Cour constitutionnelle

Arrêt n° 131/2023
du 12 octobre 2023
Numéro du rôle : 6713

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 » (actuellement « Ligue des droits humains »).

La Cour constitutionnelle,

composée du président P. Nihoul, de la juge J. Moerman, faisant fonction de présidente, et des juges T. Giet, M. Pâques, Y. Kherbache, D. Pieters, S. de Bethune, E. Bribosia, W. Verrijdt et K. Jadin, assistée du greffier F. Meersschaut, présidée par le président P. Nihoul,

après en avoir délibéré, rend l'arrêt suivant :

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 (articles 3, § 1er, et 8, § 2, et chapitre 11) de la loi du 25 décembre 2016 « relative au traitement des données des passagers » (publiée au *Moniteur belge* du 25 janvier 2017).

Par arrêt interlocutoire n° 135/2019 du 17 octobre 2019 (ECLI:BE:GHCC:2019:ARR.135), publié au *Moniteur belge* du 6 mars 2020, la Cour a posé 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 ' ?

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 ?

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 ? ».

Par arrêt du 21 juin 2022, dans l'affaire C-817/19 (ECLI:EU:C:2022:491), la Cour de justice de l'Union européenne a répondu aux questions.

Par ordonnance du 13 juillet 2022, la Cour, après avoir entendu les juges-rapporteurs T. Giet et W. Verrijdt, a décidé :

- de rouvrir les débats,

- d'inviter les parties à exposer, dans un mémoire complémentaire à introduire le 30 septembre 2022 au plus tard et à communiquer aux autres parties dans le même délai, leur point de vue sur l'incidence de l'arrêt de la Cour de Justice de l'Union européenne précité sur le recours en annulation, plus précisément :

a) quant aux répercussions, sur la poursuite de l'examen du recours en annulation devant la Cour, des considérations relatives notamment :

- à l'articulation de la directive PNR et du RGPD;

- au champ d'application de la collecte et du traitement des données PNR (données identifiées, finalités et infractions visées, vols concernés);

- aux garanties entourant le traitement des données PNR (évaluation préalable, traitement automatisé, accès aux données PNR, notion d'« autorité nationale indépendante », délai de conservation des données PNR);

- l'absence d'une possibilité de maintien des effets en cas d'annulation partielle de la loi du 25 décembre 2016 « relative au traitement des données des passagers »;

b) quant aux justifications et conditions, concrètement étayées, du caractère limité au « strict nécessaire » et de la conformité avec l'interprétation de la directive PNR de chacun des éléments évoqués ci-dessus, tels qu'ils sont prévus en l'espèce dans la loi du 25 décembre 2016 « relative au traitement des données des passagers »;

- 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 5 octobre 2022 et l'affaire mise en délibéré.

Des mémoires complémentaires ont été introduits par :

- la partie requérante;

- le Conseil des ministres, assisté et représenté par Me E. Jacubowitz et Me C. Caillet, avocats au barreau de Bruxelles.

À la suite de la demande du Conseil des ministres à être entendu, la Cour, par ordonnance du 21 septembre 2022, a fixé l'audience au 26 octobre 2022.

Par ordonnance du 26 octobre 2022, la Cour, à la demande des conseils du Conseil des ministres, a reporté l'affaire à l'audience du 23 novembre 2022.

À l'audience publique du 23 novembre 2022 :

- ont comparu :

. Me C. Forget, pour la partie requérante;

. Me E. Jacubowitz, Me C. Caillet et Gunter Ceuppens, pour le Conseil des ministres;

- les juges-rapporteurs T. Giet et W. Verrijdt ont fait rapport;

- les parties précitées ont été entendues;

- l'affaire a été mise en délibéré.

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 –

Quant aux mémoires complémentaires introduits à la suite de l'arrêt de la Cour de justice de l'Union européenne du 21 juin 2022

A.1.1. La partie requérante estime que, à la lumière de l'arrêt rendu par la Cour de justice dans l'affaire C-817/19, la loi du 25 décembre 2016 « relative au traitement des données des passagers » (ci-après : la loi attaquée) viole le principe de proportionnalité inscrit à l'article 52, paragraphe 1, de la Charte des droits fondamentaux, lu en combinaison avec les articles 7 et 8 de celle-ci.

A.1.2. *Primo*, il ressort des considérants 128 à 140 de l'arrêt précité que les données PNR (*Passenger Name Record*), ainsi que les données API (*Advance Passenger Information*), visées respectivement aux articles 4, 10°, et 9 de la loi attaquée, excèdent les limites du « strict nécessaire », en l'absence de précision et de clarté de certaines de ces données.

A.1.3. *Secundo*, la loi attaquée implique différents traitements de données à caractère personnel qui, en l'absence de précision, violent également le principe de proportionnalité, tel qu'il a été rappelé dans l'arrêt de la Cour de justice précité.

(1°) L'article 3, § 2, de la loi attaquée délègue au Roi le soin de déterminer, par secteur de transport et par opérateur, les modalités relatives aux obligations pour les transporteurs et opérateurs de voyage de transmettre les données des passagers. Une telle ingérence dans la vie privée aurait dû être prévue par une loi, d'autant que les notions de « document d'identité » et de « document de voyage » ne sont pas définies à l'article 7, §§ 1er et 2, de la loi attaquée.

(2°) La création d'une banque de données de passagers, organisée par les articles 12 à 15 de la loi attaquée, excède également les limites du strict nécessaire.

(3°) La corrélation entre les bases de données, visée à l'article 24 de la loi attaquée, n'est pas limitée aux bases de données qui sont exploitées en rapport avec la lutte contre le terrorisme et la criminalité grave, contrairement à ce que la Cour de justice énonce dans les considérants 182 à 191 de l'arrêt précité. En ce qui concerne le croisement de la banque de données des passagers à l'aide de critères préétablis servant d'« indicateurs de la menace », il est renvoyé aux considérants 202 à 213 de l'arrêt de la Cour de justice précité : compte tenu de son caractère vague, la loi attaquée ne répond pas à l'exigence selon laquelle les ingérences qu'elle emporte doivent être « prévues par la loi » au sens des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

(4°) Enfin, en ce qui concerne les recherches ponctuelles, la loi attaquée ne précise pas quelles données seront accessibles aux services compétents, et les agents de ces services détachés au sein de l'« Unité information passager » (UIP) sont en quelque sorte juges et parties.

A.1.4. *Tertio*, il est renvoyé aux considérants 142 à 152 de l'arrêt de la Cour de justice précité, dont il ressort que les finalités du traitement des données PNR, visées à l'article 8 de la loi attaquée, sont nettement plus larges que les finalités prévues à l'article 1er, § 2, de la directive PNR. Ainsi, l'article 8, § 2, de la loi attaquée dispose que les données des passagers sont également traitées en vue de lutter contre l'immigration illégale, ce qui est une finalité beaucoup plus large que le strict nécessaire au sens des dispositions visées au moyen. De même, les considérants 232 à 236 de l'arrêt de la Cour de justice précité font apparaître que la finalité relative aux activités liées à la sûreté de l'État n'est pas limitée au strict nécessaire.

A.1.5. *Quarto*, concernant la durée de conservation des données, il est renvoyé aux considérants 250 à 257 de l'arrêt de la Cour de justice précité, dont il ressort que l'article 18 de la loi attaquée ne respecte pas les conditions de nécessité et de proportionnalité en ce qui concerne l'ingérence qu'il prévoit dans le droit au respect de la vie privée et à la protection des données à caractère personnel.

A.2.1. Le Conseil des ministres rappelle tout d'abord que le juge national n'est tenu par le dispositif de l'arrêt préjudiciel rendu par la Cour de justice qu'en ce qui concerne le droit de l'Union. Il appartient en revanche au seul juge national d'appliquer le droit de l'Union, et, dès lors, de décider que ce droit s'applique au litige dont il est saisi.

En l'espèce, la Cour de justice a validé l'ensemble de la directive PNR, en l'interprétant de manière conforme aux droits fondamentaux, et le législateur belge a transposé celle-ci de manière très fidèle, en y intégrant dès lors les garanties du respect des droits fondamentaux.

A.2.2. En ce qui concerne le premier moyen, le Conseil des ministres constate que la Cour de justice estime que le Règlement général sur la protection des données (ci-après : le RGPD) est applicable aux traitements de données à caractère personnel prévus par une législation nationale visant à transposer, en droit interne, les dispositions de la directive API, de la directive 2010/65/UE et de la directive PNR lues conjointement, ou uniquement de la directive API ou de la directive 2010/65/UE. En revanche, la Cour de justice estime que le RGPD n'est pas applicable aux traitements de données prévus par une telle législation ne relevant que de la directive PNR qui sont effectués par l'UIP ou par les autorités compétentes. Le premier moyen n'est donc pas fondé en ce qu'il vise l'article 23 du RGPD.

Pour le surplus, le Conseil des ministres ne conteste pas ce point du dispositif, qui n'a pas d'incidence sur la loi attaquée, dans la mesure où l'article 15, § 4, de cette dernière soumet les traitements de données prévus par la loi attaquée à la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, laquelle exécute le RGPD.

A.2.3. En ce qui concerne les données PNR, la Cour de justice conclut que l'annexe I de la directive PNR présente, dans son ensemble, un caractère suffisamment clair et précis, de sorte qu'il en va de même de l'article 9, § 1er, de la loi attaquée, qui présente une formulation très similaire à cette annexe. Le Conseil des ministres en déduit que le premier moyen n'est pas fondé en ce qu'il est dirigé contre cette disposition.

