est fait usage d'une norme acceptée au niveau international (pour les compagnies aériennes il s'agit par exemple du format PNRGOV, développé par IATA/ICAO/WCO).

L'article 9 fait une distinction entre, d'une part, les données de réservation prévues au § 1er et, d'autre part, les données d'enregistrement et d'embarquement mentionnées au § 2 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, pp. 20-21).

Cette distinction correspond à la distinction entre les données qui sont visées par la directive « API » et celles qui sont visées par la directive « PNR ».

B.36.2.2. Le transfert des données des passagers organisé par la loi du 25 décembre 2016 n'impose toutefois pas aux transporteurs et opérateurs de voyage de collecter des données autres que celles dont ils disposent déjà :

COPIE NON CORRIGÉE

« Les transporteurs et opérateurs de voyage collectent et traitent déjà les données de leurs passagers à des fins commerciales. En ce qui concerne, par exemple, les compagnies aériennes, celles-ci conservent aussi des données de passagers à remettre préalablement (données API) comme données PNR, mais ce n'est pas une généralité. Les données API sont, entre autres, les données lues par la ' *machine readable zone* ' du document d'identité. Conformément à la directive PNR, les transporteurs et opérateurs de voyage ne doivent transmettre que les données dont ils disposent et ne doivent pas recueillir ou conserver des données supplémentaires auprès des passagers. Ils ne devraient pas non plus obliger les passagers à communiquer des données en sus de celles qui leur sont déjà transmises » (*ibid.*, pp. 15-16).

Les considérants 8 et 9 de la directive « PNR » indiquent également, à ce sujet :

« (8) Les transporteurs aériens recueillent et traitent déjà des données PNR de leurs passagers pour leur propre usage commercial. La présente directive ne devrait pas leur imposer l'obligation de recueillir ou de conserver des données supplémentaires des passagers et ne devrait pas non plus contraindre les passagers à communiquer des données en sus de celles qui sont déjà transmises aux transporteurs aériens.

(9) Certains transporteurs aériens conservent les données API qu'ils recueillent en les regroupant avec les données PNR, alors que d'autres ne le font pas. L'utilisation combinée des données PNR et des données API présente une valeur ajoutée en ce qu'elle aide les États membres à vérifier l'identité d'une personne, renforçant ainsi la valeur du résultat en termes de prévention, de détection et de répression des infractions et réduisant au minimum le risque de soumettre des personnes innocentes à des vérifications et à des enquêtes. C'est pourquoi il est important de veiller à ce que, lorsque les transporteurs aériens recueillent des données API, ils les transfèrent, que les données API soient conservées ou non par des moyens techniques différents de ceux utilisés pour d'autres données PNR ».

B.37.1. En ce qui concerne les données « API », l'article 3, paragraphe 2, de la directive « API » prévoit que, parmi les renseignements relatifs aux passagers que les transporteurs aériens vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire d'un État membre, figurent les renseignements suivants :

« - le numéro et le type du document de voyage utilisé;

- la nationalité;

- le nom complet;

- la date de naissance;

- le point de passage frontalier utilisé pour entrer sur le territoire des États membres;

COPIE NON CORRIGÉE

- le code de transport;

- les heures de départ et d'arrivée du transport;

- le nombre total des personnes transportées;

- le point d'embarquement initial ».

B.37.2.1. Auparavant, les transporteurs aériens étaient déjà tenus de communiquer les données « API », conformément à l'arrêté royal du 11 décembre 2006, qui a été abrogé par l'article 10 de l'arrêté royal du 18 juillet 2017.

Les travaux préparatoires de la loi du 25 décembre 2016 confirment en effet :

« Le projet de loi reprend en substance le régime prévu par l'arrêté royal du 11 décembre 2006 concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers, mentionné plus haut. La liste des données ' API ' prévue par l'avant-projet de loi correspond donc en substance à celle établie par cet arrêté.

Toutefois, l'avant-projet de loi a un champ d'application plus large que celui de la directive 2004/82/CE car l'obligation faite aux transporteurs est généralisée à tous les secteurs de transport » (*ibid.*, p. 11).

B.37.2.2. Avant son abrogation par l'arrêté royal du 18 juillet 2017, l'article 3, § 2, de l'arrêté royal du 11 décembre 2006 visait comme renseignements à transmettre par les compagnies aériennes :

« 1° le numéro et le type du document de voyage utilisé;

2° la nationalité;

3° le nom complet;

4° la date de naissance;

5° le point de passage frontalier utilisé pour entrer sur le territoire belge;

6° le numéro de vol;

7° les heures de départ et d'arrivée du vol;

8° le nombre total des personnes transportées;

COPIE NON CORRIGÉE

9° le point d'embarquement initial ».

Cette liste de renseignements reprenait donc la liste minimale prévue par l'article 3, paragraphe 2, de la directive « API ».

B.38.1. En ce qui concerne les données « PNR », le considérant 15 de la directive « PNR » indique :

« Une liste des données PNR à transmettre à une UIP devrait être établie dans le but de refléter les exigences légitimes des pouvoirs publics en matière de prévention et de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, renforçant par-là la sécurité intérieure de l'Union et la protection des droits fondamentaux, notamment le respect de la vie privée et la protection des données à caractère personnel. À cette fin, il convient d'appliquer des normes élevées conformément à la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée ' Charte '), la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après dénommée ' convention n° 108 ') et la convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). Une telle liste ne devrait pas être fondée sur l'origine raciale ou ethnique, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne. Les données PNR ne devraient comporter que des informations relatives aux réservations et aux itinéraires de voyage des passagers qui permettent aux autorités compétentes d'identifier les passagers aériens représentant une menace pour la sécurité intérieure ».

B.38.2. Conformément à l'article 3, point 5), de la directive « PNR » on entend par « dossier(s) passager(s) » ou « PNR » « un dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs (utilisés pour contrôler les passagers lors de l'embarquement) ou des systèmes équivalents offrant les mêmes fonctionnalités ».

L'article 4, 9°, de la loi du 25 décembre 2016 reprend, dans des termes quasiment identiques, cette définition du dossier « PNR ».

B.38.3.1. L'annexe I de la directive « PNR », intitulée « Données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens », dispose :

COPIE NON CORRIGÉE

« 1. Code repère du dossier passager

2. Date de réservation/d'émission du billet

3. Date(s) prévue(s) du voyage

4. Nom(s)

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

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

7. Itinéraire complet pour le PNR concerné

8. Informations ' grands voyageurs '

9. Agence de voyages/agent de voyages

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

11. Indications concernant la scission/division du PNR

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

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

14. Numéro du siège et autres informations concernant le siège

15. Informations sur le partage de code

16. Toutes les informations relatives aux bagages

17. Nombre et autres noms de voyageurs figurant dans le PNR

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

COPIE NON CORRIGÉE

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

B.38.3.2. Le point 18 de l'annexe I de la directive « PNR » étend donc la notion de données « API », qui était visée à l'article 3, paragraphe 2, de la directive « API ».

B.39.1.1. En ce qui concerne les données de réservation, l'article 9, § 1er, de la loi du 25 décembre 2016 vise au maximum comme « données PNR » :

« En ce qui concerne les données de réservation, les données des passagers comprennent au maximum :

1° le code repère du PNR;

2° la date de réservation et d'émission du billet;

3° les dates prévues du voyage;

4° les noms, prénoms et la date de naissance;

5° l'adresse et les coordonnées (numéro de téléphone, adresse électronique);

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

7° l'itinéraire complet pour le passager concerné;

8° les informations relatives aux ' voyageurs enregistrés ', c'est-à-dire les grands voyageurs;

9° l'agence de voyage ou l'agent de voyage;

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

11° les indications concernant la scission ou la division du PNR;

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

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

COPIE NON CORRIGÉE

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

15° les informations sur le partage de code;

16° toutes les informations relatives aux bagages;

17° le nombre et les noms des autres voyageurs figurant dans le PNR;

18° toutes les données préalables sur les passagers (données API) qui ont été collectées et sont énumérées au § 2;

19° l'historique complet des modifications des données énumérées aux 1° à 18°; ».

B.39.1.2. Les données « PNR » visées à l'article 9, § 1er, de la loi du 25 décembre 2016 reprennent donc les données visées dans l'annexe I de la directive « PNR ».

B.39.2.1. En ce qui concerne les données préalables d'enregistrement et d'embarquement, l'article 9, § 2, de la loi du 25 décembre 2016 vise comme étant les « données API » :

« En ce qui concerne les données d'enregistrement et d'embarquement, les données préalables visées au § 1er, 18°, sont :

1° le type de document de voyage;

2° le numéro de document;

3° la nationalité;

4° le pays de délivrance du document;

5° la date d'expiration du document;

6° le nom de famille, le prénom, le sexe, la date de naissance;

7° le transporteur / opérateur de voyage;

8° le numéro du transport;

9° la date de départ, la date d'arrivée;

10° le lieu de départ, le lieu d'arrivée;

11° l'heure de départ, l'heure d'arrivée;

12° le nombre total de personnes transportées;

COPIE NON CORRIGÉE

13° le numéro de siège;

14° le code repère du PNR;

15° le nombre, le poids et l'identification des bagages;

16° le point de passage frontalier utilisé pour entrer sur le territoire national ».

B.39.2.2. Les « données API » visées à l'article 9, § 2, de la loi du 25 décembre 2016 reprennent, pour l'essentiel, les données visées au point 18 de l'annexe I de la directive « PNR » et sont donc plus larges que les données qui étaient visées par l'article 3, paragraphe 2, de la directive « API ».

B.40.1. Comme il est dit en B.3, la loi du 25 décembre 2016 a pour objectif d'assurer la sécurité publique, en instaurant un transfert des données des passagers et l'utilisation de celles-ci, dans le cadre de la lutte contre des infractions terroristes et la criminalité transnationale grave.

Ces objectifs constituent des objectifs d'intérêt général susceptibles de justifier des ingérences dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel (CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, point 42). La Cour de justice a d'ailleurs confirmé que ces objectifs d'intérêt général pouvaient justifier le transfert et le traitement de données des dossiers passagers (CJUE, grande chambre, 26 juillet 2017, avis 1/15, points 148 et 149).

B.40.2. Il convient maintenant d'examiner si, comme il est dit en B.35, ces ingérences sont suffisamment précises, proportionnées et limitées au « strict nécessaire », en tenant compte de l'ampleur des données visées par la loi du 25 décembre 2016.

B.41.1. La collecte des données des passagers visées par la loi du 25 décembre 2016 est entourée de garanties quant au contenu de ces données.

B.41.2. Tout d'abord, comme il est dit en B.24.1, ces données sont déterminées de manière exhaustive par l'article 9 de la loi du 25 décembre 2016.

COPIE NON CORRIGÉE

Ces données sont des informations directement liées au voyage donnant lieu au transport entrant dans le champ d'application de la loi du 25 décembre 2016. Comme il est dit en B.36.2.2, il s'agit de données dont les transporteurs et opérateurs de voyage disposent en principe déjà. Par ailleurs, ces données correspondent à l'annexe I des lignes directrices de l'Organisation de l'aviation civile internationale (OACI) (CJUE, 26 juillet 2017, avis 1/15, point 156). Ces données sont dès lors pertinentes eu égard aux objectifs poursuivis par la loi du 25 décembre 2016.

B.41.3.1. Par ailleurs, les articles 10 et 11, non attaqués, de la loi du 25 décembre 2016 disposent :

« Art. 10. Les données des passagers ne peuvent pas concerner l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à une organisation syndicale, ou les données concernant son état de santé, sa vie sexuelle ou son orientation sexuelle.

Art. 11. Lorsque les données des passagers transférées par les transporteurs et opérateurs de voyage comportent des données autres que celles énumérées à l'article 9 ou comportent des données comme énumérées à l'article 10, l'UIP efface ces données supplémentaires dès leur réception et de façon définitive ».

B.41.3.2. Les travaux préparatoires de la loi du 25 décembre 2016 confirment à ce sujet :

« Les données des passagers ne peuvent en aucun cas avoir trait à l'origine raciale ou ethnique de l'intéressé, ni à ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à une organisation syndicale, sa santé, sa vie sexuelle ou son orientation sexuelle. Les données doivent en revanche comporter des informations détaillées sur la réservation effectuée par le passager et sur son itinéraire, qui permettront aux instances compétentes de déterminer quels passagers sont susceptibles de constituer un risque pour la sécurité.

[…]

Les listes de données relatives aux passagers sont limitées à ce qui est strictement nécessaire pour répondre aux exigences légitimes des autorités compétentes dans le cadre des objectifs fixés dans la loi. Les autres données que celles énoncées aux articles 9 et 10 de la présente loi ne sont pas collectées et sont effacées immédiatement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 21).

COPIE NON CORRIGÉE

B.41.4. Ces dispositions garantissent ainsi que des données sensibles ne peuvent, en principe, être collectées ou conservées au titre de « données des passagers » visées par la loi du 25 décembre 2016.

B.41.5. Dans son avis n° 1/15, précité, du 26 juillet 2017, la Cour de justice a également considéré, en ce qui concerne les données sensibles, que « les articles 7, 8 et 21 ainsi que l'article 52, paragraphe 1, de la Charte s'opposent tant au transfert des données sensibles vers le Canada qu'à l'encadrement négocié par l'Union avec cet État tiers des conditions tenant à l'utilisation et à la conservation de telles données par les autorités de cet État tiers » (point 167).

Cette observation est transposable en l'espèce.

B.42.1. Bien qu'il existe des garanties entourant les données des passagers visées par la loi du 25 décembre 2016, il convient néanmoins de se demander si ces garanties sont suffisantes, compte tenu de l'ampleur des données visées.

B.42.2. Les données visées à l'article 9, § 1er, de la loi du 25 décembre 2016, lequel reprend les données visées dans l'annexe I de la directive « PNR », comprennent en effet des données très larges, outre les données d'enregistrement et d'embarquement, notamment : l'itinéraire complet pour le passager, l'agence de voyage, le numéro de siège, toutes les informations relatives aux bagages, les informations relatives aux modes de paiement, y compris l'adresse de facturation, les remarques générales, « y compris toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans » (article 9, § 1er, 12°).

B.42.3.1. Dans son avis n° 1/15 du 26 juillet 2017, précité, la Cour de justice a d'ailleurs observé que, « même si certaines des données PNR, prises isolément, ne paraissent pas pouvoir révéler des informations importantes sur la vie privée des personnes concernées, il n'en demeure pas moins que, prises ensemble, lesdites données peuvent, entre autres, révéler un itinéraire de voyage complet, des habitudes de voyage, des relations existant entre deux ou plusieurs personnes ainsi que des informations sur la situation financière des passagers aériens, leurs habitudes alimentaires ou leur état de santé, et pourraient même fournir des informations sensibles sur ces passagers, telles que définies à l'article 2, sous e), de l'accord envisagé » (point 128).

COPIE NON CORRIGÉE

B.42.3.2. Dans son avis du 19 août 2016 « sur les implications en matière de protection des données du traitement des dossiers passagers », le Comité consultatif de la Convention n° 108 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » a également observé :

« Les PNR contiennent des informations visant à faciliter le voyage d'un passager, et peuvent comprendre un certain nombre de données sensibles (données pouvant servir à indiquer l'origine raciale, les opinions politiques, les convictions religieuses et autres, l'état de santé ou l'orientation sexuelle d'une personne), non seulement sous certaines données 'codées' mais aussi dans le champ ouvert contenant des observations générales (telles que les demandes diététiques et médicales, ou le fait qu'une association politique ou religieuse a bénéficié de billets à prix réduit pour le voyage de ses membres), ce qui pourrait conduire à une discrimination directe » (Conseil de l'Europe, avis du 19 août 2016, T-PD(2016)18rev, p. 7).

B.42.3.3. L'Agence des droits fondamentaux de l'Union européenne a également remarqué que les données « PNR » « peuvent comprendre des données sensibles ou particulières sous l'intitulé ' remarques générales ' » (Avis 1/2011 de l'Agence des droits fondamentaux de l'Union européenne sur la proposition de 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, ainsi que pour les enquêtes et les poursuites en la matière (COM(2011) 32 final), 14 juin 2011, p. 8; voy. aussi *ibid.*, p. 13).