A.2.4. En ce qui concerne les finalités des traitements de données PNR, la Cour de justice a jugé que les finalités prévues par la directive PNR étaient claires et précises, et que l'énumération des objectifs revêt un caractère exhaustif. En ce qui concerne les finalités des services de renseignement et de sécurité, la Cour de justice laisse à la juridiction qui pose les questions le soin de déterminer si ces finalités sont incluses dans les objectifs exhaustifs de la directive PNR. Le Conseil des ministres estime que tel est le cas, en se référant aux considérants 5 et 6 de la directive PNR et au fait que la Cour de justice reconnaît qu'en cas de menace terroriste réelle et actuelle ou prévisible, l'utilisation maximale des données PNR n'excède pas les limites du strict nécessaire. Or, la mission des services de renseignement et de sécurité consiste en la prévention et la détection d'activités qui menacent ou pourraient menacer le fonctionnement démocratique et les intérêts fondamentaux de la société, en particulier la sécurité intérieure. Ces menaces présentent des recoupements avec plusieurs infractions graves, qui sont de plus en plus hybrides, listées dans l'annexe II de la directive PNR (espionnage, extrémisme, crime organisé, ingérence), et la Cour, par son arrêt n° 64/2021 du 22 avril 2021 (ECLI:BE:GHCC:2021:ARR.064), a mis en lumière les spécificités des finalités des services de renseignement axés sur la détection et la prévention des menaces les plus graves pour la sécurité de l'État, et sur leur complémentarité avec les autorités policières et judiciaires, qui sont averties par les services de renseignement et de sécurité dès que ces derniers détectent l'existence d'infractions terroristes ou d'autres formes de criminalité grave. Enfin, il convient de rappeler que la Belgique est particulièrement exposée aux menaces précitées, à la fois comme pays hôte de nombreuses institutions européennes et internationales et comme « nœud » de transports pouvant être utilisé comme « plaque tournante » par les organisations terroristes et criminelles.

A.2.5. En ce qui concerne l'évaluation préalable des données par des traitements automatisés, elle a été validée par la Cour de justice, pour autant qu'elle soit réalisée de façon non discriminatoire, sur la base de critères ciblés, proportionnés et spécifiques. Constatant que la Cour, par son arrêt n° 135/2019 du 17 octobre 2019, précité,

a jugé que l'évaluation préalable était entourée de critères apparaissant comme suffisants, le Conseil des ministres estime que le moyen n'est pas fondé en ce qu'il est dirigé contre l'article 25 de la loi attaquée.

A.2.6. En ce qui concerne le délai de conservation des données PNR, la Cour de justice estime que la conservation au-delà d'une période initiale de six mois des données de passagers dont ni l'évaluation préalable ni les vérifications ni aucune autre circonstance n'ont permis d'établir un risque en matière d'infractions terroristes ou de formes graves de criminalité excède le strict nécessaire. Une durée générale de conservation de cinq ans, applicable indifféremment à tous les passagers, est dès lors susceptible de violer l'article 12, paragraphe 1, de la directive PNR, lu à la lumière des articles 7 et 8, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux. Cependant, dès lors que l'article 18 de la loi attaquée prévoit que le délai de cinq ans est un délai maximal au terme duquel les données doivent être détruites, le Conseil des ministres invite la Cour à interpréter cette disposition de manière conforme aux dispositions précitées de la Charte, et de considérer que toutes les données des passagers ne seront pas nécessairement conservées pendant un délai de cinq ans.

A.2.7. Concernant le second moyen, le Conseil des ministres constate que la Cour de justice considère que la directive API doit être interprétée comme ne s'appliquant pas aux vols intra-UE et que le droit de l'Union s'oppose à une règlementation nationale prévoyant un système de transfert et de traitement des données API aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine. Le Conseil des ministres estime qu'une interprétation du chapitre 11 de la loi attaquée est possible dans la mesure où l'article 29 de la loi attaquée ne s'applique qu'aux vols extra-UE et ne concerne que les données API. Il en découle que ce chapitre ne peut être conçu comme la réinstauration d'un contrôle aux frontières intérieures à l'espace Schengen, de sorte que le moyen n'est pas fondé.

– *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*).

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).

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 » (ci-après : directive 2010/65/UE). 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 1er, 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).

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'identit[é]) 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).

B.4.1. 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.4.2. 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'Unité d'information des passagers (ci-après : 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).

Dans le cadre des finalités visées à l'article 8, § 1er, l'article 16 de la loi du 25 décembre 2016 prévoit que 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.

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 aux articles 18 et suivants de la loi du 25 décembre 2016.

Quant à l'étendue du recours

B.5.1. La Cour doit déterminer l'étendue du recours en annulation en se basant sur le contenu de la requête.

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.5.2. 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.5.3. 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.6. 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 :

[...]

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;

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;

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;

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.

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.

§ 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 :

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.

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.

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.

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.7. 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.

B.8. La loi du 25 décembre 2016 est entrée en vigueur le 7 août 2017, en ce qui concerne les compagnies aériennes, conformément à l'article 12 de 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).

Depuis le 22 février 2019, la loi du 25 décembre 2016 est également entrée en vigueur en ce qui concerne les transporteurs « HST » (*High speed train* – service international de transport de voyageurs par voie ferroviaire) et les distributeurs de tickets « HST », conformément à 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 », de même qu'en ce qui concerne les transporteurs par bus, conformément à 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 ».

Quant aux modifications apportées à la loi du 25 décembre 2016

B.9. La loi du 25 décembre 2016 a été modifiée par 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), par la loi du 15 juillet 2018 « portant des dispositions diverses Intérieur » (ci-après : la loi du 15 juillet 2018) et par la loi du 2 mai 2019 « modifiant diverses dispositions relatives au traitement des données des passagers » (ci-après : la loi du 2 mai 2019).

B.10.1. L'article 280, alinéa 4, de la loi du 30 juillet 2018 a abrogé, avec effet au 5 septembre 2018, l'article 15, § 3, de la loi du 25 décembre 2016.

Aucun recours en annulation n'ayant été introduit contre l'article 280, alinéa 4, de la loi du 30 juillet 2018, le recours en annulation présentement examiné, en ce qu'il porte sur l'article 15, § 3, de la loi du 25 décembre 2016, est définitivement devenu sans objet.

B.10.2. 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.

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).

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.11.1. 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 :

' 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 :

‘ 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° ' ».

Ces modifications sont entrées en vigueur le 5 octobre 2018.

B.11.2. Les articles 62, 63, 65, 66 et 67 de la loi du 15 juillet 2018 remplacent, respectivement, 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.

Aucun recours en annulation n'ayant été introduit contre les articles précités de la loi du 15 juillet 2018, le recours en annulation présentement examiné est en principe devenu sans objet en ce qu'il est dirigé contre les articles remplacés de la loi du 25 décembre 2016.

Le recours en annulation présentement examiné 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 un objet ou non.

B.11.3. 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° ».

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

B.12.1. Les articles 2 à 11 de 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 :

« 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[e] 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)* ’».

Ces modifications sont entrées en vigueur le 3 juin 2019.

B.12.2. Les articles 2, 4 et 7 de la loi du 2 mai 2019 ne constituant que des corrections techniques des articles 3, § 2, 14, § 2, 15, § 4, 29 et 30, § 1er, de la loi du 25 décembre 2016, ces modifications n’ont pas d’incidence sur l’objet du présent recours.

Par ailleurs, 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.

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 renvoi préjudiciel devant la Cour de justice

B.13.1. Par son arrêt interlocutoire n° 135/2019 du 17 octobre 2019, la Cour a interrogé la Cour de justice sur l’interprétation 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), ainsi que sur l’interprétation et la validité de la directive PNR et de la directive API. La Cour a également demandé à la Cour de justice si cette dernière pouvait, en cas d’annulation de la loi attaquée pour violation du droit européen, maintenir provisoirement les effets de cette loi.

B.13.2. La Cour a dès lors posé à la Cour de justice de l'Union européenne les dix 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 ' ?

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 ?

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 ? ».

B.14. Par son arrêt du 21 juin 2022 en cause de *Ligue des droits humains c. Conseil des ministres*, (C-817/19, ECLI:EU:C:2022:491), la Cour de justice de l'Union européenne, réunie en grande chambre, a répondu aux questions préjudicielles précitées.

Dans l’arrêt précité, la Cour de justice examine, successivement :

- la première question préjudicielle concernant l’articulation du RGPD avec la directive PNR (points 63 à 84);

- les deuxième à quatrième et sixième questions préjudicielles, qui portent sur la validité de la directive PNR et/ou de ses annexes en ce qui concerne le système de collecte de données et les données visées (points 85 à 228);

- la cinquième question préjudicielle, qui porte sur l’interprétation de la directive PNR en ce qui concerne les finalités de renseignement et de sécurité (points 229 à 237);

- la septième question préjudicielle, qui porte sur l’interprétation de la notion d’autorité nationale indépendante visée par la directive PNR (points 238 à 247);

- la huitième question préjudicielle, qui porte sur l’interprétation de la durée de conservation des données visée par la directive PNR (points 248 à 262);

- la neuvième question préjudicielle, point *a)*, qui porte sur la validité de la directive API, si cette directive s’applique aux vols intra-UE (points 263 à 269);

- la neuvième question préjudicielle, point *b)*, qui porte sur l’interprétation de la directive API en ce qu’elle permettrait de lutter contre l’immigration illégale et de réinstaurer une forme de contrôle aux frontières (points 270 à 291);

- la dixième question préjudicielle, qui porte sur un éventuel maintien des effets de la loi qui serait éventuellement incompatible avec le droit de l’Union (points 292 à 298).

Quant au premier moyen

B.15. Le premier moyen, formulé à titre principal, est pris de la violation de l'article 22 de la Constitution, lu en combinaison ou non avec l'article 23 du 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.

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.16.1. 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.16.2. 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.16.3. 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.