B.42.4. Ainsi, eu égard à leur champ d'application très large, les données visées à l'article 9 de la loi du 25 décembre 2016, bien que ne pouvant pas contenir directement des données sensibles, pourraient néanmoins révéler, indirectement, des éléments sensibles relevant de la protection des données à caractère personnel et du respect de la vie privée.

Compte tenu de l'avis n° 1/15 de la Cour de justice, mentionné en B.35.5, il y a lieu de se demander si les données visées à l'article 9 de la loi du 25 décembre 2016, qui comprennent les données visées dans l'annexe I de la directive « PNR », ne vont pas au-delà du « strict nécessaire » pour atteindre les objectifs poursuivis par la directive « PNR ».

COPIE NON CORRIGÉE

B.42.5. L'article 267 du TFUE habilite la Cour de justice à statuer, à titre préjudiciel, aussi bien sur l'interprétation des traités et des actes des institutions de l'Union européenne que sur la validité de ces actes. En vertu du troisième alinéa de cette disposition, une juridiction nationale est tenue de saisir la Cour de justice lorsque ses décisions - comme celles de la Cour constitutionnelle - ne sont pas susceptibles d'un recours juridictionnel de droit interne. En cas de doute sur l'interprétation ou sur la validité d'une disposition du droit de l'Union européenne importante pour la solution d'un litige pendant devant une telle juridiction nationale, celle-ci doit, même d'office, poser une question préjudicielle à la Cour de justice.

Avant de statuer quant au fond, il convient dès lors de poser à la Cour de justice de l'Union européenne la deuxième question préjudicielle figurant dans le dispositif.

B.43.1. Dans son avis n° 1/15, précité, du 26 juillet 2017, la Cour de justice a par ailleurs émis les observations suivantes, en ce qui concerne l'exigence d'une définition claire et précise des données visées par le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers :

« 155. En ce qui concerne les données visées par l'accord envisagé, cet accord devrait définir de manière claire et précise les données PNR que les transporteurs aériens sont appelés à transférer vers le Canada en application dudit accord.

156. À cet égard, si les 19 rubriques des données PNR figurant à l'annexe de l'accord envisagé correspondent, selon les observations de la Commission, à l'annexe I des lignes directrices de l'Organisation de l'aviation civile internationale (OACI) relatives aux données PNR, il convient cependant de souligner, comme l'a relevé M. l'avocat général au point 217 de ses conclusions, que la rubrique 5, qui vise les ' informations disponibles sur " les grands voyageurs " et les programmes de fidélisation (billets gratuits, surclassement, etc.) ', et la rubrique 7, qui couvre ' toutes les coordonnées disponibles (y compris les informations sur la source) ', ne définissent pas de manière suffisamment claire et précise les données PNR à transférer.

157. En effet, s'agissant de la rubrique 5, l'emploi du terme ' etc. ' ne détermine pas à suffisance l'étendue des données à transférer. En outre, les termes de cette rubrique ne permettent pas de savoir si celle-ci vise des informations concernant le seul statut des passagers aériens dans des programmes de fidélisation ou si, au contraire, elle vise l'ensemble des informations relatives aux voyages aériens et aux transactions effectuées dans le cadre de tels programmes.

158. De même, la rubrique 7, en employant les termes ‘ toutes les coordonnées disponibles ’, ne détermine pas suffisamment l’étendue des données à transférer. Notamment, elle ne précise pas quel est le type des coordonnées qu’elle vise ni si ces coordonnées couvrent également, ainsi qu’il peut être déduit de la réponse écrite de la Commission aux questions posées par la Cour, celles des tiers ayant effectué la réservation du vol pour le passager aérien, des tiers par l’intermédiaire desquels un passager aérien peut être joint, ou encore des tiers devant être informés en cas d’urgence.

159. En ce qui concerne la rubrique 8, celle-ci porte sur ‘ toutes les informations disponibles relatives au paiement/à la facturation (à l’exclusion des autres détails de l’opération liés à la carte de crédit ou au compte et n’ayant pas de lien avec l’opération relative au voyage) ’. Certes, cette rubrique pourrait paraître particulièrement large en ce qu’elle emploie l’expression ‘ toutes les informations disponibles ’. Néanmoins, ainsi qu’il ressort de la réponse de la Commission aux questions posées par la Cour, ladite rubrique doit être considérée comme ne visant que les informations relatives aux modalités de paiement et à la facturation du billet d’avion, à l’exclusion de toute autre information sans rapport direct avec le vol. Interprétée en ce sens, cette même rubrique peut donc être considérée comme répondant aux exigences de clarté et de précision.

160. S’agissant de la rubrique 17, celle-ci vise les ‘ remarques générales, y compris les données OSI (*Other Supplementary Information*), les données SSI (Special Service Information) et les données SSR (Special Service Request) ’. Selon les explications apportées, notamment, par la Commission, cette rubrique constitue une rubrique dite ‘ texte libre ’ *(free text)*, ayant vocation à inclure ‘ toutes les informations supplémentaires ’, en plus de celles énumérées par ailleurs dans l’annexe de l’accord envisagé. Ainsi, une telle rubrique ne fournit aucune indication sur la nature et l’étendue des renseignements qui doivent être transmis, et paraît même susceptible d’englober des informations dépourvues de tout rapport avec la finalité du transfert des données PNR. En outre, dès lors que les informations visées dans ladite rubrique ne sont fournies qu’à titre d’exemples, comme en témoigne l’usage des termes ‘ y compris ’, cette même rubrique ne fixe aucune limitation quant à la nature et l’étendue des informations susceptibles d’y figurer. Dans ces conditions, la rubrique 17 ne saurait être considérée comme étant délimitée avec suffisamment de clarté et de précision.

161. En ce qui concerne, enfin, la rubrique 18, celle-ci porte sur ‘ toute information préalable sur les voyageurs (IPV) collectée à des fins de réservation ’. Selon les précisions apportées par le Conseil et la Commission, ces informations correspondent aux renseignements visés à l’article 3, paragraphe 2, de la directive 2004/82, à savoir le numéro et le type du document de voyage utilisé, la nationalité, le nom complet, la date de naissance, le point de passage frontalier utilisé pour entrer sur le territoire des États membres, le code de transport, les heures de départ et d’arrivée du transport, le nombre total des personnes transportées ainsi que le point d’embarquement initial. Cette rubrique, pour autant qu’elle soit interprétée comme ne couvrant que les renseignements expressément visés à cette dernière disposition, peut être considérée comme satisfaisant aux exigences de clarté et de précision.

162. Les dispositions de l'article 4, paragraphe 3, de l'accord envisagé, qui prévoient l'obligation du Canada de supprimer toute donnée PNR qui lui a été transférée si elle ne figure pas dans la liste de l'annexe de cet accord, ne permettent pas de pallier l'imprécision entachant les rubriques 5, 7 et 17 de cette annexe. En effet, dans la mesure où cette liste ne délimite pas, en tant que telle, avec suffisamment de clarté et de précision, les données PNR à transférer, ces dispositions ne sont pas de nature à remédier aux incertitudes quant aux données PNR devant faire l'objet du transfert.

163. Dans ces conditions, s'agissant des données PNR à transférer vers le Canada, les rubriques 5, 7 et 17 de l'annexe de l'accord envisagé n'encadrent pas de manière suffisamment claire et précise la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte ».

B.43.2. Dès lors que certaines de ces observations pourraient être transposables en l'espèce, à l'égard du caractère exemplatif et non exhaustif de certaines données contenues dans l'annexe I de la directive « PNR », que l'article 9 de la loi du 25 décembre 2016 transpose, il y a lieu, avant de statuer quant au fond, de poser à la Cour de justice de l'Union européenne la troisième question préjudicielle figurant dans le dispositif.

4. *La notion de « passager » (article 4, 10°)*

B.44. La partie requérante critique le caractère large de la notion de « passager », qui donne lieu à un traitement automatisé systématique, non ciblé, des données de tous les passagers.

B.45.1. L'article 4, 10°, de la loi attaquée définit le « passager » comme « toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par le transporteur, avec le consentement de ce dernier, lequel se traduit par l'inscription de cette personne sur la liste des passagers ».

Cet article reprend le contenu de l'article 3, point 4), de la directive « PNR », qui définit également le « passager » comme « toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers ».

COPIE NON CORRIGÉE

B.45.2. La définition de « passager » a pour conséquence que la collecte, le transfert et le traitement des données « PNR » de ces « passagers » constituent des obligations générales et indifférenciées, qui s'appliquent à toute personne transportée ou devant être transposée et inscrite sur la liste des passagers.

Les obligations que la loi du 25 décembre 2016 impose s'appliquent ainsi indépendamment de l'existence de motifs sérieux de croire que les personnes concernées ont commis une infraction ou sont sur le point de commettre une infraction, ou ont été reconnues coupables d'une infraction.

B.45.3. Dans son avis du 19 août 2016 « sur les implications en matière de protection des données du traitement des données passagers », le Comité consultatif de la Convention n° 108 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » a observé à cet égard :

« Le traitement des données PNR – qui a l'avantage unique de permettre l'identification des personnes d'intérêt – est un filtrage général et non sélectif de tous les passagers, y compris de ceux qui ne sont pas soupçonnés d'avoir commis une quelconque infraction pénale, par différentes autorités compétentes, et il concerne des données collectées initialement à des fins commerciales par des entités privées. Eu égard à l'ampleur de l'atteinte aux droits à la vie privée et à la protection des données qui découlerait du traitement des données PNR, il doit être clairement établi que ledit traitement est une mesure nécessaire dans une société démocratique dans un but légitime; il faut en outre que les garanties appropriées soient mises en place. Il est indispensable de démontrer expressément la nécessité de la collecte et de l'exploitation ultérieure des données PNR » (avis du 19 août 2016, T-PD(2016)18rev, p. 5).

Le Comité a également souligné la nécessité d'une évaluation périodique d'un tel système « PNR », afin de déterminer s'il est toujours justifié :

COPIE NON CORRIGÉE

« Dans le cas des systèmes existants de traitement des données PNR par les autorités publiques compétentes, une plus grande transparence sur l'évaluation de l'efficacité de ces systèmes doit être recherchée en vue de permettre une évaluation fondée et indépendante de la nécessité du système. Si cette transparence doit être détaillée, elle ne doit toutefois pas aller à l'encontre de l'objectif légitime. Par exemple, des informations objectives et quantifiables concernant les résultats atteints, comme le nombre de personnes arrêtées, les menaces terroristes qui pourraient être évitées, les autres effets dissuasifs, la modification des comportements des délinquants (par exemple, le renoncement à des actes criminels envisagés), la probabilité d'une augmentation importante du coût et de la difficulté de la perpétration d'infractions (tels que des attentats terroristes) permettraient d'éclairer l'évaluation de la nécessité d'un système de traitement des PNR.

Il convient de procéder à intervalles réguliers à un examen de la nécessité du système des PNR afin de déterminer s'il est toujours justifié » (*ibid.*, p. 6).

B.45.4.1. L'article 19 de la directive « PNR », intitulé « Réexamen », prévoit que, sur la base des informations communiquées par les États membres, y compris des informations statistiques, la Commission procède, au plus tard le 25 mai 2020, au réexamen de tous les éléments de la directive et communique et présente un rapport au Parlement européen et au Conseil.

L'article 19, paragraphe 3, de la directive « PNR » prévoit que « la Commission tient compte de l'expérience acquise par les États membres, en particulier ceux qui appliquent la présente directive aux vols intra-UE conformément à l'article 2 » et « examine également s'il est nécessaire d'inclure des opérateurs économiques autres que les transporteurs, tels que des agences et des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, dans le champ d'application de la présente directive ».

B.45.4.2. L'article 52, § 1er, de la loi du 25 décembre 2016 prévoit que « la présente loi est soumise à une évaluation trois ans après son entrée en vigueur ».

B.46.1. Dans le domaine des communications électroniques, la Cour de justice de l'Union européenne s'est prononcée, par un arrêt rendu en grande chambre le 21 décembre 2016, sur une réglementation nationale qui prévoyait une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, ainsi que l'obligation pour les fournisseurs de services de communications électroniques de conserver ces données de manière systématique et continue, et ce sans aucune exception (CJUE, grande chambre, 21 décembre 2016, C-203/15, *Tele2 Sverige AB c. Post-och telestyrelsen* et C-698/15, *Secretary of State for the Home Department c. Tom Watson e.a.).*

La Cour de justice a jugé que, « si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte » (point 103).

La Cour de justice a jugé :

« 104. À cet égard, il convient de relever, d'une part, qu'une telle réglementation a pour effet, eu égard à ses caractéristiques décrites au point 97 du présent arrêt, que la conservation des données relatives au trafic et des données de localisation est la règle, alors que le système mis en place par la directive 2002/58 exige que cette conservation des données soit l'exception.

105. D'autre part, une réglementation nationale telle que celle en cause au principal, qui couvre de manière généralisée tous les abonnés et utilisateurs inscrits et vise tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic, ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi. Elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves. En outre, elle ne prévoit aucune exception, de telle sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, points 57 et 58).

COPIE NON CORRIGÉE

106. Une telle réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 59).

107. Une réglementation nationale telle que celle en cause au principal excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte.

108. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire.

109. Pour satisfaire aux exigences énoncées au point précédent du présent arrêt, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (voir, par analogie, à propos de la directive 2006/24, arrêt *Digital Rights*, point 54 et jurisprudence citée).

110. En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné.

COPIE NON CORRIGÉE

111. S’agissant de la délimitation d’une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d’une manière ou d’une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique. Une telle délimitation peut être assurée au moyen d’un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d’éléments objectifs, qu’il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes.

112. Eu égard à l’ensemble des considérations qui précèdent, il convient de répondre à la première question dans l’affaire C-203/15 que l’article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l’article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu’il s’oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l’ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ».

B.46.2. À la seconde question préjudicielle dans l’affaire C-203/15 et à la première question préjudicielle dans l’affaire C-698/15, la Cour de justice répond que l’article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11 ainsi que de l’article 52, paragraphe 1, de la Charte, doit être interprété « en ce sens qu’il s’oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l’accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l’Union » (point 125).

B.46.3. De son côté, la Cour européenne des droits de l’homme a entre-temps jugé la législation suédoise relative à l’interception massive de communications électroniques conforme à l’article 8 de la Convention européenne des droits de l’homme, dans son arrêt *Centrum för Rättvisa c. Suède*, du 19 juin 2018. Pour conclure à l’absence de violation, elle se base sur les critères qu’elle a développés dans sa jurisprudence antérieure (cf. notamment CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*). Elle observe, en particulier, ce qui suit :

COPIE NON CORRIGÉE

« La Cour a expressément reconnu que les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder la sécurité nationale (cf. *Weber et Saravia*, précité, § 106). Dans les affaires *Weber et Saravia* et *Liberty e.a.*, la Cour a admis que les régimes d'interception massive n'excèdent pas en eux-mêmes cette marge d'appréciation. Au vu de la motivation de la Cour dans ces décisions et compte tenu des menaces auxquelles sont confrontés de nombreux États contractants (dont le fléau du terrorisme international et d'autres formes graves de criminalité telles que le trafic de stupéfiants, la traite d'êtres humains, l'exploitation sexuelle des enfants et la cybercriminalité) des progrès technologiques qui permettent aux terroristes et aux criminels d'échapper plus facilement à la détection sur internet et de l'impossibilité de prévoir les voies par lesquelles les communications électroniques seront transmises, la Cour considère que la décision de recourir à un régime d'interception massive afin de repérer des menaces jusqu'alors inconnues pour la sécurité nationale relève de la marge d'appréciation des États » (CEDH, 19 juin 2018, *Centrum för Rättvisa c. Suède*, § 112).

La Cour européenne des droits de l'homme a par contre jugé que la loi anglaise sur l'interception des communications violait l'article 8 de la Convention européenne des droits de l'homme car elle ne respectait pas les critères énoncés dans sa jurisprudence. Elle a considéré également que « le fonctionnement des régimes d'interception en masse relève en principe de la marge d'appréciation de l'État. L'interception en masse est par définition non ciblée, et la subordonner à la présence d'un ' soupçon raisonnable ' en rendrait la mise en œuvre impossible » (CEDH, 13 septembre 2018, *Big Brother Watch e.a. c. Royaume-Uni*, § 317).

B.46.4. La question se pose de savoir dans quelle mesure la jurisprudence précitée, qui concerne la conservation généralisée et indifférenciée de données en matière de communications électroniques, est transposable à la collecte, au transfert et au traitement généralisés et indifférenciés des données des passagers, tels qu'ils sont organisés par la loi du 25 décembre 2016.

B.47.1. Dans son avis n° 1/15, précité, du 26 juillet 2017, la Cour de justice s'est prononcée sur un système « PNR » analogue mais au champ d'application plus limité, puisque le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers prévoyait « le transfert systématique et continu des données PNR de l'ensemble des passagers aériens empruntant des vols entre l'Union et le Canada » (point 127).

COPIE NON CORRIGÉE

La Cour de justice a considéré que « le transfert des données PNR vers le Canada et les traitements ultérieurs de celles-ci peuvent être considérés comme étant aptes à garantir la réalisation de l'objectif tenant à la protection de la sécurité et de la sûreté publiques, poursuivi par l'accord envisagé » (point 153).

En ce qui concerne les passagers concernés, la Cour de justice a considéré :

« 186. L'accord envisagé couvre les données PNR de l'ensemble des passagers aériens empruntant des vols entre l'Union et le Canada. Le transfert de ces données vers le Canada a lieu indépendamment de tout élément objectif permettant de considérer que les passagers sont susceptibles de présenter un risque pour la sécurité publique au Canada.

187. À cet égard, il convient de relever que, ainsi qu'il a été rappelé aux points 152 et 169 du présent avis, les données PNR sont, notamment, destinées à être soumises à un traitement automatisé. Or, comme l'ont avancé plusieurs intervenants, ce traitement vise à identifier le risque pour la sécurité publique que pourraient éventuellement présenter des personnes qui ne sont pas, à ce stade, connues des services compétents et qui pourraient être, en raison de ce risque, soumises à un examen approfondi. À cet égard, le traitement automatisé de ces données, préalablement à l'arrivée des passagers au Canada, facilite et accélère les contrôles de sécurité, notamment aux frontières. En outre, l'exclusion de certaines catégories de personnes, ou de certaines zones d'origine, serait de nature à faire obstacle à la réalisation de l'objectif du traitement automatisé des données PNR, à savoir l'identification, au moyen d'une vérification de ces données, des personnes susceptibles de présenter un risque pour la sécurité publique parmi l'ensemble des passagers aériens, et à permettre que cette vérification puisse être contournée.

188. Au demeurant, conformément à l'article 13 de la convention de Chicago, auquel se sont référés en particulier le Conseil et la Commission dans leurs réponses aux questions posées par la Cour, tous les passagers aériens doivent, à l'entrée, à l'intérieur ainsi qu'à la sortie du territoire d'un État contractant, observer les lois et les règlements de cet État concernant l'entrée ou la sortie des passagers aériens de son territoire. L'ensemble des passagers aériens désireux d'entrer au Canada ou de sortir de ce pays est donc soumis, sur le fondement de cet article, aux contrôles aux frontières et tenu de respecter les conditions d'entrée et de sortie prescrites par le droit canadien en vigueur. En outre, ainsi qu'il ressort des points 152 et 187 du présent avis, l'identification, au moyen des données PNR, des passagers susceptibles de présenter un risque pour la sécurité publique fait partie des contrôles aux frontières. Par conséquent, dès lors qu'ils font l'objet de ces contrôles, les passagers aériens souhaitant entrer et séjourner au Canada sont, en raison de la nature même de cette mesure, soumis à la vérification de leurs données PNR.

189. Dans ces conditions, il n'apparaît pas que l'accord envisagé dépasse les limites du strict nécessaire en ce qu'il permet le transfert des données PNR de l'ensemble des passagers aériens vers le Canada ».

B.47.2. La question se pose toutefois de savoir si ces considérations pourraient être transposées à l'égard de la directive « PNR » et d'une législation nationale, telle que la loi du 25 décembre 2016, qui, transposant la directive « PNR », instaure la collecte, le transfert et l'utilisation généralisés et indifférenciés des données « PNR » pour l'ensemble des passagers qui voyagent par transport aérien, ferroviaire ou par bus, indépendamment d'un passage aux frontières extérieures de l'Union.

Ce système s'applique en effet à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves (comp. avec CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, point 58), et est plus large que le système prévu par l'accord « PNR » avec le Canada. Au regard de l'ampleur des données visées, la question se pose de savoir si cette mesure respecte les limites du « strict nécessaire ».

Avant de statuer quant au fond, il y a lieu dès lors de poser à la Cour de justice de l'Union européenne la quatrième question préjudicielle figurant dans le dispositif.

5. *Les finalités du traitement des données « PNR » (article 8)*

B.48. La partie requérante critique la définition des finalités du traitement des données « PNR », contenue dans l'article 8 de la loi du 25 décembre 2016, qui serait beaucoup plus large que les « finalités spécifiques », qui, elles, sont limitées aux seules infractions terroristes et formes graves de criminalités de la directive « PNR ». Elle estime que ces finalités excèdent les limites du « strict nécessaire ».

B.49.1. L'article 1er, paragraphe 2, de la directive « PNR » dispose :

« Les données PNR recueillies conformément à la présente directive ne peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière, comme prévu à l'article 6, paragraphe 2, points a), b) et c) ».

L'article 6, paragraphe 2, de la directive « PNR » dispose :

COPIE NON CORRIGÉE

« 2. L'UIP ne traite les données PNR qu'aux fins suivantes :

a) réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes visées à l'article 7 et, le cas échéant, par Europol conformément à l'article 10, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité;

b) répondre, au cas par cas, aux demandes dûment motivées fondées sur des motifs suffisants des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière, et visant à communiquer aux autorités compétentes ou, le cas échéant, à Europol le résultat de ce traitement; et

c) analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées au titre du paragraphe 3, point b), en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité ».

Le considérant 7 de la directive « PNR » précise aussi :

« L'utilisation des données PNR permet de contrer la menace que représentent les infractions terroristes et les formes graves de criminalité sous un angle autre que par le traitement d'autres catégories de données à caractère personnel. Cependant, pour veiller à ce que le traitement de données PNR reste limité à ce qui est nécessaire, la création et l'application de critères d'évaluation devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente ».

B.49.2. Les finalités du traitement des données « PNR », telles qu'elles sont prévues par la directive « PNR », constituent donc uniquement des objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière.

B.49.3. L'article 3, point 8), de la directive « PNR » définit les « infractions terroristes » comme « les infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI ».

L'article 3, point 9), de la directive « PNR » définit les « formes graves de criminalité » comme étant « les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre ».

L'annexe II, intitulée « Liste des infractions visées à l'article 3, point 9) », de la directive « PNR » dispose :

« 1. Participation à une organisation criminelle

2. Traite des êtres humains

3. Exploitation sexuelle des enfants et pédopornographie

4. Trafic de stupéfiants et de substances psychotropes

5. Trafic d'armes, de munitions et d'explosifs

6. Corruption

7. Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union

8. Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro

9. Cybercriminalité

10. Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées

11. Aide à l'entrée et au séjour irréguliers

12. Meurtre, coups et blessures graves

13. Trafic d'organes et de tissus humains

14. Enlèvement, séquestration et prise d'otage

15. Vol organisé ou vol à main armée

16. Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art

17. Contrefaçon et piratage de produits

18. Falsification de documents administratifs et trafic de faux

19. Trafic de substances hormonales et d'autres facteurs de croissance

20. Trafic de matières nucléaires et radioactives

21. Viol

22. Infractions graves relevant de la Cour pénale internationale

23. Détournement d'avion/de navire

24. Sabotage

25. Trafic de véhicules volés

26. Espionnage industriel ».

B.50.1. Dans sa version initiale, l'article 8 de la loi du 25 décembre 2016 disposait :

« § 1er. Les données des passagers sont traitées aux fins :

1° de la recherche et la poursuite, en ce compris l'exécution des peines ou des mesures limitatives de liberté, relatives aux infractions visées à l'article 90*ter*, § 2, 1°*bis*, 1°*ter*, 1°*quater*, 1°*quinquies*, 1°*octies*, 4°, 5°, 6°, 7°, 7°*bis*, 7°*ter*, 8°, 9°, 10°, 10°*bis*, 10°*ter*, 11°, 13°, 13°*bis*, 14°, 16°, 17°, 18°, 19° et § 3, du Code d'instruction criminelle;

2° de la recherche et la poursuite, en ce compris l'exécution des peines ou des mesures limitatives de liberté, relatives aux infractions visées aux articles 196, en ce qui concerne les infractions de faux en écritures authentiques et publiques, 198, 199, 199*bis*, 207, 213, 375 et 505 du Code pénal;

3° de la prévention des troubles graves à la sécurité publique dans le cadre de la radicalisation violente par le suivi des phénomènes et groupements conformément à l'article 44/5, § 1er, 2° et 3° et § 2, de la loi du 5 août 1992 sur la fonction de police;

4° du suivi des activités visées aux articles 7, 1° et 3° /1, et 11, § 1er, 1° à 3° et 5°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

5° de la recherche et la poursuite des infractions visées à l'article 220, § 2, de la loi générale sur les douanes et accises du 18 juillet 1977 et l'article 45, alinéa 3, de la loi du 22 décembre 2009 relative au régime général d'accise.

§ 2. Sous les conditions prévues au chapitre 11, les données des passagers sont également traitées en vue de l'amélioration des contrôles de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale ».

COPIE NON CORRIGÉE

En vertu de l'article 13, § 2, de la loi du 25 décembre 2016, sans préjudice d'autres dispositions légales, « l'UIP ne peut utiliser les données conservées en vertu du chapitre 9 pour d'autres finalités que celles visées à l'article 8 ».

B.50.2.1. Comme il est dit en B.13, l'article 8, § 1er, 1° et 5°, de la loi du 25 décembre 2016 a par ailleurs été remplacé par l'article 62 de la loi du 15 juillet 2018.

B.50.2.2. L'article 62 de la loi du 15 juillet 2018 remplace tout d'abord l'article 8, § 1er, 1°, de la loi du 25 décembre 2016. Étaient initialement visées les « infractions visées à l'article 90*ter*, § 2, 1°*bis*, 1°*ter*, 1°*quater*, 1°*quinquies*, 1°*octies*, 4°, 5°, 6°, 7°, 7°*bis*, 7°*ter*, 8°, 9°, 10°, 10°*bis*, 10°*ter*, 11°, 13°, 13°*bis*, 14°, 16°, 17°, 18°, 19° et § 3, du Code d'instruction criminelle ». Depuis la modification apportée par l'article 62 de la loi du 15 juillet 2018, sont visées les « infractions visées à l'article 90*ter*, § 2, 2°, 3°, 7°, 8°, 11°, 14°, 17° à 20°, 22°, 24° à 28°, 30°, 32°, 33°, 34°, 36° à 39°, 43° à 45° et § 3, du Code d'instruction criminelle ».

Eu égard à ces modifications, le recours en annulation a perdu son objet en ce que l'article 8, § 1er, 1°, de la loi du 25 décembre 2016 concerne des infractions visées à l'article 90*ter*, § 2, 1°*bis*, 1°*ter*, 1°*quater*, 1°*quinquies*, 1°*octies*, 4°, 5°, 6°, 7°*bis*, 7°*ter*, 9°, 10°, 10°*bis*, 10°*ter*, 13°, 13°*bis* et 16°, du Code d'instruction criminelle. Par contre, le recours en annulation conserve son objet en ce qu'il est dirigé contre l'article 8, § 1er, 1°, de la loi du 25 décembre 2016, dès lors que cet article concerne des infractions visées à l'article 90*ter*, § 2, 7°, 8°, 11°, 14°, 17°, 18°, 19° et § 3, du Code d'instruction criminelle.

Les infractions visées à l'article 90*ter*, § 2, 7°, 8°, 11°, 14°, 17°, 18°, 19° et § 3, du Code d'instruction criminelle sont les infractions visées à l'article 210*bis* du Code pénal (faux en informatique), aux articles 246, 247, 248, 249 et 250 du même Code (corruption de personnes qui exercent une fonction publique), aux articles 324*bis* et 324*ter* du même Code (participation à une organisation criminelle), à l'article 347*bis* du même Code (prise d'otages), aux articles 379, 380 et 383*bis*, §§ 1er et 3, du même Code (corruption de la jeunesse, prostitution et outrage aux bonnes mœurs), à l'article 393 du même Code (homicide) et aux articles 394 et 397 du même Code (meurtre et empoisonnement).

COPIE NON CORRIGÉ

B.50.2.3. L'article 62 de la loi du 15 juillet 2018 remplace ensuite l'article 8, § 1er, 5°, de la loi du 25 décembre 2016. Étaient initialement visées les « infractions visées à l'article 220, § 2, de la loi générale sur les douanes et accises du 18 juillet 1977 et l'article 45, alinéa 3, de la loi du 22 décembre 2009 relative au régime général d'accise ». Depuis la modification apportée par l'article 62 de la loi du 15 juillet 2018, sont visées les « infractions visées à l'article 220, § 2, de la loi générale sur les douanes et accises du 18 juillet 1977, à l'article 45, alinéa 3, de la loi du 22 décembre 2009 relative au régime général d'accise, à l'article 5 de la loi du 15 mai 2007 relative à la répression de la contrefaçon et de la piraterie de droits de la propriété intellectuelle, à l'article 26 du décret de la Communauté germanophone du 20 février 2017 visant la protection des biens culturels mobiliers particulièrement remarquables ainsi qu'à l'article 24 du décret de la Communauté flamande du 24 janvier 2003 portant protection du patrimoine culturel mobilier présentant un intérêt exceptionnel, l'arrêté ministériel du 7 février 2012 soumettant à licence l'importation des marchandises originaires ou en provenance de Syrie modifié par l'arrêté ministériel du 1er juillet 2014, l'arrêté ministériel du 23 mars 2004 abrogeant l'arrêté ministériel du 17 janvier 2003 soumettant à une autorisation préalable l'importation, l'exportation et le transit des marchandises originaires, en provenance ou à destination de l'Iraq et soumettant à une licence l'importation, l'exportation et le transit de certaines marchandises originaires, en provenance ou à destination de l'Iraq ainsi que la recherche des infractions visées à l'article 5 de la loi du 28 juillet 1981 portant approbation de la Convention sur le commerce international des espèces de faune et de flore sauvages menacées d'extinction, et des Annexes, faites à Washington le 3 mars 1973, ainsi que l'Amendement à la Convention, adopté à Bonn le 22 juin 1979 ».

Dès lors que la modification apportée à l'article 8, § 1er, 5°, de la loi du 25 décembre 2016 par l'article 62 de la loi du 15 juillet 2018 étend uniquement le champ d'application des infractions visées, le recours en annulation conserve son objet en ce qu'il est dirigé contre l'article 8, § 1er, 5°, de la loi du 25 décembre 2016, puisque cet article concerne les « infractions visées à l'article 220, § 2, de la loi générale sur les douanes et accises du 18 juillet 1977 et l'article 45, alinéa 3, de la loi du 22 décembre 2009 relative au régime général d'accise ».

COPIE NON CORRIGÉE

Ces infractions visent la fraude fiscale grave, organisée ou non, à la législation sur les douanes et accises.

B.50.3. En ce qui concerne les finalités inspirées de la directive « PNR », l'exposé des motifs de la loi du 25 décembre 2016 indique :

« L'article 8 détermine limitativement les finalités pour lesquelles le traitement des données des passagers sera autorisé.

Le § 1er concerne les [cinq] finalités qui forment le *corpus* et l'essence même de l'utilisation des données des passagers en vue d'améliorer le niveau de sécurité notamment par une analyse précise, objective et professionnelle du risque et de la menace que peuvent représenter certains passagers.

La première finalité concerne la recherche et la poursuite des infractions graves en ce compris terroristes qui sont inscrites à l'article 90*ter*, § 2, 1°*bis*, 1°*ter*, 1°*quater*, 1°*quinquies*, 1°*octies*, 4°, 5°, 6°, 7°, 7°*bis*, 7°*ter*, 8°, 9°, 10°, 10°*bis*, 10°*ter*, 11°, 13°, 13°*bis*, 14°, 16°, 17°, 18°, 19° et § 3 du Code d'instruction criminelle. L'article 90*ter* du C.i.cr constitue dans notre droit matériel la référence dans le cadre de la prise de connaissance de communications et télécommunications privées mais également dans de nombreuses autres procédures afin de garantir le principe de proportionnalité (par exemple en matière de recherche proactive ou de témoignage anonyme).