B.17.1. 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, entre autres, le respect de l'intégrité physique de la personne (CEDH, grande chambre, 8 avril 2021, *Vavřička e.a. c. République tchèque*, ECLI:CE:ECHR:2021:0408JUD004762113, § 261) et la protection des données à caractère personnel et des informations personnelles relatives à la santé (CEDH, 25 février 1997, *Z. c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; 10 octobre 2006, *L.L. c. France*, ECLI:CE:ECHR:2006:1010JUD000750802, § 32; 27 février 2018, *Mockuté c. Lituanie*, ECLI:CE:ECHR:2018:0227JUD006649009, § 93). 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, les informations concernant des biens et les données médicales (voy. notamment CEDH, 26 mars 1987, *Leander c. Suède*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66-68; 17 décembre 2009, *B.B. c. France*, ECLI:CE:ECHR:2009:1217JUD000533506, § 57; 10 février 2011, *Dimitrov-Kazakov c. Bulgarie*, ECLI:CE:ECHR:2011:0210JUD001137903, §§ 29-31; 18 octobre 2011, *Khelili c. Suisse*, ECLI:CE:ECHR:2011:1018JUD001618807, §§ 55-57; 9 octobre 2012, *Alkaya c. Turquie*, ECLI:CE:ECHR:2012:1009JUD004281106, § 29; 18 avril 2013, *M.K. c. France*, ECLI:CE:ECHR:2013:0418JUD001952209, § 26; 18 septembre 2014, *Brunet c. France*, ECLI:CE:ECHR:2014:0918JUD002101010, § 31; 13 octobre 2020, *Frâncu c. Roumanie*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

B.17.2. 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*, ECLI:CE:ECHR:1994:1027JUD001853591, § 31; grande chambre, 12 novembre 2013, *Söderman c. Suède*, ECLI:CE:ECHR:2013:1112JUD000578608, § 78).

Lorsqu'elles mettent en balance l'intérêt de l'État à traiter des données à caractère personnel et l'intérêt individuel à la protection de la confidentialité de ces données, les autorités nationales disposent d'une certaine marge d'appréciation (*ibid.*, § 99). Eu égard à l'importance fondamentale de la protection des données à caractère personnel, cette marge est toutefois assez limitée (CEDH, 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 73). Pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut qu'un juste équilibre soit atteint entre tous les droits et intérêts en cause. Pour juger de cet équilibre, il faut tenir compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après : la Convention n° 108) (CEDH, 25 février 1997, *Z c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, § 103; 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

La 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 a été actualisée par un protocole d'amendement ouvert à signature le 10 octobre 2018.

Il découle de la Convention n° 108 que le droit national doit notamment garantir que les données à caractère personnel sont pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou détenues, que les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle qui est nécessaire et que les données détenues sont protégées efficacement contre les usages impropres et abusifs. Elle a aussi indiqué qu'il est essentiel que le droit national prévoie des règles claires et détaillées relatives à la portée et à l'application des mesures concernées, ainsi que des garanties minimales concernant, entre autres, la durée, la conservation, l'utilisation, l'accès des tiers, les procédures de préservation de l'intégrité et de la confidentialité des données et les procédures de destruction de celles-ci, de sorte qu'il existe suffisamment de garanties contre le risque d'abus et d'arbitraire à chaque étape du traitement des données (CEDH, 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

B.18.1. 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.18.2. L'article 8 de la même Charte 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.18.3. Dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR et autres,* ECLI:EU:C:2010:662),

alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel (CJUE, grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, point 129; 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, point 114).

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 Kft.*, ECLI:EU:C:2015:832, point 70; 14 février 2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122, point 65).

B.18.4. La Cour de justice de l'Union européenne considère 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 physique identifiée ou identifiable (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR e.a*, ECLI:EU:C:2010:662, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, ECLI:EU:C:2019:26, point 54).

B.18.5. Les droits consacrés aux articles 7 et 8 de la Charte n'apparaissent pas non plus comme étant des prérogatives absolues (CJUE, grande chambre, 16 juillet 2020, C-311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, point 172).

Conformément à l'article 52, paragraphe 1, première phrase, de la Charte, toute limitation de l'exercice des droits et libertés reconnus par celle-ci, dont notamment le droit au respect de la vie privée garanti par l'article 7 et le droit à la protection des données à caractère personnel consacré par l'article 8, doit être prévue par la loi, respecter le contenu essentiel de ces droits et, dans le respect du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui (CJUE,

grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 64).

B.18.6. 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*, ECLI:EU:C:2017:592, 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.*).

B.19.1. L'article 22 de la Constitution réserve 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. Il garantit ainsi à tout citoyen 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.

B.19.2. Outre l'exigence de légalité formelle, l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, impose que l'ingérence dans l'exercice du droit au respect de la vie privée et du droit à la protection des données à caractère personnel 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.

En matière de protection des données, cette exigence de prévisibilité implique qu'il doit être prévu de manière suffisamment précise dans quelles circonstances les traitements de données à caractère personnel sont autorisés (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). L'exigence selon laquelle la limitation doit être prévue par la loi implique notamment que la base légale qui permet l'ingérence dans ces droits doit elle-même définir la portée de la limitation de l'exercice du droit concerné (CJUE, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 65).

Toute personne doit dès lors pouvoir avoir une idée suffisamment claire des données traitées, des personnes concernées par un traitement de données déterminé et des conditions et finalités dudit traitement.

B.20.1. 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;

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 ».

Conformément à cette disposition, les limitations apportées à certaines obligations des responsables du traitement – lesquelles sont prévues par la Charte – et aux droits des intéressés doivent être prévues par la loi, respecter l'essence des libertés et des droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique pour atteindre le but poursuivi et respecter les dispositions spécifiques contenues au paragraphe 2 (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, points 209-210; 10 décembre 2020, C-620/19, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, point 46).

B.20.2. 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.20.3. 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 ».

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.20.4. 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.21.1. 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.21.2. 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'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, et comme il est dit en B.2, un contenu qui va au-delà de la transposition de cette directive.

B.21.3. Interrogée par la Cour sur la question de savoir si l'article 23, lu en combinaison avec l'article 2, paragraphe 2, *d)*, du RGPD doit être interprété comme s'appliquant à une législation nationale telle que la loi du 25 décembre 2016, qui transpose à la fois la directive PNR, la directive API et la directive 2010/65/UE, la Cour de justice a répondu, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, que le libellé de l'article 2, paragraphe 2, *d)*, du RGPD « met clairement en évidence que deux conditions sont exigées pour qu'un traitement de données relève de l'exception qu'il prévoit » et que « [s]i la première de ces conditions est relative aux finalités du traitement, à savoir 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 des menaces pour la sécurité publique et la prévention de telles menaces, la seconde condition porte sur l'auteur

de ce traitement, à savoir une ‘ autorité compétente ’, au sens de ladite disposition » (point 67), l’exception visée à l’article 2, paragraphe 2, sous *d)*, du RGPD devant « recevoir, à l’instar des autres exceptions au champ d’application du RGPD prévues à l’article 2, paragraphe 2, de ce règlement, une interprétation stricte » (point 70) :

« 71. Ainsi qu’il ressort du considérant 19 dudit règlement, ladite exception est motivée par la circonstance que les traitements de données à caractère personnel effectués, par les autorités compétentes, aux fins, notamment, de prévention et de détection des infractions pénales, y compris de protection contre des menaces pour la sécurité publique et la prévention de telles menaces, sont régis par un acte plus spécifique de l’Union, à savoir la directive 2016/680, laquelle a été adoptée le même jour que le RGPD [arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, point 69].

72. Comme le précisent, par ailleurs, les considérants 9 à 11 de la directive 2016/680, celle-ci fixe des règles spécifiques relatives à la protection des personnes physiques à l’égard de ces traitements, en respectant la nature spécifique de ces activités relevant des domaines de la coopération judiciaire en matière pénale et de la coopération policière, tandis que le RGPD définit des règles générales concernant la protection de ces personnes qui ont vocation à s’appliquer auxdits traitements lorsque l’acte plus spécifique que constitue la directive 2016/680 n’est pas applicable. En particulier, selon le considérant 11 de cette directive, le RGPD s’applique au traitement de données à caractère personnel qui serait effectué par une ‘autorité compétente’, au sens de l’article 3, paragraphe 7, de ladite directive, mais à des fins autres que celles prévues dans celle-ci [voir, en ce sens, arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, point 70].

73. S’agissant de la première condition visée au point 67 du présent arrêt, et plus particulièrement des finalités poursuivies par les traitements de données à caractère personnel prévus par la directive PNR, il convient de rappeler que, conformément à l’article 1er, paragraphe 2, de cette directive, les données PNR 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. Ces finalités relèvent de celles visées à l’article 2, paragraphe 2, sous *d)*, du RGPD et à l’article 1er, paragraphe 1, de la directive 2016/680, de sorte que de tels traitements sont susceptibles de relever de l’exception visée à l’article 2, paragraphe 2, sous *d)*, de ce règlement et, par suite, de relever du champ d’application de cette directive.

74. En revanche, tel n’est pas le cas en ce qui concerne les traitements prévus par la directive API et par la directive 2010/65, dont les finalités sont autres que celles prévues à l’article 2, paragraphe 2, sous *d)*, du RGPD et à l’article 1er, paragraphe 1, de la directive 2016/680.

75. En effet, s’agissant de la directive API, celle-ci vise à améliorer les contrôles aux frontières et à lutter contre l’immigration clandestine, ainsi qu’il ressort de ses considérants 1, 7 et 9 ainsi que de son article 1er, au moyen de la transmission préalable aux autorités nationales compétentes, par les transporteurs, de données relatives aux passagers. D’ailleurs, plusieurs considérants et dispositions de cette directive mettent en évidence que les traitements de données prévus en vue de sa mise en œuvre relèvent du champ d’application du RGPD. Ainsi, le considérant 12 de ladite directive énonce que ‘ la directive [95/46] s’applique en ce qui

concerne le traitement des données à caractère personnel par les autorités des États membres ’. En outre, l’article 6, paragraphe 1, cinquième alinéa, de la directive API précise que les États membres peuvent faire également usage des données API pour répondre aux besoins des services répressifs, ‘ sous réserve des dispositions relatives à la protection des données figurant dans la directive [95/46] ’, cette expression étant également employée au troisième alinéa de cette disposition. De même est utilisée, notamment au considérant 9 de la directive API, l’expression ‘ sans préjudice des dispositions de la directive [95/46] ’. L’article 6, paragraphe 2, de la directive API prévoit, enfin, que les passagers doivent être informés, par les transporteurs, ‘ conformément aux dispositions de la directive [95/46] ’.

76. Quant à la directive 2010/65, il résulte de son considérant 2 et de son article 1er, paragraphe 1, que 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, afin de faciliter les transports maritimes et de réduire la charge administrative pesant sur les compagnies maritimes. Or, l’article 8, paragraphe 2, de ladite directive confirme que les traitements de données prévus en vue de sa mise en œuvre relèvent du champ d’application du RGPD, cette disposition imposant en effet aux États membres, concernant les données à caractère personnel, de s’assurer du respect de la directive 95/46.

77. Il s’ensuit que les traitements de données prévus par une législation nationale qui transpose, en droit interne, les dispositions de la directive API et de la directive 2010/65 relèvent du champ d’application du RGPD. En revanche, les traitements de données prévus par une législation nationale qui transpose, en droit interne, la directive PNR sont susceptibles d’échapper, conformément à l’exception figurant à l’article 2, paragraphe 2, sous *d)*, de ce règlement, à l’application de celui-ci, sous réserve du respect de la seconde condition rappelée au point 67 du présent arrêt, à savoir que l’auteur des traitements soit une autorité compétente, au sens de cette dernière disposition.

78. S’agissant de cette seconde condition, la Cour a jugé que, dans la mesure où la directive 2016/680 définit, à son article 3, paragraphe 7, la notion d’‘ autorité compétente ’, une telle définition doit être appliquée, par analogie, à l’article 2, paragraphe 2, sous *d)*, du RGPD [voir, en ce sens, arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, point 69].

79. Or, en vertu des articles 4 et 7 de la directive PNR, chaque État membre doit, respectivement, désigner, en tant que son UIP, 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, et arrêter une liste des autorités compétentes habilitées à demander à l’UIP ou à recevoir de celle-ci des données PNR ou le résultat du traitement de telles données, ces dernières autorités étant également des autorités compétentes en la matière, comme précisé à l’article 7, paragraphe 2, de ladite directive.

80. Il ressort de ces éléments que les traitements de données PNR effectués par l’UIP et lesdites autorités compétentes à de telles fins remplissent les deux conditions mentionnées au point 67 du présent arrêt, de sorte que ces traitements relèvent, outre des dispositions de la directive PNR elle-même, de celles de la directive 2016/680 et non du RGPD, ce que confirme au demeurant le considérant 27 de la directive PNR.

81. En revanche, dès lors que des opérateurs économiques, tels que des transporteurs aériens, même s'ils sont tenus à une obligation légale de transfert des données PNR, ne sont ni chargés de l'exercice de l'autorité publique ni investis de prérogatives de puissance publique par cette directive, ces opérateurs ne sauraient être regardés comme étant des autorités compétentes, au sens de l'article 3, paragraphe 7, de la directive 2016/680 et de l'article 2, paragraphe 2, sous *d)*, du RGPD, de sorte que le recueil et le transfert à l'UIP de ces données, par les transporteurs aériens, relèvent de ce règlement. La même conclusion s'impose dans une situation, telle que celle prévue par la loi du 25 décembre 2016, où le recueil et le transfert desdites données sont effectués par d'autres transporteurs ou par les opérateurs de voyage.

82. La juridiction de renvoi s'interroge, enfin, sur l'incidence éventuelle de l'adoption d'une législation nationale visant à transposer à la fois les dispositions de la directive PNR, de la directive API et de la directive 2010/65, à l'instar de la loi du 25 décembre 2016. À cet égard, il convient de rappeler que, ainsi qu'il ressort des points 72 et 75 à 77 du présent arrêt, les traitements de données prévus en vertu de ces deux dernières directives relèvent du champ d'application du RGPD, lequel contient des règles générales relatives à la protection des personnes physiques à l'égard du traitement de données à caractère personnel.

83. Ainsi, lorsqu'un traitement de données effectué sur la base de cette législation relève de la directive API et/ou de la directive 2010/65, le RGPD est applicable à ce traitement. Il en va de même d'un traitement de données effectué sur cette même base et relevant, quant à sa finalité, outre de la directive PNR, de la directive API et/ou de la directive 2010/65. Enfin, lorsqu'un traitement de données effectué sur la base de la même législation ne relève, quant à sa finalité, que de la directive PNR, le RGPD est applicable s'il s'agit du recueil et du transfert des données PNR à l'UIP, par les transporteurs aériens. En revanche, lorsqu'un tel traitement est effectué par l'UIP ou les autorités compétentes aux fins visées à l'article 1er, paragraphe 2, de la directive PNR, ce traitement relève, outre du droit national, de la directive 2016/680.

84. Eu égard aux considérations qui précèdent, il convient de répondre à la première question que l'article 2, paragraphe 2, sous *d)*, et l'article 23 du RGPD doivent être interprétés en ce sens que ce règlement est applicable aux traitements de données à caractère personnel prévus par une législation nationale visant à transposer, en droit interne, à la fois les dispositions de la directive API, de la directive 2010/65 et de la directive PNR pour ce qui est, d'une part, des traitements de données effectués par des opérateurs privés et, d'autre part, des traitements de données effectués par des autorités publiques relevant, uniquement ou également, de la directive API ou de la directive 2010/65. En revanche, ledit règlement n'est pas applicable aux traitements de données prévus par une telle législation ne relevant que de la directive PNR, qui sont effectués par l'UIP ou par les autorités compétentes aux fins visées à l'article 1er, paragraphe 2, de cette directive ».

B.21.4. Il découle de ce qui précède que le RGPD est applicable aux traitements de données à caractère personnel prévus par une législation nationale, telle que la loi du 25 décembre 2016, visant à transposer à la fois les dispositions de la directive PNR, de la directive API et de la directive 2010/65/UE, soit (1) lorsqu'un traitement de données effectué sur la base de cette législation relève de la directive API et/ou de la directive 2010/65/UE, soit (2) lorsqu'un traitement de données effectué sur cette même base, relève, quant à sa finalité, outre de la directive PNR, de la directive API et/ou de la directive 2010/65/UE, soit

(3) lorsqu'un traitement de données effectué sur la base de cette législation ne relève, quant à sa finalité, que de la directive PNR, mais qu'il s'agit du recueil et du transfert des données PNR à l'UIP, par les transporteurs aériens ou d'autres transporteurs, ou d'opérateurs de voyage.

En revanche, lorsqu'un traitement de données effectué sur la base de la même législation ne relève, quant à sa finalité, que de la directive PNR, et qu'il est effectué par l'UIP ou par les autorités compétentes aux fins visées à l'article 1er, paragraphe 2, de la directive PNR, le RGPD n'est pas applicable, mais ce traitement relève du droit national et de la directive « police ».

B.21.5. La Cour tient dès lors compte, dans l'examen du moyen, de l'article 23 du RGPD, sauf lorsque le traitement de données effectué sur la base de la loi du 25 décembre 2016 ne relève, quant à sa finalité, que de la directive PNR, et qu'il est effectué par l'UIP ou les autorités compétentes aux fins visées à l'article 1er, paragraphe 2, de la directive PNR.

B.21.6. Pour le surplus, la Cour constate que les parties requérantes ne déduisent pas de cette disposition des arguments distincts de ceux qui sont pris de la violation des articles 7 et 8 de la Charte.

B.21.7. L'exception du Conseil des ministres est rejetée dans cette mesure.

En ce qui concerne la validité de la directive PNR

B.22.1. Interrogée par la Cour sur la validité de la directive PNR, la Cour de justice a répondu, dans l'arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, que, « dès lors qu'une interprétation de la directive PNR à la lumière des articles 7, 8 et 21 ainsi que de l'article 52, paragraphe 1, de la Charte assure la conformité de cette directive avec ces articles de la Charte, l'examen des deuxième à quatrième et sixième questions n'a révélé aucun élément de nature à affecter la validité de ladite directive » (point 228).

B.22.2. À titre liminaire, la Cour de justice rappelle que, « selon un principe général d'interprétation, un acte de l'Union doit être interprété, dans la mesure du possible, d'une manière qui ne remette pas en cause sa validité et en conformité avec l'ensemble du droit primaire et, notamment, avec les dispositions de la Charte » (point 86), et qu'il incombe aux États membres, « lors de la mise en œuvre de ces mesures, non seulement d'interpréter leur droit national d'une manière conforme à la directive dont il s'agit, mais également de veiller à ne pas se fonder sur une interprétation de celle-ci qui entrerait en conflit avec les droits fondamentaux protégés par l'ordre juridique de l'Union ou avec les autres principes généraux reconnus dans cet ordre juridique » (point 87).

En ce qui concerne la directive PNR, la Cour de justice relève que « ses considérants 15, 20, 22, 25, 36 et 37 mettent l'accent sur l'importance que le législateur de l'Union accorde, en se référant à un niveau élevé de protection des données, au plein respect des droits fondamentaux consacrés aux articles 7, 8 et 21 de la Charte ainsi que du principe de proportionnalité » (point 88), de même que « l'article 19, paragraphe 2, de la directive PNR impose à la Commission, dans le cadre du réexamen de cette directive, d'accorder une attention particulière ' au respect des normes applicables de protection des données à caractère personnel ', ' à la nécessité et à la proportionnalité de la collecte et du traitement des données PNR au regard de chacune des finalités énoncées dans la présente directive' ainsi qu'à ' la durée de la période de conservation des données ' » (point 90).