La liste limitative de l'article 90*ter* C.i.cr. énumère les infractions graves qui sont à même de menacer gravement la sécurité intérieure et européenne et rejoint dès lors précisément l'objectif du présent projet.

L'exécution des peines et des mesures limitatives de liberté en relation avec lesdites infractions figurent textuellement dans la finalité. Par exemple, un passager est signalé parce qu'il a été condamné, en Belgique, par défaut à 4 ans de prison pour infraction en matière de trafic de stupéfiants et dont l'arrestation immédiate est ordonnée ou dans le cadre d'une mesure de liberté sous conditions dans un dossier lié à un foreign fighter, le juge d'instruction a posé pour condition une interdiction de quitter le territoire.

Cette finalité est judiciaire et relève dès lors des compétences des services de police, des Douanes et des autorités judiciaires.

La deuxième finalité concerne les catégories d'infractions énumérées à l'annexe II de la directive européenne PNR qui ne sont pas inclus[es] dans l'article 90*ter* C.i.cr: falsification de documents administratifs et trafic de faux, viol et trafic de véhicules volés. La référence à l'article 196 du Code pénal porte dès lors sur les écritures authentiques et publiques et n'englobe donc pas les écritures de commerce ou de banque ou écritures privées dont il est question à l'article 196, conformément à la Directive.

COPIE NON CORRIGÉE

Le traitement des données des passagers pour cette finalité est limitée [lire : limité] au traitement des données dans le cadre des recherches ponctuelles comme réglé dans l'article 27 de la loi.

[…]

La cinquième finalité concerne les infractions douane et accises de l'annexe II de la directive européenne PNR : Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, pp. 17-20).

B.50.4. Les finalités mentionnées à l'article 8 de la loi du 25 décembre 2016 encadrent de manière exhaustive les traitements autorisés des données des passagers.

Comme il est dit en B.12, l'article 8 de la loi du 25 décembre 2016 doit par ailleurs être interprété à la lumière de la loi du 30 juillet 2018.

Les travaux préparatoires de la loi du 30 juillet 2018, cités en B.12.2, indiquent que les finalités visées à l'article 8 de la loi du 25 décembre 2016 relèvent de trois catégories :

- la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales (article 8, § 1er, 1°, 2°, 3° et 5°, de la loi du 25 décembre 2016); ces traitements sont régis par le titre 2 de la loi du 30 juillet 2018;

- les missions des services de renseignement et de sécurité visés aux articles 7 et 11 de la loi du 30 novembre 1998 (article 8, § 1er, 4°, de la loi du 25 décembre 2016); ces traitements sont régis par le titre 3 de la loi du 30 juillet 2018;

- l'amélioration des contrôles de personnes aux frontières extérieures et la lutte contre l'immigration illégale (article 8, § 2, de la loi du 25 décembre 2016); ces traitements sont régis par le titre 2 de la loi du 30 juillet 2018.

B.51.1. Il ressort de ce qui est dit en B.50 que certaines des finalités de traitement visées à l'article 8 de la loi du 25 décembre 2016 correspondent aux infractions visées dans l'annexe II de la directive « PNR », conformément aux objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, visés par la directive (article 8, § 1er, 1°, 2° et 5°).

COPIE NON CORRIGÉE

Comme il est dit en B.40.1, la poursuite de ces objectifs, par la collecte et le traitement des données « PNR », constitue un but d'intérêt général permettant de justifier une ingérence dans le droit au respect de la vie privée et de la protection des données à caractère personnel.

B.51.2. Les termes utilisés pour déterminer ces finalités sont définis avec clarté et précision, dès lors qu'ils renvoient aux infractions définies par les dispositions du Code pénal.

De telles règles qui déterminent les infractions que l'on vise à prévenir, détecter et poursuivre sont claires et précises et limitées au strict nécessaire, conformément aux exigences rappelées en B.35.

B.52.1. Par contre, certaines finalités du traitement des données « PNR » s'ajoutent à celles qui sont prévues par la directive « PNR ». Il en va ainsi :

- de la « prévention des troubles graves à la sécurité publique dans le cadre de la radicalisation violente par le suivi des phénomènes et groupements conformément à l'article 44/5, § 1er, 2° et 3° et § 2, de la loi du 5 août 1992 sur la fonction de police » (article 8, § 1er, 3°);

- du « suivi des activités visées aux articles 7, 1° et 3°/1, et 11, § 1er, 1° à 3° et 5°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité » (article 8, § 1er, 4°);

- de l'amélioration des contrôles de personnes aux frontières extérieures et de la lutte contre l'immigration illégale (article 8, § 2).

B.52.2. Il convient d'examiner si ces autres finalités sont exprimées en des règles claires, précises et limitées au strict nécessaire, conformément aux exigences rappelées en B.35.

COPIE NON CORRIGÉE

B.53.1. En ce qui concerne la finalité de prévention des troubles graves à la sécurité publique dans le cadre de la radicalisation violente, visée à l'article 8, § 1er, 3°, de la loi du 25 décembre 2016, il est fait référence au suivi des « phénomènes » et « groupements » conformément à l'article 44/5, § 1er, 2° et 3°, et § 2, de la loi du 5 août 1992 « sur la fonction de police » (ci-après : loi du 5 août 1992).

L'article 44/1 de la loi du 5 août 1992 prévoit que, dans le cadre de l'exercice de leurs missions, les services de police peuvent traiter des informations et des données à caractère personnel.

Conformément à l'article 44/2 de la loi du 5 août 1992, lorsque l'exercice des missions de police administrative et de police judicaire nécessite que les services de police structurent ces données à caractère personnel et informations de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une banque de données policière opérationnelle (1° la banque de données Nationale Générale, 2° les banques de données de base ou 3° les banques de données particulières), selon les finalités propres à chaque catégorie de banques de données.

L'article 44/5, § 1er, 2° et 3° et § 2, de la loi du 5 août 1992 dispose :

« Les données à caractère personnel traitées dans les banques de données visées à l'article 44/2, § 1er, alinéa 2, 1° et 2°, aux fins de police administrative sont les suivantes :

[…]

2° les données relatives aux personnes impliquées dans les phénomènes de police administrative entendus comme, l'ensemble des problèmes, portant atteinte à l'ordre public et nécessitant des mesures appropriées de police administrative, parce qu'ils sont de même nature et répétitifs, qu'ils sont commis par les mêmes personnes ou qu'ils visent les mêmes catégories de victimes ou de lieux;

3° les données relatives aux membres d'un groupement national ou international susceptible de porter atteinte à l'ordre public tel que visé à l'article 14;

[…]

§ 2. La liste des phénomènes visés au § 1er, 2°, et des groupements visés au § 1er, 3°, est établie au moins annuellement par le ministre de l'Intérieur, sur la base d'une proposition conjointe de la police fédérale, de l'Organe de coordination pour l'analyse de la menace et des services de renseignements et de sécurité ».

COPIE NON CORRIGÉE

B.53.2. En ce qui concerne la finalité visée à l'article 8, § 1er, 3°, l'exposé des motifs indique :

« La troisième finalité s'inscrit dans le cadre de l'exercice des missions de police administrative des services de police.

Conformément à la loi sur la fonction de police, les services de police peuvent, dans le cadre de l'exercice de leurs missions de police administrative, traiter les données à caractère personnel pour autant qu'elles soient adéquates, pertinentes et non excessives.

Cette finalité spécifique s'inscrit dans une perspective d'approche globale du phénomène lié à la radicalisation violente ayant une incidence directe sur la protection des intérêts défendus par le présent avant-projet de loi.

La Circulaire GPI 78 du 31 janvier 2014 définit le radicalisme violent comme ' un processus par lequel un individu ou un groupe est influencé de sorte que l'individu ou le groupe en question soit mentalement prêt à commettre des actes extrémistes, ces actes allant jusqu'à être violents ou même terroristes '.

Il est essentiel que dans le cadre du suivi du radicalisme ou de groupements y liés présentant une menace grave pour l'ordre public, les données des passagers puissent également être utilisées d'une manière limitée. On peut penser par exemple à la venue sur notre territoire lors d'événements planifiés ou non de membres d'un groupe prônant des thèses extrémistes opposées aux valeurs et principes démocratiques.

L'information traitée à cette occasion doit uniquement servir à prendre des mesures afin de garantir l'ordre public. Si, par exemple, on apprend qu'une trentaine de membres d'un tel groupement a l'intention de se rendre en Belgique pour un rassemblement, des mesures plus adaptées en matière de maintien de l'ordre public pourront être prises (renforcement du dispositif, moyens spéciaux,…).

Dans cette optique, cette finalité est extrêmement limitée dans son application.

En effet, seul le phénomène de la radicalisation violente et les groupements y liés tels que mentionnés dans une liste fermée, établie annuellement par le ministre de l'Intérieur, après avis de la Police fédérale, l'OCAM, et les services de renseignement et de sécurité, peuvent fonder le traitement. Il ne s'agira dès lors pas de traiter les données des passagers pour n'importe quel événement ou menace de trouble à l'ordre public.

En outre, l'article 24, § 3, en projet limite fortement les modes, les conditions de traitement et exclut l'utilisation de profils de risques de cette finalité. L'article 27 exclut la recherche ponctuelle de cette finalité (*cfr infra*) » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, pp. 18-19).

COPIE NON CORRIGÉE

Le ministre de la Sécurité et de l'Intérieur a aussi précisé que la notion de radicalisation violente doit « être entendue au sens de la circulaire » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/003, p. 31).

B.53.3. Il ressort de ce qui précède que la finalité de prévention des troubles graves à la sécurité publique dans le cadre de la radicalisation violente est limitée à une menace grave pour l'ordre public, découlant de la radicalisation violente au sens de la circulaire ministérielle GPI 78 du 31 janvier 2014 « relative au traitement de l'information au profit d'une approche intégrée du terrorisme et de la radicalisation violente par la police » (ci-après : la circulaire ministérielle).

B.53.4. Cette finalité fait par ailleurs l'objet, dans le cadre de l'évaluation préalable des passagers, d'un traitement plus limité que les autres finalités de prévention et de recherche des infractions pénales visées à l'article 8, § 1er, de la loi du 25 décembre 2016.

Ainsi, l'article 24, § 3, de la loi du 25 décembre 2016 prévoit que, dans le cadre des finalités visées à l'article 8, § 1er, 3°, « l'évaluation préalable des passagers repose sur une correspondance positive, résultant d'une corrélation des données des passagers avec les banques de données visées au § 2, 1° ». En outre, l'article 26, § 1er, de la loi du 25 décembre 2016 prévoit que, pour la finalité visée à l'article 8, § 1er, 3°, seules les données des passagers visées à l'article 9, § 1er, 18° (données « API »), relatives à la ou les personnes pour lesquelles une correspondance positive est générée sont accessibles. Enfin, l'article 27 de la loi du 25 décembre 2016 exclut de procéder à des recherches ponctuelles aux fins visées à l'article 8, § 1er, 3°.

Les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« Le § 3 de l'article 24 concerne l'évaluation préalable dans le cadre de la finalité relative au suivi des phénomènes de police administrative et des groupements lié à la radicalisation violente.

COPIE NON CORRIGÉE

Cette finalité est soumise à des conditions beaucoup plus restrictives que les autres finalités. L'évaluation préalable dans ce cadre ne peut se baser que sur une corrélation avec les banques de données des services de police. Aucun critère préétabli ne peut être appliqué. Ces conditions limitatives se justifient par le fait que le traitement est généralement lié à l'éventuelle prise de mesure immédiate pour assurer l'ordre public. Il est par exemple indispensable que les services soient informés de la venue sur notre territoire d'une personne figurant sur la liste d'un groupement à suivre. On rappellera à ce sujet que l'établissement de ces listes est soumis à des conditions strictes et que seules les personnes présentant une menace grave pour l'ordre public en lien avec la radicalisation violente s'y retrouvent. La simple participation à une manifestation par exemple antimondialiste ne constitue pas un critère suffisant » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 30).

B.53.5. Si les notions de « phénomènes » et de « groupements » sont définies à l'article 44/5, § 1er, 2° et 3°, et § 2, de la loi du 5 août 1992, il n'en va toutefois pas de même de la notion de « radicalisation violente », qui n'est pas définie légalement.

Néanmoins, l'article 3, 15°, de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » (ci-après : la loi du 30 novembre 1998) définit le « processus de radicalisation » comme « un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ».

Par ailleurs, l'article M.1. de la circulaire ministérielle définit la « radicalisation violente » en ces termes :

« La radicalisation violente est un processus par lequel un individu ou un groupe est influencé de sorte que l'individu ou le groupe en question soit mentalement prêt à commettre des actes extrémistes, ces actes allant jusqu'à être violents ou même terroristes. L'adjectif ' violent ' est dans ce cas utilisé pour établir une distinction claire entre d'une part les idées non punissables et leur expression et, d'autre part, les infractions ou actes qui représentent un danger pour la sécurité publique commis pour réaliser ces idées ou l'intention de commettre ces infractions ou actes.

Par violence extrémiste, on entend la violence contre les personnes ou les biens commise par motivation idéologique, politique ou religieuse sans toutefois répondre à la définition pénale du terrorisme ».

COPIE NON CORRIGÉE

Bien que la notion de « radicalisation violente » ne soit pas définie légalement, sa définition par le biais de la circulaire ministérielle indique qu'elle est appréhendée au travers des notions de « phénomènes » et de « groupements », légalement définies à l'article 44/5, § 1er, 2° et 3°, et § 2, de la loi du 5 août 1992. Une telle mesure n'est donc pas dépourvue de clarté et de précision.

B.53.6. Cette définition fait en outre apparaître que la radicalisation violente, appréhendée au travers de « phénomènes » et de « groupements », est en lien direct avec des actes de terrorisme ou des formes graves de criminalité, que tant la directive « PNR » que la loi du 25 décembre 2016 visent à prévenir, détecter et poursuivre.

Une telle mesure est donc claire et précise et n'est pas disproportionnée eu égard aux objectifs légitimes poursuivis en l'espèce.

B.54.1. Conformément à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016, le traitement des données « PNR » tend au suivi des activités visées aux articles 7, 1° et 3°/1, et 11, § 1er, 1° à 3° et 5°, de la loi du 30 novembre 1998.

L'article 7 de la loi du 30 novembre 1998 dispose :

« La Sûreté de l'Etat a pour mission :

1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité;

[…]

3°/1 de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge;

[…] ».

L'article 11, § 1er, de la loi du 30 novembre 1998 dispose :

COPIE NON CORRIGÉE

« Le Service Général du Renseignement et de la Sécurité a pour mission :

1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer :

a) l'intégrité du territoire national ou la population,

b) les plans de défense militaires,

c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,

d) l'accomplissement des missions des Forces armées,

e) la sécurité des ressortissants belges à l'étranger,

f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité;

et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense;

2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés;

3° de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense nationale gère;

[…]

5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge ».

COPIE NON CORRIGÉE

B.54.2. En ce qui concerne cette finalité, l'exposé des motifs indique :

« La quatrième finalité a trait aux compétences des services de renseignement, à savoir, la Sûreté de l'État et le Service général de Renseignement et de Sécurité (SGRS). Afin de mener leurs missions de recherche, d'analyse et de traitement des renseignements relatifs aux activités susceptibles de menacer les intérêts fondamentaux de l'État, ces services doivent être en mesure d'analyser les données des passagers afin de détecter le plus tôt possible des menaces concrètes, suivre les déplacements de personnes précises ou d'établir des analyses de phénomènes ou tendances plus larges. Les missions concernant la recherche, l'analyse et le traitement des renseignements relatifs aux activités des services de renseignement étrangers sur le territoire belge entrent dans cette finalité.

La Sûreté de l'État joue un rôle indispensable dans la détection et la surveillance de *foreign fighters* et mais également dans d'autres activités déstabilisantes telles que celles liées aux organisations criminelles ou extrémistes.

Le SGRS exerce notamment des missions en rapport avec la protection de l'intégrité du territoire national, la protection de nos forces armées en mission à l'étranger et à l'égard de la sécurité des Belges à l'étranger.

Enfin, l'action des services de renseignement participe également dans de nombreux cas, à la réponse policière et judiciaire en aval au regard de la première finalité » (*ibid.*, pp. 19-20).