B.22.3. Sur les ingérences résultant de la directive PNR dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, la Cour de justice constate que la directive PNR « comporte des ingérences d'une gravité certaine dans les droits garantis aux articles 7 et 8 de la Charte, dans la mesure notamment où elle vise à instaurer un régime de surveillance continu, non ciblé et systématique, incluant l'évaluation automatisée de données à caractère personnel de l'ensemble des personnes faisant usage de services de transport aérien » (point 111) :

« 97. Ainsi, tant le transfert des données PNR par les transporteurs aériens vers l'UIP de l'État membre concerné, prévu à l'article 1er, paragraphe 1, sous *a)*, de la directive PNR, lu en combinaison avec l'article 8 de celle-ci, que l'encadrement des conditions tenant à la conservation de ces données, à leur utilisation ainsi qu'à leurs éventuels transferts ultérieurs aux autorités compétentes de cet État membre, aux UIP et aux autorités compétentes des autres États membres, à Europol ou encore à des autorités de pays tiers, que permettent, notamment,

les articles 6, 7, 9 et 10 à 12 de cette directive, constituent des ingérences dans les droits garantis aux articles 7 et 8 de la Charte.

98. S'agissant de la gravité de ces ingérences, il convient de relever, premièrement, que, en vertu de son article 1er, paragraphe 1, sous *a)*, lu en combinaison avec son article 8, la directive PNR prévoit le transfert systématique et continu aux UIP des données PNR de tout passager empruntant un vol extra-UE, au sens de l'article 3, point 2, de cette directive, opéré entre des pays tiers et l'Union. Ainsi que M. l'avocat général l'a relevé au point 73 de ses conclusions, un tel transfert implique un accès général de la part des UIP à toutes les données PNR communiquées, concernant l'ensemble des personnes faisant usage de services de transport aérien, indépendamment de l'utilisation ultérieure de ces données.

99. Deuxièmement, l'article 2 de la directive PNR prévoit, à son paragraphe 1, que les États membres peuvent décider d'appliquer cette dernière aux vols intra-UE, au sens de l'article 3, point 3, de celle-ci, et précise, à son paragraphe 2, que, dans ce cas, toutes les dispositions de ladite directive ' s'appliquent aux vols intra-UE comme s'il s'agissait de vols extra-UE et aux données PNR des vols intra-UE comme s'il s'agissait de données PNR de vols extra-UE '.

100. Troisièmement, même si certaines des données PNR énumérées à l'annexe I de la directive PNR, telles que résumées au point 93 du présent arrêt, prises isolément, ne paraissent pas pouvoir révéler des informations précises 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 révéler des informations sensibles sur ces passagers [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 128].

101. Quatrièmement, en vertu de l'article 6, paragraphe 2, sous *a)* et *b)*, de la directive PNR, les données transférées par les transporteurs aériens sont destinées à faire l'objet non seulement d'une évaluation préalable, intervenant avant l'arrivée prévue ou le départ prévu des passagers, mais également d'une évaluation postérieure.

102. S'agissant de l'évaluation préalable, il ressort de l'article 6, paragraphe 2, sous *a)*, et paragraphe 3, de la directive PNR que cette évaluation est effectuée, par les UIP des États membres, de manière systématique et par des moyens automatisés, c'est-à-dire de manière continue et indépendamment du point de savoir s'il existe la moindre indication quant au risque d'implication des personnes concernées dans des infractions de terrorisme ou des formes graves de criminalité. À cette fin, ces dispositions prévoient que les données PNR peuvent être confrontées aux ' bases de données utiles ' et faire l'objet de traitements au regard de ' critères préétablis '.

103. Dans ce contexte, il convient de rappeler que la Cour a déjà jugé que l'étendue de l'ingérence que comportent les analyses automatisées des données PNR dans les droits consacrés aux articles 7 et 8 de la Charte dépend essentiellement des modèles et des critères préétablis ainsi que des bases de données sur lesquels se fonde ce type de traitement de données [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 172].

104. Or, ainsi que M. l'avocat général l'a relevé au point 78 de ses conclusions, le traitement prévu à l'article 6, paragraphe 3, sous *a)*, de la directive PNR, à savoir la confrontation des données PNR aux ' bases de données utiles ', est susceptible de fournir des informations supplémentaires sur la vie privée des passagers aériens et de permettre de tirer des conclusions très précises à ce sujet.

105. Quant aux traitements des données PNR au regard de ' critères préétablis ', prévus à l'article 6, paragraphe 3, sous *b)*, de la directive PNR, il est vrai que l'article 6, paragraphe 4, de cette directive exige que l'évaluation des passagers au moyen de ces critères soit réalisée de façon non discriminatoire et, notamment, sans être fondée sur toute une série de caractéristiques visées à la dernière phrase de ce paragraphe 4. En outre, les critères retenus doivent être ciblés, proportionnés et spécifiques.

106. Cela étant, la Cour a déjà jugé que, dans la mesure où des analyses automatisées des données PNR sont effectuées à partir de données à caractère personnel non vérifiées et où elles se fondent sur des modèles et des critères préétablis, elles présentent nécessairement un certain taux d'erreur [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 169]. En particulier, ainsi que M. l'avocat général l'a relevé, en substance, au point 78 de ses conclusions, il ressort du document de travail de la Commission [SWD(2020) 128 final] annexé à son rapport du 24 juillet 2020, portant réexamen de la directive PNR, que le nombre de cas de concordances positives résultant des traitements automatisés prévus à l'article 6, paragraphe 3, sous *a)* et *b)*, de cette directive qui se sont révélées erronées après réexamen individuel par des moyens non automatisés est assez conséquent et s'élevait, au cours des années 2018 et 2019, à au moins cinq personnes sur six identifiées. Ces traitements aboutissent ainsi à une analyse poussée des données PNR relatives auxdites personnes.

107. S'agissant de l'évaluation postérieure des données PNR prévue à l'article 6, paragraphe 2, sous *b)*, de la directive PNR, il ressort de cette disposition que, au cours de la période de six mois suivant le transfert des données PNR, visée à l'article 12, paragraphe 2, de cette directive, l'UIP est tenue, sur demande des autorités compétentes, de communiquer à celles-ci les données PNR et de procéder à un traitement dans des cas spécifiques, aux fins de la lutte contre les infractions terroristes ou les formes graves de criminalité.

108. En outre, même si, après l'expiration de cette période de six mois, les données PNR sont dépersonnalisées par un masquage de certains éléments de ces données, l'UIP peut être tenue, conformément à l'article 12, paragraphe 3, de la directive PNR, de communiquer, à la suite d'une telle demande, l'intégralité des données PNR sous une forme permettant d'identifier la personne concernée aux autorités compétentes lorsqu'il existe des motifs raisonnables de croire que cela est nécessaire aux fins visées à l'article 6, paragraphe 2, sous *b)*, de cette directive, une telle communication étant toutefois subordonnée à l'autorisation accordée par une autorité judiciaire ou une ' autre autorité nationale compétente '.

109. Cinquièmement, en prévoyant, à son article 12, paragraphe 1, sans fournir plus de précisions à cet égard, que les données PNR sont 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, la directive PNR permet, compte tenu du fait que, malgré leur dépersonnalisation à l'expiration de la période initiale de six mois par un masquage de certains éléments de données, l'intégralité des données PNR est encore susceptible d'être communiquée dans l'hypothèse visée au point précédent, de disposer d'informations sur la vie

privée des passagers aériens sur une durée que la Cour a déjà qualifiée, dans son avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 132), de particulièrement longue.

110. Au regard du caractère habituel de l'usage des transports aériens, un tel délai de conservation a pour conséquence qu'une très grande partie de la population de l'Union est susceptible de voir ses données PNR conservées, de manière répétée, dans le cadre du système institué par la directive PNR et, de ce fait, accessibles à des analyses effectuées dans le cadre des évaluations préalables et postérieures de l'UIP et des autorités compétentes pendant une période considérable, voire indéfinie, s'agissant des personnes qui voyagent par avion plus d'une fois tous les cinq ans ».

B.22.4.1. Sur la justification des ingérences résultant de la directive PNR, la Cour de justice rappelle plus particulièrement « la possibilité pour les États membres de justifier une limitation aux droits garantis aux articles 7 et 8 de la Charte doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité » (point 116) :

« 117. Pour satisfaire à l'exigence de proportionnalité, la réglementation en cause comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application des mesures qu'elle prévoit 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 lorsque les données PNR sont de nature à pouvoir révéler des informations sensibles sur les passagers [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141, ainsi que arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 132 et jurisprudence citée].

118. Ainsi, une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 191 et jurisprudence citée, ainsi que arrêts du 3 octobre 2019, A e.a., C-70/18, EU:C:2019:823, point 63, et du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 133].

a) Sur le respect du principe de légalité et du contenu essentiel des droits fondamentaux en cause

119. La limitation de l'exercice des droits fondamentaux garantis aux articles 7 et 8 de la Charte résultant du système établi par la directive PNR est prévue par un acte législatif de l'Union. Quant à la question de savoir si, conformément à la jurisprudence rappelée au point 114 du présent arrêt, cette directive, en tant qu'acte du droit de l'Union qui permet l'ingérence dans ces droits, définit elle-même la portée de la limitation de l'exercice desdits droits, il convient de relever que les dispositions de ladite directive ainsi que les annexes I et II de celle-ci contiennent, d'une part, une énumération des données PNR et, d'autre part, encadrent le traitement de ces données, notamment, en définissant les finalités et les modalités de ces traitements. Du reste, cette question se confond largement avec celle du respect de l'exigence de proportionnalité rappelée au point 117 du présent arrêt (voir, en ce sens, arrêt du 16 juillet 2020, Facebook *Ireland et Schrems*, C-311/18, EU:C:2020:559, point 180) et sera examinée aux points 125 et suivants du présent arrêt.

120. En ce qui concerne le respect du contenu essentiel des droits fondamentaux consacrés aux articles 7 et 8 de la Charte, il est vrai que les données PNR peuvent, le cas échéant, révéler des informations très précises sur la vie privée d'une personne. Toutefois, dans la mesure où, d'une part, la nature de ces informations est limitée à certains aspects de cette vie privée, relatifs en particulier aux voyages aériens de cette personne, et, d'autre part, la directive PNR interdit expressément, à son article 13, paragraphe 4, le traitement de données sensibles, au sens de l'article 9, paragraphe 1, du RGPD, les données visées par cette directive ne permettent pas, à elles seules, d'avoir un aperçu complet de la vie privée d'une personne. En outre, ladite directive circonscrit, à son article 1er, paragraphe 2, lu en combinaison avec son article 3, points 8 et 9, ainsi qu'avec son annexe II, les finalités du traitement de ces données. Enfin, cette même directive fixe, à ses articles 4 à 15, des règles encadrant le transfert, les traitements et la conservation desdites données ainsi que des règles destinées à assurer, notamment, la sécurité, la confidentialité et l'intégrité de ces mêmes données, ainsi qu'à les protéger contre les accès et les traitements illégaux. Dans ces conditions, les ingérences que comporte la directive PNR ne portent pas atteinte au contenu essentiel des droits fondamentaux consacrés aux articles 7 et 8 de la Charte.

b) Sur l'objectif d'intérêt général et l'aptitude des traitements des données PNR au regard de cet objectif

121. S'agissant de la question de savoir si le système établi par la directive PNR poursuit un objectif d'intérêt général, il ressort des considérants 5, 6 et 15 de cette directive que celle-ci a pour objectif d'assurer la sécurité intérieure de l'Union et ainsi de protéger la vie et la sécurité des personnes, tout en créant un cadre juridique qui garantit un niveau de protection élevé des droits fondamentaux des passagers, en particulier des droits au respect de la vie privée et à la protection des données à caractère personnel, lorsque des données PNR sont traitées par les autorités compétentes.

122. À cet effet, l'article 1er, paragraphe 2, de la directive PNR dispose que les données PNR recueillies conformément à cette directive ne peuvent faire l'objet des traitements prévus à l'article 6, paragraphe 2, sous *a)* à *c)*, de celle-ci 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. Or, ces finalités constituent indubitablement des objectifs d'intérêt

général de l'Union susceptibles de justifier des ingérences, mêmes graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte [voir, en ce sens, arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 42, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 148 et 149].

123. En ce qui concerne l'aptitude du système établi par la directive PNR à réaliser les objectifs poursuivis, il convient de constater que, si la possibilité de résultats ' faux négatifs ' et le nombre assez conséquent de résultats ' faux positifs ' qui, ainsi qu'il a été relevé au point 106 du présent arrêt, ont été obtenus à la suite des traitements automatisés prévus par cette directive au cours des années 2018 et 2019 sont de nature à limiter l'aptitude de ce système, ils ne sont toutefois pas de nature à rendre ledit système inapte à contribuer à la réalisation de l'objectif tenant à la lutte contre les infractions terroristes et les formes graves de criminalité. En effet, ainsi qu'il ressort du document de travail de la Commission visé au point 106 du présent arrêt, les traitements automatisés effectués au titre de ladite directive ont effectivement déjà permis l'identification de passagers aériens présentant un risque dans le cadre de la lutte contre des infractions terroristes et des formes graves de criminalité.

124. En outre, eu égard au taux d'erreur inhérent aux traitements automatisés des données PNR et, notamment, au nombre assez conséquent de résultats ' faux positifs ', l'aptitude du système établi par la directive PNR, dépend essentiellement du bon fonctionnement de la vérification subséquente des résultats obtenus au titre de ces traitements, par des moyens non automatisés, tâche qui incombe, en vertu de cette directive, à l'UIP. Les dispositions prévues à cet effet par ladite directive contribuent donc à la réalisation de ces objectifs ».

B.22.4.2. Concernant le caractère nécessaire des ingérences résultant de la directive PNR, la Cour de justice rappelle qu'« il convient de vérifier si les ingérences résultant de la directive PNR sont limitées au strict nécessaire et, notamment, si cette directive énonce des règles claires et précises qui régissent la portée et l'application des mesures qu'elle prévoit et si le système qu'elle établit répond toujours à des critères objectifs, établissant un rapport entre les données PNR, qui sont étroitement liées à la réservation et à la réalisation de voyages aériens, et les finalités poursuivies par ladite directive, à savoir la lutte contre les infractions terroristes et les formes graves de criminalité » (point 125).

La Cour de justice conclut n'avoir révélé aucun élément de nature à affecter la validité de la directive PNR « dès lors qu'une interprétation de la directive PNR à la lumière des articles 7, 8 et 21 ainsi que de l'article 52, paragraphe 1, de la Charte assure la conformité de cette directive avec ces articles de la Charte » (point 228), respectant ainsi les limites du strict nécessaire, en apportant plusieurs précisions concernant (1) les données des passagers aériens visés par la directive PNR (points 126-140), (2) les finalités de traitement des données PNR

(points 141-152), (3) le lien entre les données PNR et les finalités des traitements de ces données (points 153-157), (4) les passagers aériens et les vols concernés (points 158-175), (5) l'évaluation préalable des données PNR au moyen de traitements automatisés (points 176-213) et (6) la communication et l'évaluation postérieures des données PNR (points 214-227).

B.22.5. Dans l'examen du moyen, la Cour tient compte de ces précisions apportées par la Cour de justice quant à l'interprétation de la directive PNR.

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

B.23.1. 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.

B.23.2. Par son arrêt n° 135/2019 du 17 octobre 2019, la Cour a jugé que le moyen n'est pas fondé en ce qu'il est dirigé contre les modalités d'exécution de la loi du 25 décembre 2016 (articles 3, § 2 et 7, § 3 – B.21 à B.29) et contre les notions de « documents d'identité » et de « documents de voyage » (article 7, §§ 1er et 2 – B.30 à B.33).

B.23.3. Les griefs qui doivent encore être examinés, compte tenu de la réponse de la Cour de justice dans son arrêt du 21 juin 2022, sont dirigés contre les aspects suivants :

1. les données visées (articles 4, 9°, et 9) (B.24-B.34);

2. la notion de « passager » (article 4, 10°) (B.35-B.41);

3. les finalités du traitement des données PNR (article 8) (B.42-B.56);

4. la gestion de la banque de données des passagers et le traitement des données dans le cadre de l'évaluation préalable et des recherches ponctuelles (articles 12 à 16 et 24 à 27 et articles 50 et 51) (B.57-B.70);

5. la durée de conservation des données PNR (article 18) (B.71 – B.75).

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

B.24. La partie requérante allègue 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.25.1. Conformément aux principes rappelés en B.17 et B.18, 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*, ECLI:CE:ECHR:1987:0326JUD000924881, § 48; grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, ECLI:CE:ECHR:2000:0504JUD002834195, § 46; CJUE, grande chambre, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland Ltd e.a.*, ECLI:EU:C:2014:238) doit donc reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur.

B.25.2. 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.19.

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 inapproprié et abusif, par les services publics, des données à caractère personnel traitées (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, ECLI:CE:ECHR:2000:0504JUD002834195, § 59; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K. c. France*, ECLI:CE:ECHR:2013:0418JUD001952209, §§ 37 et 42-44; 18 septembre 2014, *Brunet c. France*, ECLI:CE:ECHR:2014:0918JUD002101010, §§ 35-37; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, ECLI:CE:ECHR:2016:0112JUD003713814, § 68; CJUE, grande chambre, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland Ltd e.a.*, ECLI:EU:C:2014:238, points 56-66).

B.25.3. 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) ».

B.26.1. 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.4.1, 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.

B.26.2.1. 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.26.2.2. 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 :

« 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.27.1. 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;

- 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.27.2.1. 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.27.2.2. 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;

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.28.1. 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.28.2. 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.28.3.1. L'annexe I de la directive PNR, intitulée « Données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens », dispose :

« 1. Code repère du dossier passager

2. Date de réservation/d'émission du billet

3. Date(s) prévue(s) du voyage

4. Nom(s)

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

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

7. Itinéraire complet pour le PNR concerné

8. Informations ' grands voyageurs '

9. Agence de voyages/agent de voyages

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

11. Indications concernant la scission/division du PNR

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

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

14. Numéro du siège et autres informations concernant le siège

15. Informations sur le partage de code

16. Toutes les informations relatives aux bagages

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

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

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

B.28.3.2. La rubrique 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.29.1.1. 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;

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.29.1.2. 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.29.2.1. 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;

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.29.2.2. Les données API visées à l'article 9, § 2, de la loi du 25 décembre 2016 reprennent, pour l'essentiel, les données visées à la rubrique 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.30.1. Par son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, la Cour de justice a, en réponse aux questions préjudicielles posées par la Cour quant à la validité de la directive PNR, s'agissant des données des passagers aériens visés par la directive PNR (points 126-140), rappelé, à titre liminaire, le considérant 15 de la directive PNR et le fait que l'article 13, paragraphe 4, première phrase, de la directive PNR interdit « le traitement des données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle », pour considérer que « les données PNR recueillies et communiquées conformément à l'annexe I de la directive PNR doivent présenter un rapport direct avec le vol effectué et le passager concerné et doivent être limitées de manière, d'une part, à répondre uniquement aux 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, et, d'autre part, à exclure des données sensibles » (point 128).