B.54.3. Si les missions des services de renseignement et de sécurité participent, de manière générale, à la sécurité nationale et internationale, le traitement des données « PNR » à l'aune de la finalité visée à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016 semble très vague et général.

Cette finalité fait en outre l'objet, en ce qui concerne l'évaluation préalable des passagers, du même traitement que les finalités visées aux articles 8, § 1er, 1°, 2° et 5°, de la loi du 25 décembre 2016 (articles 24, § 2, et 26, § 2).

B.54.4. Dans ce contexte, il convient, pour juger si cette finalité est suffisamment claire, précise et limitée au strict nécessaire, de poser à la Cour de justice de l'Union européenne la cinquième question préjudicielle figurant dans le dispositif.

COPIE NON CORRIGÉE

B.55.1. Enfin, l'article 8, § 2, de la loi du 25 décembre 2016 permet de traiter les données « PNR » en vue de l'amélioration des contrôles de personnes aux frontières extérieures, et plus précisément en vue de lutter contre l'immigration illégale, dans les conditions prévues au chapitre 11 (articles 28 à 31) de la loi du 25 décembre 2016.

B.55.2. En ce qui concerne cette finalité, l'exposé des motifs indique :

« La participation des services de police et de l'Office des étrangers dans la gestion des phénomènes de radicalisation violente, des ' *foreign fighters* ', des ' *returnees* ' et dans la lutte contre le terrorisme et la grande criminalité, telle que la traite et le trafic d'êtres humains, est nécessaire et incontournable.

[…]

Il est donc primordial que les services de police et l'Office des étrangers puissent utiliser certaines données de passagers dans le cadre du contrôle aux frontières extérieures et sur le territoire ainsi que dans le cadre des procédures de séjour et d'asile.

Ils auront donc accès à certaines données de passagers et ce, pendant une durée limitée. Le but est que les services de police et l'Office des étrangers soient en mesure d'exercer leurs missions légales correctement, tout en garantissant un niveau de protection des données personnelles suffisant au regard des objectifs poursuivis.

La banque de données des passagers constitue un outil indispensable à leur action. Les données de passagers auxquelles ils auront accès ou qui devront leur être transmises sont de nature à les aider à l'accomplissement de leurs tâches, telles que : l'identification des personnes, la vérification de l'authenticité et de la validité des documents ayant servi à entrer en Belgique, à y séjourner ou à quitter le pays (document d'identité, passeport, visas, document ou titre de séjour, billets de transport, etc.), la vérification des déclarations des personnes concernées, la motivation et l'exécution des décisions prises en la matière.

Elles seront donc utilisées dans les procédures de visa, lors des contrôles effectués aux frontières extérieures et sur le territoire, pour le suivi du séjour ou encore pour l'exécution des mesures d'éloignement. Elles pourront servir également dans les procédures d'asile, pour la détermination de l'État responsable de la demande d'asile et pour la prise de décision, y compris pour le retrait du statut de réfugié ou de la protection subsidiaire » (*ibid.*, pp. 9-10).

« Le paragraphe 2 autorise le traitement des données des passagers en matière de migration et d'asile.

COPIE NON CORRIGÉE

Les autorités compétentes en la matière pourront donc traiter ces données dans l'exercice des missions qui leur sont attribuées, en particulier dans le but d'améliorer le contrôle des frontières et de lutter contre l'immigration illégale.

Ce traitement aura lieu dans les limites fixées prévues au chapitre XI » (*ibid.*, p. 20).

« Les finalités du traitement des données de passagers sont identiques à celles de la directive 2004/82/CE. Il ressort clairement de ses considérants et de son dispositif qu'elle vise essentiellement le contrôle des flux migratoires, la lutte contre l'immigration illégale, l'amélioration des contrôles aux frontières extérieures et la protection de l'ordre public et de la sécurité nationale » (*ibid.*, p. 33).

La section de législation du Conseil d'État a également fait observer :

« Les articles 28 et 29, faisant partie du chapitre XI – Du traitement des données des passagers en vue de l'amélioration du contrôle au(x) frontière(s) et de la lutte contre l'immigration illégale, de l'avant-projet, font usage de la notion de ' frontières extérieures ' de la Belgique. Cette notion de frontières extérieures est définie à l'article 2, b), de la directive 2004/82/CE, que transpose plus spécifiquement le chapitre XI de l'avant-projet » (*ibid.*, p. 97).

B.55.3. Le traitement des données des passagers en ce qui concerne la finalité visée à l'article 8, § 2, est encadré par les articles 28 à 31 de la loi du 25 décembre 2016.

Seules les données des passagers visées à l'article 9, § 1er, 18°, de la loi du 25 décembre 2016 sont transmises aux services de police visés à l'article 14, § 1er, 2°, *a)*, et à l'Office des étrangers pour leur permettre d'exercer leurs missions légales (article 29). Seuls sont concernés les passagers qui envisagent d'entrer ou sont entrés sur le territoire par les frontières extérieures de la Belgique (article 29, § 2, 1°), les passagers qui envisagent de quitter ou ont quitté le territoire par les frontières extérieures de la Belgique (article 29, § 2, 2°) et les passagers qui envisagent de passer par, se trouvent dans ou sont passés par une zone internationale de transit située en Belgique (article 29, § 2, 3°).

COPIE NON CORRIGÉE

Ces données sont transmises, immédiatement après leur enregistrement dans la banque de données des passagers, aux services de police visés à l'article 14, § 1er, 2°, *a)*, et à l'Office des étrangers lorsqu'il en a besoin pour l'exercice de ses missions légales; ces données sont conservées dans un fichier temporaire et détruites dans les vingt-quatre heures qui suivent la transmission (article 29, §§ 3 et 4). L'Office des étrangers peut également, à l'expiration de ce délai, adresser une requête dûment motivée à l'UIP afin d'accéder à ces données (article 29, § 4, alinéa 2). L'Office des étrangers transmet mensuellement un rapport à la Commission de la protection de la vie privée - devenue l'Autorité de protection des données - concernant l'application de l'article 29, § 4, l'alinéa 2 (article 29, § 4, alinéa 3).

Un protocole précisant les modalités techniques de sécurisation, d'accès et de transmission des données des passagers aux services de police chargés du contrôle aux frontières et à l'Office des étrangers doit être conclu, en concertation avec le délégué à la protection des données et après avis de la Commission de la protection de la vie privée (Autorité de protection des données) entre le fonctionnaire dirigeant de l'UIP, d'une part, et le Commissaire général de la police fédérale et le fonctionnaire dirigeant de l'Office des étrangers, chacun en ce qui le concerne, d'autre part (article 30).

Dans les vingt-quatre heures après la fin du transport, visé à l'article 4, 3° à 6°, les transporteurs et les opérateurs de voyage détruisent toutes les données des passagers visées à l'article 9, § 1er, 18°, qu'ils transfèrent conformément à l'article 7 (article 31, tel qu'il a été modifié par la loi du 15 juillet 2018).

B.55.4. Il résulte de ce qui précède que seules les données « API », visées à l'article 9, § 1er, 18°, de la loi du 25 décembre 2016, de certaines catégories de passagers peuvent être traitées à l'aune de la finalité, liée à la lutte contre l'immigration illégale et le contrôle aux frontières extérieures, mentionnée à l'article 8, § 2, de la loi du 25 décembre 2016, dans les conditions prévues au chapitre 11 de la loi du 25 décembre 2016.

Comme l'indiquent les travaux préparatoires cités en B.55.2, une telle mesure s'inscrit dans le cadre de la transposition de la directive 2004/82/CE, dont l'objectif est, comme l'indique son premier considérant, de lutter efficacement contre l'immigration clandestine et d'améliorer les contrôles aux frontières. Plus précisément, le chapitre 11 de la loi du 25 décembre 2016 reprend, en l'adaptant, le contenu de l'arrêté royal du 11 décembre 2006 « concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers », qui, avant son abrogation par l'arrêté royal du 18 juillet 2017, transposait en droit interne la directive 2004/82/CE.

B.55.5. Compte tenu des différentes limites, énumérées en B.55.3, qui entourent le traitement des données à l'aune de la finalité visée à l'article 8, § 2, cette mesure est suffisamment claire, précise et limitée au strict nécessaire et n'est donc pas disproportionnée.

6. *La gestion de la banque de données des passagers et le traitement des données dans le cadre de l'évaluation préalable des passagers et des recherches ponctuelles (articles 12 à 16 et 24 à 27 et 50 et 51)*

B.56. La partie requérante estime que les différents traitements et flux de données à caractère personnel sont manifestement disproportionnés.

D'une part, elle critique la création de la banque de données des passagers, gérée par l'UIP, au sein du SPF Intérieur en vue de l'échange des informations avec les UIP étrangères et Europol. Elle estime que le traitement des données des passagers ne nécessitait pas la création d'une banque de données.

D'autre part, elle critique la corrélation entre les bases de données et la méthode de « *pre-screening* », laquelle devrait être effectuée sur la base de critères préétablis servant d'indicateurs de la menace.

Enfin, elle critique le fait que les membres détachés des services compétents pourront se prononcer sur une requête d'accès individuelle dans le cadre de recherches ponctuelles.

COPIE NON CORRIGÉE

B.57.1. En vertu de l'article 4, paragraphe 1, de la directive « PNR », chaque État membre met en place ou désigne une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, ou crée ou désigne une antenne d'une telle autorité, en tant que son UIP.

Conformément à l'article 4, paragraphe 2, de la directive « PNR », l'UIP est chargée :

« a) de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement aux autorités compétentes visées à l'article 7;

b) de l'échange à la fois des données PNR et du résultat de leur traitement avec les UIP d'autres États membres et avec Europol, conformément aux articles 9 et 10 ».

B.57.2. En ce qui concerne le traitement des données, l'article 6 de la directive « PNR » dispose :

« 1. Les données PNR transférées par les transporteurs aériens sont recueillies par l'UIP de l'État membre concerné comme prévu à l'article 8. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données immédiatement et de façon définitive dès leur réception.

2. L'UIP ne traite les données PNR qu'aux fins suivantes :

a) réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes visées à l'article 7 et, le cas échéant, par Europol conformément à l'article 10, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité;

b) répondre, au cas par cas, aux demandes dûment motivées fondées sur des motifs suffisants des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière, et visant à communiquer aux autorités compétentes ou, le cas échéant, à Europol le résultat de ce traitement; et

c) analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées au titre du paragraphe 3, point b), en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité.

CORRIGÉE

3. Lorsqu'elle réalise l'évaluation visée au paragraphe 2, point a), l'UIP peut :

a) confronter les données PNR aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière, y compris les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données; ou

b) traiter les données PNR au regard de critères préétablis.

4. L'évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci effectuée au titre du paragraphe 3, point b), au regard de critères préétablis est réalisée de façon non discriminatoire. Ces critères préétablis doivent être ciblés, proportionnés et spécifiques. Les États membres veillent à ce que ces critères soient fixés et réexaminés à intervalles réguliers par les UIP en coopération avec les autorités compétentes visées à l'article 7. Lesdits critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

5. Les États membres s'assurent que toute concordance positive obtenue à la suite du traitement automatisé des données PNR effectué au titre du paragraphe 2, point a), est réexaminée individuellement par des moyens non automatisés, afin de vérifier si l'autorité compétente visée à l'article 7 doit prendre des mesures en vertu du droit national.

6. L'UIP d'un État membre transmet, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au paragraphe 2, point a), ou le résultat du traitement de ces données aux autorités compétentes visées à l'article 7 de ce même État membre. Ces transferts ne sont effectués qu'au cas par cas et, en cas de traitement automatisé des données PNR, après un réexamen individuel par des moyens non automatisés.

7. Les États membres veillent à ce que le délégué à la protection des données ait accès à toutes les données traitées par l'UIP. Si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, le délégué à la protection des données peut renvoyer l'affaire à l'autorité de contrôle nationale.

8. Le stockage, le traitement et l'analyse des données PNR par les UIP sont effectués exclusivement dans un ou des endroits sécurisés situés sur le territoire des États membres.

9. Les conséquences des évaluations des passagers visées au paragraphe 2, point a), du présent article ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union à la libre circulation sur le territoire de l'État membre concerné prévu dans la directive 2004/38/CE du Parlement européen et du Conseil. En outre, lorsque des évaluations sont réalisées pour des vols intra-UE entre des États membres auxquels s'applique le règlement (CE) n° 562/2006 du Parlement européen et du Conseil, les conséquences de ces évaluations doivent respecter ledit règlement ».

a) La gestion de la banque de données des passagers par l'UIP (articles 12 à 16)

B.58.1. En vertu de l'article 5 de la loi du 25 décembre 2016, chaque transporteur et opérateur de voyage recueille et transmet les données des passagers à destination de, en provenance de et transitant par le territoire national, dont il dispose, en vue de leur enregistrement dans la banque de données passagers visée à l'article 15. En vertu de l'article 6 de la loi du 25 décembre 2016, les transporteurs et les opérateurs de voyage informent les personnes concernées que leurs données sont transmises à l'UIP et peuvent être traitées ultérieurement pour les finalités visées à l'article 8.

Cette banque de données des passagers est gérée par l'UIP, créée au sein du Service public fédéral Intérieur (article 12). L'UIP est chargée de la collecte, de la conservation et du traitement des données des passagers, ainsi que de la gestion de la banque de données des passagers, et de l'échange des données et des résultats de leur traitement avec les UIP d'autres États membres de l'Union européenne et avec Europol (article 13). L'UIP est composée d'un fonctionnaire dirigeant, assisté par un service d'appui, et de membres détachés issus des services compétents (article 14).

B.58.2. Conformément à l'article 15, § 1er, de la loi du 25 décembre 2016, il est créé une banque de données des passagers gérée par le Service public fédéral Intérieur dans laquelle sont enregistrées les données des passagers. Le fonctionnaire dirigeant de l'UIP est le responsable du traitement de la banque de données des passagers au sens de l'article 1er, § 4, de la loi du 8 décembre 1992 « relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel » (article 15, § 2).

Les traitements des données des passagers effectués en vertu de la loi attaquée sont soumis à la loi du 8 décembre 1992 précitée (article 15, § 4).

Dans le cadre des finalités visées à l'article 8, § 1er, la banque de données des passagers est directement accessible par l'UIP pour les traitements visés aux articles 24 à 27, conformément aux dispositions prévues au chapitre 9 (article 16). Le chapitre 9, qui contient les articles 18 à 23, de la loi du 25 décembre 2016 prévoit les délais de conservation des données des passagers.

COPIE NON CORRIGÉE

Un protocole d'accord mettant en oeuvre les modalités techniques de sécurisation et d'accès est conclu par le fonctionnaire dirigeant de l'UIP et les services compétents après concertation avec le délégué à la protection des données et après avis de l'autorité compétente de contrôle des traitements de données à caractère personnel (article 17, tel qu'il a été remplacé par la loi du 15 juillet 2018).

B.58.3. En ce qui concerne la création de la banque de données des passagers, les travaux préparatoires exposent :

« Le premier paragraphe prévoit la création d'une Banque de données des passagers. En effet, pour traiter et analyser les données des passagers visées à l'article 9, il est nécessaire de les traiter dans une banque de données spécifique, afin de pouvoir les structurer, les exploiter et les détruire après un délai déterminé.

Étant donné que le but ultime du traitement des données consiste à assurer la sécurité des citoyens, la banque de données est gérée par le SPF Intérieur. Le fonctionnaire dirigeant est désigné comme responsable du traitement de cette banque de données tel que visé à l'article 1er, § 4, de la Loi sur la Protection des données à caractère personnel. Il sera par conséquent responsable, dans le cadre établi par la loi, de la rédaction et du suivi des plans stratégiques pour le traitement des données et déterminera les moyens nécessaires pour atteindre ses objectifs stratégiques » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 24).

B.59.1. En créant une banque de données des passagers, dont la gestion est confiée à l'UIP, la loi du 25 décembre 2016 organise une centralisation du stockage des données des passagers, sous la responsabilité de l'UIP, tout en prévoyant de nombreuses garanties quant à la sécurisation, à l'accès et à la conservation de ces données et en limitant les traitements des données pouvant être effectués par l'UIP dans le cadre des finalités visées par l'article 8, § 1er. En identifiant précisément le lieu d'enregistrement de ces données, la création d'une telle banque de données permet ainsi de limiter les flux de données.