La Cour de justice juge que les rubriques 1 à 4, 7, 9, 11, 15, 17 et 19 de l'annexe I de la directive PNR répondent à ces exigences ainsi qu'à celles de clarté et de précision, en ce qu'elles visent des informations clairement identifiables et circonscrites, en rapport direct avec le vol effectué et avec le passager concerné, et qu'il en va de même, nonobstant leur libellé ouvert, des rubriques 10, 13, 14 et 16 (point 129).

B.30.2. En revanche, la Cour de justice estime nécessaire d'apporter les précisions suivantes aux fins de l'interprétation des rubriques 5, 6, 8, 12 et 18 :

« 131. En ce qui concerne la rubrique 5, qui vise l’ ’ [a]dresse et [les] coordonnées (numéro de téléphone, adresse électronique) ’, cette rubrique ne précise pas expressément si ladite adresse et lesdites coordonnées se réfèrent au seul passager aérien ou également aux tiers ayant effectué la réservation du vol pour le passager aérien, aux tiers par l’intermédiaire desquels un passager aérien peut être joint, ou encore aux tiers devant être informés en cas d’urgence. Toutefois, ainsi que M. l’avocat général l’a relevé, en substance, au point 162 de ses conclusions, compte tenu des exigences de clarté et de précision, cette rubrique ne saurait être interprétée comme permettant, de manière implicite, également la collecte et la transmission de données à caractère personnel de tels tiers. Par conséquent, il convient d’interpréter ladite rubrique comme ne visant que l’adresse postale et les coordonnées, à savoir le numéro de téléphone et l’adresse électronique, du passager aérien au nom duquel la réservation est faite.

132. S’agissant de la rubrique 6, qui vise ‘ [t]outes les informations relatives aux modes de paiement, y compris l’adresse de facturation ’, cette rubrique doit être interprétée, afin de répondre aux exigences de clarté et de précision, en ce sens qu’elle concerne seulement 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 [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 159].

133. Pour ce qui est de la rubrique 8, qui vise les ‘ informations “ grands voyageurs ” ’, elle doit être interprétée, ainsi que M. l’avocat général l’a relevé au point 164 de ses conclusions, comme visant exclusivement les données relatives au statut du passager concerné dans le contexte d’un programme de fidélisation d’une compagnie aérienne donnée ou d’un groupe de compagnies aériennes donné ainsi que le numéro identifiant ce passager en tant que ‘ grand voyageur ’. La rubrique 8 ne permet donc pas la collecte des informations relatives aux transactions par lesquelles ce statut a été acquis.

134. En ce qui concerne la rubrique 12, celle-ci vise les ‘ [r]emarques 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) ’.

135. À cet égard, il y a lieu de relever d’emblée que, si les termes ‘ remarques générales ’ ne répondent pas aux exigences de clarté et de précision en ce qu’ils ne fixent, en tant que tels, aucune limitation quant à la nature et à l’étendue des informations pouvant être recueillies et communiquées à une UIP au titre de la rubrique 12 [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 160], l’énumération qui figure entre parenthèses satisfait, quant à elle, à ces exigences.

136. Par conséquent, pour donner à la rubrique 12 une interprétation qui, en application de la jurisprudence rappelée au point 86 du présent arrêt, rende celle-ci conforme aux exigences de clarté et de précision et, plus largement, aux articles 7 et 8 ainsi qu’à l’article 52, paragraphe 1, de la Charte, il convient de considérer que seules sont admises la collecte et la communication des renseignements expressément énumérés dans cette rubrique, à savoir le nom et le sexe du passager aérien 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.

137. Enfin, s'agissant de la rubrique 18, celle-ci vise ' [t]oute 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) '.

138. Comme M. l'avocat général l'a relevé, en substance, aux points 156 à 160 de ses conclusions, il ressort de cette rubrique 18, lue à la lumière des considérants 4 et 9 de la directive PNR, que les renseignements auxquels elle se réfère sont exhaustivement les données API énumérées à ladite rubrique ainsi qu'à l'article 3, paragraphe 2, de la directive API.

139. Ainsi, la rubrique 18, à la condition qu'elle soit interprétée comme ne couvrant que les renseignements expressément visés par cette même rubrique ainsi qu'audit article 3, paragraphe 2, de la directive API, peut être considérée comme répondant aux exigences de clarté et de précision [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 161].

140. Dès lors, il convient de constater que, interprétée conformément aux considérations exposées notamment aux points 130 à 139 du présent arrêt, l'annexe I de la directive PNR présente dans son ensemble un caractère suffisamment clair et précis, délimitant ainsi la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte ».

B.31.1. 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*, ECLI:EU:C:2014:238, 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, ECLI:EU:C:2017:592, points 148 et 149; CJUE, grande chambre, 21 juin 2022, C-817/19, *Ligue des droits humains c. Conseil des ministres*, ECLI:EU:C:2022:491, point 122).

B.31.2. 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.31.3. Tout d'abord, comme il est dit en B.4.1, ces données sont déterminées de manière exhaustive par l'article 9 de la loi du 25 décembre 2016.

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.26.2.2, 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, grande chambre, 26 juillet 2017, avis 1/15, ECLI:EU:C:2017:592, point 156). Ces données sont dès lors pertinentes eu égard aux objectifs poursuivis par la loi du 25 décembre 2016.

B.31.4.1. 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.31.4.2. 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).

B.31.5. Ces dispositions garantissent ainsi que des données sensibles ne peuvent pas être collectées ou conservées au titre de « données des passagers » visées par la loi du 25 décembre 2016 (article 10). Les données qui excéderaient celles qui sont exhaustivement énumérées dans l'article 9 ou celles qui comporteraient des données sensibles sont effacées par l'UIP (article 11).

Cette garantie, en ce qui concerne les données sensibles, rejoint ainsi celle que la Cour de justice a soulignée dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, concernant le considérant 15 et l'article 13, paragraphe 4, première phrase, de la directive PNR (point 128), comme elle l'avait déjà souligné dans son avis n° 1/15 du 26 juillet 2017, précité (point 167).

La circonstance que de telles données, lorsqu'elles sont combinées, seraient susceptibles de révéler des informations sensibles ne conduit pas à une autre conclusion, dès lors qu'une telle opération supposerait un traitement ultérieur des données énumérées dans l'article 9 de la loi du 25 décembre 2016, qui ne correspondrait pas aux objectifs et finalités poursuivis par la loi du 25 décembre 2016.

B.32.1. Comme il est dit en B.29, les données PNR visées à l'article 9, § 1er, de la loi du 25 décembre 2016 correspondent aux données visées dans l'annexe I de la directive PNR, et les données API visées à l'article 9, § 2, de la loi du 25 décembre 2016 reprennent, pour l'essentiel, les données visées dans la rubrique 18 de l'annexe I de la directive PNR.

B.32.2. Il convient maintenant d'examiner si ces ingérences sont suffisamment précises, proportionnées et limitées au « strict nécessaire » pour atteindre les objectifs poursuivis par la loi du 25 décembre 2016, en tenant compte de l'arrêt de la Cour de justice en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, rappelé en B.30.

B.33.1. Il ressort de l’arrêt de la Cour de justice précité que les données PNR « doivent présenter un rapport direct avec le vol effectué et le passager concerné et doivent être limitées de manière, d’une part, à répondre uniquement aux 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, et, d’autre part, à exclure des données sensibles » (point 128). Ces considérations sont transposables aux autres moyens de transport visés par le système PNR.

De manière analogue à ce que la Cour de justice a jugé en ce qui concerne la directive PNR (point 129), la Cour constate que les données visées à l’article 9, § 1er, 1° à 4°, 7°, 9°, 11°, 15°, 17° et 19°, de la loi du 25 décembre 2016 répondent à ces exigences ainsi qu’à celles de clarté et de précision, en ce qu’elles visent des informations clairement identifiables et circonscrites, en rapport direct avec le vol effectué et avec le passager concerné, et il en va de même, nonobstant leur libellé ouvert, des données visées à l’article 9, § 1er, 10°, 13°, 14° et 16°, de la même loi.

B.33.2. En ce qui concerne l’article 9, § 1er, 5°, de la loi du 25 décembre 2016, qui vise « l’adresse et les coordonnées (numéro de téléphone, adresse électronique) », il convient d’interpréter ces termes, de manière analogue à ce que la Cour de justice a jugé en ce qui concerne la rubrique 5 de la directive PNR (point 131), comme ne visant que l’adresse postale et les coordonnées, à savoir le numéro de téléphone et l’adresse électronique, du passager au nom duquel la réservation est faite. De la sorte, ces termes ne peuvent être interprétés comme permettant, de manière implicite, également la collecte et la transmission de données à caractère personnel de tiers.

B.33.3. En ce qui concerne l’article 9, § 1er, 6°, de la loi du 25 décembre 2016, qui vise « les informations relatives aux modes de paiement, y compris l’adresse de facturation », il convient, afin de répondre aux exigences de clarté et de précision, d’interpréter ces termes de manière analogue à ce que la Cour de justice a jugé en ce qui concerne la rubrique 6 de la directive PNR (point 132), en ce sens qu’ils visent seulement les informations relatives aux modalités de paiement et à la facturation du billet d’avion ou du titre de transport, à l’exclusion de toute autre information sans rapport direct avec le vol ou le trajet.