Bien qu'elle ne soit pas prévue expressément par la directive « PNR », la création d'une banque de données des passagers, telle qu'elle est assortie des garanties rappelées en B.58, constitue un élément essentiel du système mis en place par la directive « PNR », que la loi du 25 décembre 2016 transpose.

COPIE NON CORRIGÉE

B.59.2. Compte tenu de ce qui précède et des différentes garanties, énumérées en B.58, qui entourent la création et la gestion de la banque de données des passagers, cette mesure n'est pas disproportionnée.

b) Le traitement des données des passagers dans le cadre de l'évaluation préalable des passagers (articles 24 à 26)

B.60.1. L'article 16 de la loi du 25 décembre 2016 prévoit que, dans le cadre des finalités visées à l'article 8, § 1er, les données des passagers font l'objet des traitements visés aux articles 24 à 27.

Les articles 24 à 26 concernent le traitement des données des passagers dans le cadre de l'évaluation préalable des passagers.

B.60.2. Conformément à l'article 24, § 1er, de la loi du 25 décembre 2016, les données des passagers sont traitées en vue de la réalisation d'une évaluation préalable des passagers avant leur arrivée, leur départ ou leur transit prévu sur le territoire national afin de déterminer quelles personnes doivent être soumises à un examen plus approfondi (article 24, § 1er).

Les travaux préparatoires de la loi du 25 décembre 2016 expliquent :

« L'article 24 concerne l'évaluation (pré-screening) du risque représenté par les passagers. Il s'agit d'évaluer la menace potentielle et de déterminer quels passagers présentent un intérêt pour l'exercice de leurs missions ou par exemple nécessitent une mesure à prendre (exécution d'un mandat d'arrêt, fouille,…).

Cette évaluation préalable s'applique avant l'arrivée, le transit ou le départ du territoire national » (*ibid.*, p. 28).

B.60.3.1. L'évaluation préalable repose sur deux axes : d'une part, la corrélation des données des passagers avec les banques de données, et, d'autre part, la corrélation des données avec des critères préétablis.

COPIE NON CORRIGÉE

Cette évaluation repose sur une correspondance positive, résultant d'une corrélation des données des passagers avec :

- les banques de données gérées par les services compétents et des critères d'évaluation préétablis par l'UIP, dans le cadre des finalités visées à l'article 8, § 1er, 1°, 2°, 4° et 5°, ou relatives aux menaces mentionnées aux articles 8, 1°, a), b), c), d), f), g) et 11, § 2, de la loi du 30 novembre 1998 (article 24, § 2, tel qu'il a été remplacé par la loi du 15 juillet 2018); pour ces finalités, toutes les données des passagers visées à l'article 9 sont accessibles (article 26, § 2, tel qu'il a été remplacé par la loi du 15 juillet 2018);

- les banques de données gérées par les services compétents, dans le cadre des finalités visées à l'article 8, § 1er, 3° (article 24, § 3). Pour cette finalité, seules les données des passagers visées à l'article 9, § 1er, 18° relatives à la ou les personnes pour lesquelles une correspondance positive est générée sont accessibles (article 26, § 1er).

La correspondance positive est validée par l'UIP dans les vingt-quatre heures après réception de la notification automatisée de la correspondance positive (article 24, § 4). Dès le moment de cette validation, le service compétent, qui est à l'origine de cette correspondance positive, donne une suite utile le plus rapidement possible (article 24, § 5).

Enfin, l'article 24, § 2, de la loi du 25 décembre 2016 a été complété par un nouvel alinéa, en vertu de l'article 5 de la loi du 2 mai 2019. Cette modification « vise à prévoir dans l'article 24, § 2, que l'évaluation préalable des passagers repose également sur une analyse des autres données des passagers liées à une correspondance positive » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3652/001, p. 5).

B.60.3.2. En ce qui concerne la corrélation avec les banques de données, les travaux préparatoires de la loi du 25 décembre 2016 exposent :

COPIE NON CORRIGÉE

« Le premier axe consiste en la recherche de correspondances positives par le biais de corrélations des données de passagers avec les données traitées dans les banques de données gérées par les services compétents. Cela permet par exemple d'évaluer si une personne présente un degré élevé de dangerosité, car elle est connue dans une banque de données policière dans le cadre d'un dossier terroriste et pour laquelle il appert de l'analyse de ses données passager, que cette dernière se rend régulièrement dans des pays abritant des camps d'entraînement pour terroristes ou dans des pays de transit vers de tels lieux. Il peut par exemple s'agir également d'une personne à propos de laquelle des renseignements disponibles auprès des services de renseignements indiquent qu'elle préparerait une prise d'otage et qu'elle se rend, sur la base des données de transport, dans un pays dont les services de renseignements savent, sur base des informations reçues, que cette personne pourrait y recruter afin de mettre ses plans à exécution. En outre, plus les correspondances positives découvertes par plusieurs services sont nombreuses pour une seule et même personne, plus la probabilité de menace est réelle.

La correspondance positive peut également requérir la prise d'une mesure sur ordre des autorités judiciaires, telle que l'exécution d'un mandat d'arrêt d'une personne qui s'apprête à quitter la Belgique.

La correspondance positive peut également ressortir d'une corrélation avec des banques de données internationale telles que SIS II, Interpol (SLTD).

L'objectif n'est naturellement pas de lier l'ensemble des banques de données des services avec la banque de données des passagers mais bien de limiter techniquement les corrélations avec les banques de données en relation directe avec les finalités telles que déterminées par la loi.

[…]

Cette corrélation pourra également se faire via des listes de personnes élaborées spécifiquement par les services compétents à cette fin. Conformément à la loi sur la protection de la vie privée et plus particulièrement, à son article 4, § 1er, 4°, ces listes devront être mises à jour régulièrement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 28-29).

En ce qui concerne la corrélation avec des critères préétablis, les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« Le deuxième axe consiste en la recherche de correspondances positives par le biais de critères préétablis par l'UIP (un ou plusieurs) appliqués aux données des passagers. Ces critères sont composés d'un ou de plusieurs indicateurs objectifs sur la base desquels il peut être déduit que les personnes qui en font l'objet, présentent un comportement à risque spécifique susceptible de constituer une menace au regard des finalités à l'article 8, § 1er, points 1, 4 et 5, de la loi.

Ces critères peuvent intégrer, par exemple, certains comportements spécifiques en matière de réservation ou de voyage.

COPIE NON CORRIGÉE

Leur utilisation présente l'avantage de pouvoir faire émerger des profils de passagers à risque qui ne sont pas nécessairement connus ou mentionnés dans les banques de données des services.

Ces critères peuvent concerner, par exemple, un pays de destination ou de départ, combiné à certaines informations sur le voyage telles que le mode de payement et la date de réservation » (*ibid.*, pp. 29-30).

« L'évaluation préalable réalisée dans le cadre de la finalité relative au suivi des phénomènes de police administrative et des groupements lié à la radicalisation violente est soumise à des conditions beaucoup plus restrictives que les autres finalités :

- elle ne peut se baser que sur une corrélation avec les banques de données des services de police;

- Seules les données visées à l'article 9, § 1er, 18° de la loi sont accessibles.

L'évaluation préalable réalisée dans le cadre des autres finalités se voit autoriser l'accès à toutes les données des passagers énumérées à l'article 9 » (*ibid.*, p. 31).

« La correspondance positive doit dans tous les cas être validée par l'UIP. En effet, pour assurer le respect total du droit à la protection des données personnelles, et plus précisément de l'article 12*bis* de la loi sur la vie privée et le droit à la non-discrimination, aucune décision aux conséquences juridiques pour une personne ou susceptible de la préjudicier gravement ne peut être prise, sur la simple base du traitement automatisé des données du fichier contenant des informations sur son voyage. C'est pourquoi l'évaluation humaine précédera toujours toute décision contraignante pour la personne concernée.

Cette validation doit intervenir dans les 24 heures afin d'ouvrir le droit d'accès à la banque de données des passagers.

§ 5. Après la validation de la correspondance positive, les services qui sont à l'origine de cette correspondance assurent le suivi utile dans un délai approprié. Un suivi utile pourrait signifier une intervention active (fouille, arrestation …), mais il peut aussi s'agir de n'entreprendre provisoire aucune intervention active. Cette appréciation opérationnelle appartient pleinement aux services compétents » (*ibid.*, pp. 30-31).

B.60.4.1. En ce qui concerne les critères d'évaluation préétablis par l'UIP, l'article 25 de la loi du 25 décembre 2016 prévoit que ces critères ne peuvent pas être fondés sur des données qui révèlent l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à une organisation syndicale, son état de santé, sa vie sexuelle ou son orientation sexuelle (article 25, § 3).

COPIE NON CORRIGÉE

L'évaluation des passagers avant leur arrivée, leur transit ou leur départ au regard des critères préétablis est réalisée de façon non discriminatoire. Ces critères ne peuvent viser l'identification d'un individu et doivent être ciblés, proportionnés et spécifiques (article 25, § 2).

Les données des passagers peuvent être exploitées par l'UIP pour mettre à jour ou définir de nouveaux critères destinés à cibler des individus lors des évaluations préalables des passagers (article 25, § 1er).

B.60.4.2. Les travaux préparatoires de la loi du 25 décembre 2016 exposent à cet égard :

« Sur le plan technique, pour toutes les modalités de consultation, un principe uniforme de traitement est applicable : sur la base d'une corrélation avec un profil de risque opérationnel ou avec une banque de données ou sur la base d'une requête ponctuelle introduite par un service compétent, des ' *hits* ' sont générés à l'égard d'une entrée PNR unique. Ce *hit* est uniquement visible pour le service en question. Chaque hit doit être validé manuellement par le membre détaché issu du service compétent concerné pour être traduit dans un ' *match* '.

Dès qu'une correspondance positive est validée, un code d'encryptions est automatiquement généré qui sera croisé, aux codes de tous les services compétents. Si les deux codes coïncident, deux ou plusieurs services sont informés que des ' correspondances positives ' existent pour cette unique entrée PNR. Ces services doivent assurer le suivi utile dans un délai approprié » (*ibid.*, p. 23; voy. aussi *Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/003, p. 7).

« L'Article 25 détermine le troisième mode de traitement des données : l'UIP traite les données des passagers pour mettre à jour ou définir de nouveaux critères qui doivent être utilisés lors des évaluations préalables des passagers afin d'objectiver l'évaluation et, par conséquent, d'opérer une sélection rigoureuse des seuls passagers à risque.

Étant donné que le traitement des données des passagers implique une ingérence dans leur vie privée, la garantie d'une objectivation des critères prédéterminés permettra également de garantir le caractère adéquat, pertinent et non excessif de l'ingérence dans la vie privée.

Les critères préétablis doivent être ciblés, proportionnés et spécifiques. En outre, ils ne peuvent viser l'identification d'un individu en particulier. Par conséquent, il est précisé qu'ils ne sont pas nominatifs.

COPIE NON CORRIGÉE

Il ne peuvent en aucun cas être fondés sur des données 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 de l'intéressé » (*ibid.*, p. 31).

B.60.4.3. En ce qui concerne les critères d'évaluation préétablis, l'article 6, paragraphe 4, de la directive « PNR » exige que ces critères préétablis soient « ciblés, proportionnés et spécifiques », et que les États membres veillent à ce que ces critères soient « fixés et réexaminés à intervalles réguliers par les UIP ».

B.61.1. Le système d'évaluation préalable implique le croisement des données « PNR » de tous les passagers avec des banques de données ou des critères préétablis, en vue d'établir des correspondances.

Dans son avis du 19 août 2016 « sur les implications en matière de protection des données du traitement des données passagers », le Comité consultatif de la Convention n° 108 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » a observé à cet égard :

« Le traitement des données à caractère personnel peut concerner tous les passagers et pas seulement les individus ciblés soupçonnés d'être impliqués dans une infraction pénale ou de constituer une menace immédiate à la sécurité nationale ou à l'ordre public.

Les données PNR peuvent être comparées (' data matching ') à des bases de données (à savoir, des bases sur les personnes condamnées pour infractions pénales graves, les personnes visées par une enquête pour soupçon d'activités terroristes, les passeports volés ou perdus) tenues par les autorités compétentes conformément à la loi afin d'identifier les suspects ou auteurs d'infractions ainsi que les personnes liées à ces suspects ou auteurs d'infractions potentiels (« graphe social »).

Les données PNR peuvent aussi être traitées dans le but d'identifier (par ' data mining ') quiconque ' pourrait ' être impliqué ou s'engager dans les activités criminelles définies par la loi qui établit le partage des PNR avec les autorités compétentes comme, par exemple, les individus voyageant dans le but de devenir des combattants terroristes étrangers. Cela pourrait être obtenu par l'exploration de données selon des sélecteurs ou des algorithmes prédictifs.

L'évaluation des passagers par la mise en correspondance de données peut soulever la question de la prévisibilité, en particulier lorsqu'elle est effectuée sur la base d'algorithmes prédictifs utilisant des critères dynamiques susceptibles d'évoluer en permanence selon les capacités d'auto-apprentissage.

COPIE NON CORRIGÉE

Le développement d'algorithmes d'exploration de données devrait se fonder sur les résultats d'évaluations régulières de l'impact probable du traitement de données sur les droits et libertés fondamentales des personnes concernées.

La structure de base des analyses devrait se fonder sur des indicateurs de risque prédéfinis ayant été clairement établis au préalable.

La pertinence des résultats individuels de ces évaluations automatiques devrait être examinée avec soin au cas par cas, par une personne et de façon non automatisée » (avis du 19 août 2016, T-PD(2016)18rev, p. 8).

B.61.2. En l'espèce, les banques de données visées à l'article 24 sont définies avec précision et sont en rapport direct avec les finalités visées à l'article 8 de la loi du 25 décembre 2016. Il s'agit en effet des banques de données des « services compétents », c'est-à-dire des services de police, de la Sûreté de l'État, du Service général de Renseignement et de Sécurité et des Douanes.

B.61.3. En outre, l'article 24, §§ 4 et 5, de la loi du 25 décembre 2016 garantit qu'en cas de concordance positive, le traitement systématique automatisé fait l'objet d'une vérification individuelle par des moyens non automatisés, afin d'apprécier si l'autorité compétente doit prendre des mesures en vertu du droit national, comme le requiert l'article 6, paragraphe 5, de la directive « PNR ».

Dans son avis n° 1/15 du 26 juillet 2017, la Cour de justice avait également insisté sur la nécessité d'un réexamen individuel par des moyens non automatisés avant l'adoption d'une mesure individuelle (CJUE, grande chambre, 26 juillet 2017, avis n° 1/15, point 173).

L'exigence d'une intervention humaine, après une correspondance positive, constitue une garantie qui est de nature à assurer que l'évaluation préalable ne repose pas uniquement sur des moyens automatisés, et participe ainsi à l'efficacité du système.

Une évaluation préalable systématique des passagers constitue dès lors, dans son principe, une mesure pertinente au regard de l'objectif qui consiste à identifier et à prévenir des menaces pour la sécurité publique.

COPIE NON CORRIGÉE

B.61.4. Comme la Cour de justice l'a toutefois constaté dans son avis n° 1/15 précité du 26 juillet 2017, les traitements découlant de l'évaluation préalable « sont susceptibles de fournir des informations supplémentaires sur la vie privée des passagers aériens » (CJUE, grande chambre, 26 juillet 2017, avis n° 1/15, point 131); en outre, « lesdites analyses sont effectuées sans qu'il existe des raisons fondées sur des circonstances individuelles permettant de considérer que les personnes concernées pourraient présenter un risque pour la sécurité publique » (*ibid.*, point 132).

Constatant que le traitement automatisé des données « PNR », fondé sur des modèles et critères préétablis, présente un taux d'erreur non négligeable (*ibid.*, points 169-170), la Cour de justice a toutefois considéré que « les modèles et les critères préétablis devraient être, d'une part, spécifiques et fiables, permettant d'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 et, d'autre part, non discriminatoires » et que « les bases de données avec lesquelles les données PNR sont recoupées doivent être fiables, actuelles et limitées à des bases de données exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave » (*ibid*., point 172). Enfin, pour garantir que cette évaluation ne présente pas un caractère discriminatoire et soit limitée au strict nécessaire, la Cour de justice a considéré que « la fiabilité et l'actualité de ces modèles et de ces critères préétablis ainsi que des bases de données utilisées devraient faire l'objet, en tenant compte de données statistiques et des résultats de la recherche internationale, de l'examen conjoint de la mise en œuvre de l'accord envisagé », un an après son entrée en vigueur, puis à intervalles réguliers (*ibid.*, point 174).

B.61.5. Pour le surplus, il apparaît techniquement impossible de définir davantage les critères préétablis qui serviront à la détermination de profils à risque. Comme il a été dit en B.61.4, ces critères doivent être spécifiques, fiables et non discriminatoires.

Bien que ni la directive « PNR » ni la loi du 25 décembre 2016 ne donnent des indications quant à la manière dont les critères à la base de l'évaluation préalable sont préétablis par l'UIP, les garanties qui entourent l'élaboration de ces critères, rappelées en B.60.4, apparaissent suffisantes pour que la mesure attaquée ne soit pas jugée disproportionnée.

B.61.6. Il convient toutefois, afin de décider si cette évaluation préalable systématique est suffisamment claire, précise et limitée au strict nécessaire, de poser à la Cour de justice de l'Union européenne la sixième question préjudicielle figurant dans le dispositif.

c) Les recherches ponctuelles (articles 27, 50 et 51)

B.62.1. L'article 27 de la loi du 25 décembre 2016, dans sa version initiale, autorise le traitement des données des passagers en vue de procéder à des recherches ponctuelles aux fins visées à l'article 8, § 1er, 1°, 2°, 4° et 5°, et aux conditions prévues à l'article 46*septies* du Code d'instruction criminelle ou à l'article 16/3 de la loi du 30 novembre 1998, insérés respectivement par les articles 50 et 51 de la loi du 25 décembre 2016.

Conformément à l'article 20 de la loi du 25 décembre 2016, les conditions d'application de l'article 27 valent également pour les demandes d'accès à l'expiration du délai de six mois prévu à l'article 19.

B.62.2. Tel qu'il a été inséré par l'article 50 de la loi du 25 décembre 2016, l'article 46*septies* du Code d'instruction criminelle dispose :

« En recherchant les crimes et délits visés à l'article 8, § 1er, 1°, 2° et 5°, de la loi du 25 décembre 2016 relative au traitement des données des passagers, le procureur du Roi peut, par une décision écrite et motivée, charger l'officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

COPIE NON CORRIGÉE

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.

La mesure peut porter sur un ensemble de données relatives à une enquête spécifique. Dans ce cas, le procureur du Roi précise la durée de la mesure qui ne peut excéder un mois à dater de la décision, sans préjudice de renouvellement.

En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et, par une décision motivée et écrite, requérir du fonctionnaire dirigeant de l'UIP la communication des données des passagers. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur du Roi et motive par ailleurs l'extrême urgence ».

Cette disposition concerne donc des recherches ponctuelles dans le cadre de la finalité visée à l'article 8, § 1er, 1°, 2° et 5°, de la loi du 25 décembre 2016. Cette mesure est entourée de plusieurs garanties, dont l'autorisation préalable du procureur du Roi.

B.62.3. Tel qu'il a été inséré par l'article 51 de la loi du 25 décembre 2016, l'article 16/3 de la loi du 30 novembre 1998 dispose :

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, décider de façon dûment motivée d'accéder aux données des passagers visées à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

§ 2. La décision visée au § 1er est prise par le dirigeant du service et communiquée par écrit à l'Unité d'information des passagers visée au chapitre 7 de la loi précitée. La décision est notifiée au Comité permanent R avec la motivation de celle-ci.

Le Comite permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales.

La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, la liste des consultations des données des passagers est communiquée une fois par mois au Comité permanent R ».

Cette disposition concerne donc des recherches ponctuelles dans le cadre de la finalité visée à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016. Cette mesure est entourée de plusieurs garanties, dont l'information et le contrôle du Comité permanent R.

COPIE NON CORRIGÉE

B.62.4. En ce qui concerne les recherches ponctuelles, les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« L'article 27 détermine le mode de traitement qui consiste pour l'UIP à réagir au cas par cas aux demandes dûment motivées d'autorités compétentes visant à obtenir des données de passagers et le traitement de celles-ci dans des cas spécifiques. Ce mode de traitement est limité à quatre finalités et exclut celle liée au suivi des phénomènes de police administrative et des membres d'un groupement telle que prévue à l'article 8, § 1er, point 3.

L'hypothèse implique, selon les services, qu'un dossier d'enquête ou de renseignement est ouvert à la suite d'une évaluation préalable positive ou sur la base d'autres éléments concrets indépendants des données des passagers.

Par exemple, sur le plan policier, une enquête pénale est ouverte suite à une fouille positive d'un passager en possession de stupéfiants résultant d'une évaluation préalable ou suite à un contrôle de véhicule ou de personne sur la voie publique. Dans les deux cas, il peut s'avérer nécessaire de consulter les données des passagers ' rétroactivement ' pour les besoins de l'enquête afin de retracer les éventuels déplacements du suspect.

La consultation de la banque de données des passagers ne se fera plus ici à proprement parler sur la base des critères préétablis ou d'une corrélation automatique mais sur la base de recherches à l'aide d'éléments issus du dossier. Par exemple, un nom, le n° de passeport du suspect, n° de GSM, destination,…

Dans ce cadre, la nécessité de pouvoir remonter à un historique des données des passagers est plus cruciale encore compte tenu de la durée et complexité de certaines enquêtes, voire de la découverte d'infractions bien plus tard après les déplacements. C'est pour cette raison que les données doivent être accessibles sur une période de 5 ans afin de recueillir des preuves, de trouver d'éventuels co-auteurs ou complices et de démanteler des réseaux criminels.

Exemple : suite à de nouveaux éléments dans une enquête terrorisme, le magistrat traitant estime devoir consulter certaines données de voyage de suspects identifiés.

L'autorisation du procureur du Roi sera nécessaire à tout moment pour accéder à toutes les informations, y compris celles qui ont été masquées en ce qui concerne les finalités de l'article 8, § 1er, 1°, 2° et 5°. En ce qui concerne la finalité de l'article 8, § 1er, 4°, l'autorisation par le dirigeant du service comme requise dans l'article 51 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, pp. 32-33).

« Les articles 50 et 51 concernent les dispositions modifiant le Code d'instruction criminelle et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et relatives aux modalités d'accès aux données des passagers dans le cadre de l'analyse a posteriori » (*ibid.*, p. 43).

COPIE NON CORRIGÉE

B.63.1. La partie requérante estime que les membres détachés des services de police qui appartiennent à l'UIP ne seraient pas suffisamment indépendants pour répondre aux demandes d'accès dans le cadre de ces recherches ponctuelles.

B.63.2. En vertu de l'article 14, § 1er, de la loi du 25 décembre 2016, l'UIP est composée d'un fonctionnaire dirigeant, assisté par un service d'appui (article 14, § 1er, 1°), ainsi que de membres détachés, issus des Services de police, de la Sûreté de l'État, du Service général de Renseignement et de Sécurité et de l'Administration Enquête et Recherche et des services d'enquête, services de recherche et services chargés de la surveillance, du contrôle et de la constatation de l'Administration générale des Douanes et Accises (article 14, § 1er, 2°, tel qu'il a été modifié par la loi du 15 juillet 2018).

En ce qui concerne la composition de l'UIP, les travaux préparatoires exposent :

« Le modèle belge repose sur un concept d'unité multidisciplinaire composée d'un fonctionnaire dirigeant assurant une mission de direction, de membres administratifs et de membres détachés issus des services compétents.

L'UIP sera composé :

- d'un fonctionnaire dirigeant, assisté par un service d'appui, qui au sein du SPF Intérieur sera responsable notamment de la gestion de la banque de données, du respect des obligations des transporteurs et opérateurs de voyage, du rapportage, de la conclusion de protocoles avec les services compétents et du respect des conditions de traitement. Le service d'appui sera notamment composé d'analystes, juristes, experts ICT et du délégué à la protection des données, qui disposeront des habilitations de sécurité nécessaires.

- de membres détachés issus des services compétents limitativement énumérés par le point 2 du § 1er, à savoir : les services de police, les services de renseignement et la Douane. Les finalités précises constituent en tant que telles la première limitation. Par exemple, au niveau des services de la police intégrée, il est évident qu'un agent de quartier au sein d'une police locale ne pourra jamais prendre connaissance des données des passagers dès lors que les finalités ne rentrent pas dans ses missions.

Le détachement des services compétents a pour objectif de garantir un certain degré d'expertise mais n'exclut d'aucune façon des accords entre ceux-ci afin de mutualiser les détachements » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 22).

COPIE NON CORRIGÉE

Le ministre de la Sécurité et de l'Intérieur a également précisé :

« Au total, quinze personnes auront accès à ces données. Les quatre services compétents détacheront chacun deux personnes. Celles-ci viendront s'ajouter aux sept membres du personnel de l'UIP. Il sera également désigné un *data protection officer* chargé de faire rapport à la Commission de la protection de la vie privée » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/003, p. 24).

B.63.3. En exécution de l'article 14, § 4, de la loi du 25 décembre 2016, l'arrêté royal du 21 décembre 2017 « relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données » détermine les modalités de composition et d'organisation de l'UIP.

Le rapport au Roi précédant cet arrêté royal précise :

« La banque de données ne peut donc être consultée qu'au sein de l'UIP, et uniquement par les membres de l'UIP, dans le cadre de leurs missions, ainsi que par le délégué à la protection des données » (*Moniteur belge* du 29 décembre 2017, deuxième édition, p. 116833).

La procédure de détachement est organisée par les articles 12 à 21 de l'arrêté royal, précité, du 21 décembre 2017.

B.63.4. Le fait que les membres détachés de services compétents participent au fonctionnement de l'UIP vise à garantir que cette UIP soit composée de personnes qui jouissent d'une certaine expertise, afin de renforcer ainsi l'efficacité de l'UIP.

Cette possibilité de détachement est d'ailleurs expressément prévue par l'article 4, paragraphe 3, de la directive « PNR » qui dispose :

« Les membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes […] ».

COPIE NON CORRIGÉE

Rien ne permet de considérer que ces personnes, même si elles gardent leur statut dans leur service d'origine, n'exercent pas leurs fonctions avec indépendance au sein de l'UIP. L'article 14, § 1er, alinéa 2, de la loi du 25 décembre 2016 précise d'ailleurs que, durant la période de leur détachement, « les membres des services compétents sont placés sous l'autorité fonctionnelle et hiérarchique du fonctionnaire dirigeant de l'UIP ».

Les membres de l'UIP sont en outre passibles de sanctions pénales s'ils ne respectent pas le secret professionnel ou s'ils retiennent sciemment et volontairement des informations, données et renseignements faisant obstacle aux finalités prévues à l'article 8 (articles 48 et 49).

B.63.5. En ce qui concerne l'accès aux données « PNR » dans le cadre de recherches ponctuelles après un délai de six mois, la Cour de justice a considéré, dans son avis précité 1/15 du 26 juillet 2017, que l'utilisation des données « PNR » ainsi stockées devrait « être fondée sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles les autorités canadiennes visées par l'accord envisagé peuvent avoir accès à ces données aux fins de leur utilisation » et que « cette utilisation devrait, sauf cas d'urgence dûment justifiés, être subordonnée à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision autorisant l'utilisation intervient à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales » (point 208).

L'article 12, paragraphe 3, de la directive « PNR » dispose à cet égard :

« À l'expiration de la période de six mois visée au paragraphe 2, la communication de l'intégralité des données PNR n'est autorisée que :

a) lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b); et

b) lorsqu'elle a été approuvée par :

i) une autorité judiciaire; ou

ii) une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post ».

B.63.6. Afin de vérifier si l'UIP peut être considérée comme cette « autre autorité nationale compétente » au sens de l'article 12, paragraphe 3, de la directive « PNR », il convient, avant dire droit, de poser à la Cour de justice la septième question préjudicielle figurant dans le dispositif.

7. *La durée de conservation des données « PNR » (article 18)*

B.64. La partie requérante critique l'article 18 de la loi du 25 décembre 2016, en ce que le délai de cinq ans durant lequel les données « PNR » sont conservées serait disproportionné.

B.65.1. L'article 12 de la directive « PNR », intitulé « Période de conservation et dépersonnalisation des données », dispose :

« 1. Les États membres veillent à ce que les données PNR fournies par les transporteurs aériens à l'UIP y soient conservées dans une base de données pendant une période de cinq ans suivant leur transfert à l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol.

2. À l'expiration d'une période de six mois suivant le transfert des données PNR visé au paragraphe 1, toutes les données PNR sont dépersonnalisées par le masquage des éléments des données suivants qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR :

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

b) l'adresse et les coordonnées;

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

d) les informations ' grands voyageurs ';

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

f) toute donnée API qui a été recueillie.

3. À l'expiration de la période de six mois visée au paragraphe 2, la communication de l'intégralité des données PNR n'est autorisée que :

a) lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b); et

b) lorsqu'elle a été approuvée par :

i) une autorité judiciaire; ou

ii) une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post.

4. Les États membres veillent à ce que les données PNR soient effacées de manière définitive à l'issue de la période visée au paragraphe 1. Cette obligation s'applique sans préjudice des cas où des données PNR spécifiques ont été transférées à une autorité compétente et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière, auquel cas la conservation de ces données par l'autorité compétente est régie par le droit national.

5. Le résultat du traitement visé à l'article 6, paragraphe 2, point a), n'est conservé par l'UIP que le temps nécessaire pour informer les autorités compétentes et, conformément à l'article 9, paragraphe 1, pour informer les UIP des autres États membres de l'existence d'une concordance positive. Lorsque, à la suite du réexamen individuel par des moyens non automatisés visé à l'article 6, paragraphe 5, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées au titre du paragraphe 4 du présent article, de manière à éviter de futures ' fausses ' concordances positives ».

Le considérant 25 de la directive « PNR » dispose :

« Les données PNR ne devraient être conservées que pour la durée nécessaire et proportionnée aux objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière. En raison de leur nature et de leurs utilisations, il est indispensable que les données PNR soient conservées pendant une période suffisamment longue pour permettre leur analyse et leur utilisation dans le cadre d'enquêtes. Pour éviter toute utilisation disproportionnée, il convient que, après le délai initial de conservation, les données PNR soient dépersonnalisées par le masquage d'éléments des données. Afin de garantir le niveau le plus élevé de protection de données, l'accès à l'intégralité des données PNR, qui permettent l'identification directe de la personne concernée, ne devrait être accordé que dans des conditions très strictes et limitées après ce délai initial ».

B.65.2.1. Selon la jurisprudence de la Cour de justice, la durée de conservation des données doit « toujours répondre à des critères objectifs, établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi » (CJUE, 6 octobre 2015, C-362/14, *Schrems*, point 93; grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige et Watson e.a.*, point 110; grande chambre, 26 juillet 2017, avis n° 1/15, point 191).

B.65.2.2. En ce qui concerne plus précisément les données « PNR », la Cour de justice a considéré, dans son avis n° 1/15, précité du 26 juillet 2017, que la durée de cinq ans « n'apparaît pas excéder les limites de ce qui est strictement nécessaire à des fins de lutte contre le terrorisme et la criminalité transnationale grave » (grande chambre, 26 juillet 2017, avis n° 1/15, point 209), sous la réserve que « s'agissant des passagers aériens pour lesquels un tel risque n'a pas été identifié à leur arrivée au Canada et jusqu'à leur départ de ce pays tiers, il n'apparaît pas exister, une fois qu'ils sont repartis, de rapport, ne serait-ce qu'indirect, entre leurs données PNR et l'objectif poursuivi par l'accord envisagé, qui justifierait […] un stockage continu des données PNR de l'ensemble des passagers aériens après leur départ du Canada aux fins d'un accès éventuel auxdites données, indépendamment d'un lien quelconque avec la lutte contre le terrorisme et la criminalité transnationale grave (voir, par analogie, arrêt du 21 décembre 2016, *Tele2 Sverige et Watson e.a.*, C-203/15 et C-698/15, EU:C:2016:970, point 119) » (*ibid.*, point 205).

B.66.1. L'article 18 de la loi du 25 décembre 2016 prévoit que les données des passagers sont conservées dans la banque de données des passagers pour une durée maximale de cinq ans à compter de leur enregistrement, et qu'à l'issue de ce délai, elles sont détruites.

Conformément à l'article 21, § 1er, de la loi du 25 décembre 2016, l'UIP veille à ce que les données des passagers soient effacées de sa banque de données de manière définitive à l'issue de la période visée à l'article 18.

B.66.2. Les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« L'article 18 précise le délai de conservation des données dans la banque de données passagers.

Conformément à l'article 4, 4° de la loi du 8 décembre 1992 relative à la protection de la vie privée eu égard au traitement des données à caractère personnel, les données à caractère personnel sont conservées sous une forme qui permet d'identifier les personnes concernées pendant un délai qui n'excède pas celui qui est nécessaire pour concrétiser les objectifs pour lesquels ils ont été collectés ou pour lesquels ils seront ultérieurement traités.

C'est pourquoi les données du fichier des données de voyage telles que visées à l'article 9 sont conservées pendant un délai maximal de 5 ans pour la prévention, la recherche, l'examen et la poursuite des infractions terroristes et de la criminalité grave ainsi que pour la protection des intérêts fondamentaux de l'État et ensuite définitivement supprimées de la Banque de données passagers. A l'issue de ce délai, elles sont détruites.

Ce délai de 5 ans maximum doit permettre d'exécuter les analyses et vérifications nécessaires en vue de la découverte de nouveaux phénomènes ou de la recherche de nouvelles tendances liées aux finalités, d'adapter ou de déterminer de nouveaux profils de risque et, le cas échéant, de recueillir des preuves, de trouver d'éventuels co-auteurs ou complices et de démanteler des réseaux criminels » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, pp. 25-26).

B.66.3.1. Le délai de cinq ans prévu par l'article 18 de la loi du 25 décembre 2016 doit toutefois être lu en combinaison avec les articles 19 et suivants de la même loi, qui organisent également les modalités de conservation des données.

B.66.3.2. L'article 19 de la loi du 25 décembre 2016 dispose :

« À l'expiration d'une période de six mois, à compter de l'enregistrement des données des passagers dans la banque de données des passagers, toutes les données des passagers sont dépersonnalisées, par masquage des éléments d'information suivants, pouvant servir à identifier directement le passager auquel se rapportent les données :

1° le(s) nom(s), notamment les noms d'autres passagers, ainsi que le nombre de passagers voyageant ensemble;

2° l'adresse et les coordonnées;

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

4° les informations concernant les grands voyageurs;

COPIE NON CORRIGÉE

5° les remarques générales, dans la mesure où elles comportent des informations pouvant servir à identifier directement le passager; et

6° toutes les données visées à l'article 9, § 1er, 18° ».

Cette disposition doit être lue en combinaison avec l'article 4, 14°, de la loi du 25 décembre 2016, qui définit la « dépersonnalisation par masquage d'éléments de données » comme « le fait de rendre invisible pour un utilisateur des éléments de données qui pourraient servir à identifier directement la personne concernée, visé à l'article 19 ».

B.66.3.3. L'article 20 de la loi du 25 décembre 2016 prévoit qu'à l'expiration de la période de six mois visée à l'article 19, la communication de l'intégralité des données des passagers n'est autorisée que pour le traitement des données prescrit par l'article 27 et uniquement selon les conditions prévues par cette disposition.

Par ailleurs, le résultat du traitement visé à l'article 24 n'est conservé par l'UIP que le temps nécessaire pour informer les autorités compétentes et, conformément à l'article 36, pour informer les UIP des autres États membres de l'Union européenne de l'existence d'une correspondance positive (article 21, § 3, alinéa 1er).

B.66.3.4. L'article 22 de la loi du 25 décembre 2016 garantit que le fonctionnaire dirigeant et le délégué à la protection des données n'ont accès à toutes les données pertinentes que dans le cadre de l'accomplissement de leurs missions.

Enfin, le traitement des données fait l'objet d'une journalisation et est en corrélation directe avec les finalités prévues à l'article 8 (article 23, § 1er). L'UIP veille à la journalisation en conservant pendant cinq ans une trace documentaire de tous les systèmes et procédures de traitement sous sa responsabilité (article 23, § 2, alinéa 1er).

B.66.4. La durée de conservation des données des passagers doit être déterminée compte tenu des finalités du traitement de ces données, en lien direct avec les objectifs de prévention, la recherche, et la poursuite des infractions terroristes et de la criminalité grave.

COPIE NON CORRIGÉE

B.67.1. La Commission de la protection de la vie privée avait toutefois constaté que, lorsque le délai de conservation des données est long et que les données sont stockées massivement, « le risque de profilage des personnes concernées augmente, tout comme le risque de détournement de finalité (‘ *function creep* ’), c’est-à-dire le détournement potentiel de l’utilisation de données pour d’autres infractions pour lesquelles il n’y avait pas initialement d’accord (politique) d’échange de données » (Commission de la Protection de la Vie privée, avis d’initiative n° 01/2010 du 13 janvier 2010 « relatif au projet de loi portant assentiment à l’Accord entre l’Union européenne et les États-Unis d’Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au Ministère américain de la sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007 », point 3.3, pp. 17-18).

Dans son avis n° 55/2015 du 16 décembre 2015 sur l’avant-projet de loi devenu la loi du 25 décembre 2016, la Commission de la protection de la vie privée estimait également que la nécessité du délai de conservation des données pendant cinq ans devait être justifiée de manière plus précise et étayée (point 32).

Dans son avis du 19 août 2016 « sur les implications en matière de protection des données du traitement des données passagers », le Comité consultatif de la Convention n° 108 du Conseil de l’Europe « pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel » avait également fait observer que « des données masquées permettent encore d’identifier les personnes et restent à ce titre des données à caractère personnel, et que leur conservation devrait aussi être limitée dans le temps pour prévenir une surveillance permanente généralisée » (avis du 19 août 2016, T-PD(2016)18rev, p. 9).

B.67.2. Afin de vérifier si ce délai de conservation de cinq ans, autorisé par la directive « PNR », est, compte tenu de ce qui précède et des différentes garanties énumérées en B.66, compatible avec les observations de la Cour de justice mentionnées en B.65.2.2, dès lors qu’il n’opère aucune distinction selon que les passagers concernés se révèlent, dans le cadre de l’évaluation préalable, susceptibles ou non de présenter un risque pour la sécurité publique, il convient, avant de statuer quant au fond, de poser à la Cour de justice de l’Union européenne la huitième question préjudicielle figurant dans le dispositif.

COPIE NON CORRIGÉE

Quant au second moyen

B.68. Le second moyen, formulé à titre subsidiaire, est pris de la violation de l'article 22 de la Constitution, combiné avec l'article 3, paragraphe 2, du Traité sur l'Union européenne et avec l'article 45 de la Charte des droits fondamentaux de l'Union européenne. Ce moyen est dirigé contre l'article 3, § 1er, l'article 8, § 2, et le chapitre 11, contenant les articles 28 à 31, de la loi du 25 décembre 2016.

La partie requérante estime qu'en étendant le système « PNR » aux vols intra-UE, les dispositions attaquées rétablissent indirectement des contrôles aux frontières qui seraient contraires à la liberté de circulation des personnes.

B.69.1. L'article 3, § 1er, de la loi du 25 décembre 2016 dispose :

« La présente loi détermine les obligations des transporteurs et des opérateurs de voyage relatives à la transmission des données des passagers à destination du, en provenance du et transitant par le territoire national ».

Le contenu des articles 8, § 2, et 28 à 31, de la loi du 25 décembre 2016 est rappelé en B.55.

B.69.2. En ce qui concerne le champ d'application de la loi du 25 décembre 2016, les travaux préparatoires exposent :

« L'inclusion intra-UE dans la collecte des données permettra d'obtenir un tableau plus complet des déplacements des passagers qui constituent une menace potentielle pour la sécurité intracommunautaire et nationale. La pratique a déjà démontré que certains ' *returnees* ' (aussi appelés ' *foreign fighters* ' qui rentrent en Europe) embarquent à bord de différents vols avant de rallier leur destination finale.

La Directive UE PNR prévoit expressément la possibilité pour les États membres de traiter les données des passagers de l'UE pour le trafic international au sein de l'Union européenne. En outre, tous les États membres ont approuvé, le 21 avril 2016 au Conseil des ministres de l'Intérieur et de la Justice, une déclaration visant à transposer la directive UE PNR dans les droits nationaux aussi pour le trafic intra-Union européenne » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 7).

COPIE NON CORRIGÉE

B.69.3. Comme il est dit en B.55, les passagers visés par le chapitre 11 de la loi du 25 décembre 2016, de même que les données visées et le délai de conservation sont limités.

Les travaux préparatoires exposent :

« Par conséquent, seuls sont concernés les passagers qui souhaitent franchir ou ont franchi les frontières extérieures de la Belgique pour y entrer ou en sortir et ce, indépendamment du type de transport utilisé (maritime, ferroviaire, terrestre, aérien). Seules les données de ces passagers seront donc traitées par les services de police chargés du contrôle aux frontières et l'Office des étrangers.

Les passagers qui envisagent de transiter par la zone internationale de transit par exemple d'un aéroport situé en Belgique sont également visés dans la mesure où les règles sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers s'appliquent également à eux. Ainsi, ces personnes doivent disposer des documents de voyage requis. Certaines personnes sont soumises à l'obligation de visa de transit aéroportuaire; des contrôles dans ces zones sont autorisés et peuvent, dans certains cas, conduire à une mesure de refoulement.

Comme déjà mentionné, seules les données de passagers dites ' API ' seront transmises aux services de police et à l'Office des étrangers en vertu du présent chapitre. Ces données sont énumérées à l'article 9, § 2, de l'avant-projet de loi.

Elles correspondent en substance à celles que les transporteurs aériens doivent déjà transmettre en vertu de l'arrêté royal du 11 décembre 2006.

[…]

L'utilisation des données est également limitée à vingt-quatre heures. Au-delà, si l'accès aux données des passagers est nécessaire dans le cadre de l'exercice de ses missions légales, l'Office des étrangers adresse une requête motivée à l'UIP » (*ibid.*, pp. 34-35).

B.70.1. Comme il est dit plus haut, le considérant 10 de la directive « PNR » autorise l'extension du système « PNR » aux vols intra-UE. L'article 2 de la directive « PNR » organise la procédure visant à étendre le champ d'application.

COPIE NON CORRIGÉE

Comme il est dit en B.55.4, la finalité de lutter contre l'immigration illégale et d'améliorer le contrôle aux frontières ne concerne que les catégories de passagers énumérées à l'article 29, § 2, de la loi du 25 décembre 2016, et se limite aux données « API » visées à l'article 9, § 1er, 18°, de la loi du 25 décembre 2016. Les traitements effectués dans le cadre de cette finalité sont également limités. Les dispositions attaquées s'inscrivent dans le cadre de la transposition de la directive « API », qui poursuit également comme objectifs la lutte contre l'immigration illégale et l'amélioration du contrôle aux frontières.

B.70.2. Dans son avis n° 55/2015 du 16 décembre 2015 sur l'avant-projet de loi devenu la loi du 25 décembre 2016, la Commission de la protection de la vie privée s'interroge toutefois sur la compatibilité avec le principe de la libre circulation des personnes du système « PNR » mis en place, qui vise « tant des transports à destination et à partir de l'espace Schengen (extra-Schengen) que les transports entrant et sortant de l'espace Schengen (intra-Schengen) », ce qui pourrait aboutir « indirectement à un rétablissement des contrôles aux frontières intérieures » (points 21-25).

B.70.3. Afin, dès lors, de vérifier si ces mesures sont compatibles avec la libre circulation des personnes, il convient, avant de statuer quant au fond, de poser à la Cour de justice de l'Union européenne la neuvième question préjudicielle figurant dans le dispositif.

COPIE NON CORRIGÉE

Par ces motifs,

la Cour

avant de statuer au fond, pose à la Cour de justice de l'Union européenne les questions préjudicielles suivantes :

1. L'article 23 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 de ces données, et abrogeant la directive 95/46/CE » (Règlement général sur la protection des données – RGPD), lu en combinaison avec l'article 2, paragraphe 2, d), de ce règlement, doit-il être interprété comme s'appliquant à une législation nationale telle que la loi du 25 décembre 2016 « relative au traitement des données des passagers », qui transpose la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 « relative à l'utilisation des données des dossiers passagers (« PNR ») pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière », ainsi que la directive 2004/82/CE du Conseil du 29 avril 2004 « concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers » et la directive 2010/65/UE du Parlement européen et du Conseil du 20 octobre 2010 « concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres et abrogeant la directive 2002/6/CE » ?

2. L'annexe I de la directive (UE) 2016/681 est-elle compatible avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, en ce sens que les données qu'elle énumère sont très larges - notamment les données visées au point 18 de l'annexe I de la directive (UE) 2016/681, qui dépassent les données visées par l'article 3, paragraphe 2, de la directive 2004/82/CE - et en ce que, prises ensemble, elles pourraient révéler des données sensibles, et violer ainsi les limites du « strict nécessaire » ?

COPIE NON CORRIGÉE

3. Les points 12 et 18 de l'annexe I de la directive (UE) 2016/681 sont-ils compatibles avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, en ce que, compte tenu des termes « notamment » et « y compris », les données qu'ils visent sont mentionnées à titre exemplatif et non exhaustif, de sorte que l'exigence de précision et de clarté des règles emportant une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel ne serait pas respectée ?

4. L'article 3, point 4), de la directive (UE) 2016/681 et l'annexe I de la même directive sont-ils compatibles avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, en ce que le système de collecte, de transfert et de traitement généralisés des données des passagers que ces dispositions instaurent vise toute personne qui utilise le moyen de transport concerné, indépendamment de tout élément objectif permettant de considérer que cette personne est susceptible de présenter un risque pour la sécurité publique ?

5. L'article 6 de la directive (UE) 2016/681, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété comme s'opposant à une législation nationale telle que la loi attaquée, qui admet, comme finalité du traitement des données « PNR », le suivi des activités visées par les services de renseignement et de sécurité, intégrant ainsi cette finalité dans la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que dans les enquêtes et les poursuites en la matière ?

6. L'article 6 de la directive (UE) 2016/681 est-il compatible avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, en ce que l'évaluation préalable qu'il organise, par une corrélation avec des banques de données et des critères préétablis, s'applique de manière systématique et généralisée aux données des passagers, indépendamment de tout élément objectif permettant de considérer que ces passagers sont susceptibles de présenter un risque pour la sécurité publique ?

COPIE NON CORRIGÉE

7. La notion d' « autre autorité nationale compétente » visée à l'article 12, paragraphe 3, de la directive (UE) 2016/681 peut-elle être interprétée comme visant l'UIP créée par la loi du 25 décembre 2016, qui pourrait dès lors autoriser l'accès aux données « PNR », après un délai de six mois, dans le cadre de recherches ponctuelles ?

8. L'article 12 de la directive (UE) 2016/681, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété comme s'opposant à une législation nationale telle que la loi attaquée qui prévoit un délai général de conservation des données de cinq ans, sans distinguer si les passagers concernés se révèlent, dans le cadre de l'évaluation préalable, susceptibles ou non de présenter un risque pour la sécurité publique ?

9. a) La directive 2004/82/CE est-elle compatible avec l'article 3, paragraphe 2, du Traité sur l'Union européenne et avec l'article 45 de la Charte des droits fondamentaux de l'Union européenne, en ce que les obligations qu'elle instaure s'appliquent aux vols à l'intérieur de l'Union européenne ?

b) La directive 2004/82/CE, lue en combinaison avec l'article 3, paragraphe 2, du Traité sur l'Union européenne et avec l'article 45 de la Charte des droits fondamentaux de l'Union européenne, doit-elle être interprétée comme s'opposant à une législation nationale telle que la loi attaquée qui, aux fins de lutter contre l'immigration illégale et d'améliorer les contrôles aux frontières, autorise un système de collecte et de traitement des données des passagers « à destination du, en provenance du et transitant par le territoire national », ce qui pourrait impliquer indirectement un rétablissement des contrôles aux frontières intérieures ?

10. Si, sur la base des réponses données aux questions préjudicielles qui précèdent, la Cour constitutionnelle devait arriver à la conclusion que la loi attaquée, qui transpose notamment la directive (UE) 2016/681, méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du 25 décembre 2016 « relative au traitement des données des passagers » afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées aux fins visées par la loi ?

COPIE NON CORRIGÉE

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 17 octobre 2019.

Le greffier, Le président,

F. Meersschaut F. Daoût

COPIE NON CORRIGÉE