B.33.4. En ce qui concerne l'article 9, § 1er, 8°, de la loi du 25 décembre 2016, qui vise « les informations relatives aux ' voyageurs enregistrés ', c'est-à-dire les grands voyageurs », il convient d'interpréter ces termes de manière analogue à ce que la Cour de justice a jugé en ce qui concerne la rubrique 8 de la directive PNR (point 133), en ce sens qu'ils visent exclusivement les données relatives au statut du passager concerné dans le contexte d'un programme de fidélisation d'une compagnie aérienne donnée ou d'un groupe de compagnies aériennes donné, ou dans un autre système de fidélisation pour les voyageurs fréquents, ainsi que le numéro identifiant ce passager en tant que « grand voyageur » ou bénéficiaire d'un autre système de fidélité. Ainsi interprétés, ces termes ne permettent donc pas la collecte des informations relatives aux transactions par lesquelles ce statut a été acquis.

B.33.5. En ce qui concerne l'article 9, § 1er, 12°, de la loi du 25 décembre 2016, qui vise « 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 », il convient d'interpréter ces termes de manière analogue à ce que la Cour de justice a jugé en ce qui concerne la rubrique 12 de la directive PNR (points 134-136), en ce sens que seules sont admises la collecte et la communication des renseignements expressément énumérés dans cette disposition, à savoir le nom et le sexe du passager aérien ou du voyageur 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.

Interprété comme établissant de manière exhaustive une liste de données, l'article 9, § 1er, 12°, de la loi du 25 décembre 2016 satisfait aux exigences de clarté et de précision.

B.33.6.1. L'article 9, § 1er, 18°, de la loi du 25 décembre 2016 vise « toutes les données préalables sur les passagers (données API) qui ont été collectées et sont énumérées au § 2 », à

savoir : le type de document de voyage (1°), le numéro de document (2°), la nationalité (3°), le pays de délivrance du document (4°), la date d'expiration du document (5°), le nom de famille, le prénom, le sexe, la date de naissance (6°), le transporteur/opérateur de voyage (7°), le numéro du transport (8°), la date de départ, la date d'arrivée (9°), le lieu de départ, le lieu d'arrivée (10°), l'heure de départ, l'heure d'arrivée (11°), le nombre total de personnes transportées *(12°)*, le numéro de siège (13°), *le code repère du PNR (14°)*, le nombre, le poids et l'identification des bagages (15°) et le point de passage frontalier utilisé pour entrer sur le territoire national (16°).

En ce qui concerne la rubrique 18 de la directive PNR, la Cour de justice a jugé qu'à la condition qu'elle soit interprétée comme ne couvrant que les renseignements expressément visés par cette même rubrique ainsi qu'audit article 3, paragraphe 2, de la directive API, cette rubrique peut être considérée comme répondant aux exigences de clarté et de précision (points 137-139).

B.33.6.2. La Cour constate, à cet égard, que, contrairement à la rubrique 18 de la directive PNR, l'article 9, § 1er, 18°, de la loi du 25 décembre 2016 se réfère à une liste de données exhaustivement énumérées à l'article 9, § 2, de la même loi, de sorte que ces dispositions répondent aux exigences de clarté et de précision.

B.33.6.3. En ce qui concerne l'étendue des « données API » visées à l'article 9, § 2, de la loi du 25 décembre 2016, ces données reprennent, pour l'essentiel, comme il est dit en B.29, les données visées dans la rubrique 18 de l'annexe I de la directive PNR.

Ainsi, les données visées à l'article 9, § 2, 1° à 11°, de la loi du 25 décembre 2016 correspondent exactement aux données expressément énumérées dans la rubrique 18 précitée.

Par ailleurs, les données visées à l'article 9, § 2, 12°, 14° et 16°, de la loi du 25 décembre 2016 correspondent exactement aux données expressément énumérées dans l'article 3, paragraphe 2, de la directive API.

B.33.6.4. Il en découle que seules les données API visées à l'article 9, § 2, 13° et 15°, de la loi du 25 décembre 2016, à savoir le numéro de siège (13°) et le nombre, le poids et l'identification des bagages (15°) ne correspondent pas expressément aux renseignements visés

par la rubrique 18 de l'annexe I de la directive PNR ainsi que par l'article 3, paragraphe 2, de la directive API.

Le constat qui précède n'aboutit cependant pas à considérer que ces données manqueraient de clarté et de précision, ni qu'elles dépasseraient la limite du « strict nécessaire » pour atteindre les objectifs poursuivis par la loi du 25 décembre 2016.

En effet, comme il est indiqué en B.3.2, les données API sont les données qui sont transmises dans le cadre du check-in et l'embarquement, et qui sont moins rapidement disponibles que les données PNR. De telles données sont, comme le souligne l'avocat général Pitruzzella dans ses conclusions présentées le 27 janvier 2022 dans l'affaire C-817/19, « recueillies par les transporteurs aériens dans le cours normal de leurs activités » (ECLI:EU:C:2022:65, point 160), et elles le sont, le cas échéant, par les autres transporteurs. Ce n'est que si les données sont collectées par les transporteurs dans le cadre de leurs activités normales qu'elles relèvent des données API visées à l'article 9, § 1er, 18°, de la loi du 25 décembre 2016, dès lors que, comme il est dit en B.26.2.2, la loi précitée ne crée pas d'obligation additionnelle de collecte des données.

Les données PNR mentionnées dans l'article 9, § 1er, 14° et 16°, visent déjà respectivement – comme les rubriques 14 et 16 de la directive PNR – « le numéro du siège et autres informations concernant le siège » et « toutes les informations relatives aux bagages », et de telles données sont considérées, comme il est dit en B.33.1, comme répondant aux exigences de clarté et de précision et comme présentant un rapport direct avec le vol ou le trajet effectué, et avec les objectifs poursuivis en l'espèce. L'article 9, § 1er, 19°, vise également, parmi les données PNR, « l'historique complet des modifications des données énumérées aux 1° à 18° », y compris les modifications éventuelles concernant le siège ou les bagages. Les informations concernant le siège et les bagages, visées à l'article 9, § 2, 13° et 15°, sont dès lors déjà comprises dans les données visées à l'article 9, § 1er, 14° et 16°.

En visant expressément, parmi les données API, à savoir les données recueillies au stade du check-in et de l'embarquement, les informations concernant le siège et les bagages, l'article 9, § 2, 13° et 15°, de la loi du 25 décembre 2016 ne crée dès lors pas de données

additionnelles par rapport à la liste des données à collecter en vertu de l'article 9, § 1er, 14° et 16°, et répond ainsi aux exigences de clarté et de précision et de proportionnalité.

B.34. Sous réserve des interprétations mentionnées en B.33.2 à B.33.5, le moyen, en ce qu'il est dirigé contre les articles 4, 9°, et 9 de la loi du 25 décembre 2016, n'est pas fondé.

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

B.35. 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.36.1. 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 ».

B.36.2. 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 transportée 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.

La loi du 25 décembre 2016 instaure la collecte, le transfert et l'utilisation généralisés et indifférenciés des données PNR pour l'ensemble des passagers qui voyagent par transport aérien, indépendamment d'un passage aux frontières extérieures de l'Union, et cette collecte de données a été étendue au transport ferroviaire ou par bus, par les arrêtés royaux des 3 février 2019, cités en B.8.

B.36.3. 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 du Conseil de l'Europe n° 108 « 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 :

« 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.36.4.1. 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 ».

Conformément à cette disposition, la Commission a adressé au Parlement européen et au Conseil son rapport « sur le réexamen de la directive 2016/681 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 », le 24 juillet 2020 (COM(2020) 305 final).

Ce rapport conclut :

« L'évaluation par la Commission des deux premières années d'application de la directive est globalement positive. La principale conclusion de ce réexamen est que la directive contribue positivement à son principal objectif de garantir la mise en place de systèmes PNR efficaces au sein des États membres, en tant qu'instrument de lutte contre le terrorisme et les formes graves de criminalité » (p. 14).

En ce qui concerne le champ d'application de la collecte des données PNR, la Commission a souligné :

« Tous les États membres, à une exception près, ont étendu la collecte des données PNR aux vols intra-UE. Les autorités nationales perçoivent la collecte des données PNR pour les

vols intra-UE (et en particulier intra-Schengen) comme un outil répressif important permettant de suivre les déplacements de suspects connus et d'identifier les schémas de déplacement suspects d'individus inconnus qui pourraient être impliqués dans des activités criminelles/terroristes lorsqu'ils voyagent dans l'espace de Schengen. Puisque les États membres recueillent déjà en réalité les données PNR pour les vols intra-UE, la Commission estime qu'il n'est pas essentiel de rendre obligatoire la collecte des données PNR pour les vols intra-UE à ce stade » (p. 11).

B.36.4.2. 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.37. Interrogée par la Cour au sujet d'un système de collecte, de transfert et d'utilisation généralisés et indifférenciés des données PNR pour l'ensemble des « passagers », indépendamment d'un passage aux frontières extérieures de l'Union, la Cour de justice a répondu, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité :

« 158. Le système établi par la directive PNR couvre les données PNR de l'ensemble des personnes qui répondent à la notion de ' passager ', au sens de l'article 3, point 4, de cette directive, et empruntent des vols relevant du champ d'application de celle-ci.

159. Selon l'article 8, paragraphe 1, de ladite directive, ces données sont transférées à l'UIP de l'État membre sur le territoire duquel le vol doit atterrir ou du territoire duquel il doit décoller, indépendamment de tout élément objectif permettant de considérer que les passagers concernés sont susceptibles de présenter un risque d'être impliqués dans des infractions terroristes ou des formes graves de criminalité. Cependant, les données ainsi transférées sont, notamment, soumises à des traitements automatisés dans le cadre de l'évaluation préalable au titre de l'article 6, paragraphe 2, sous *a)*, et paragraphe 3, de la directive PNR, cette évaluation ayant pour finalité, ainsi qu'il ressort du considérant 7 de cette directive, d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité avant cette évaluation et qui devraient être soumises à un examen plus approfondi par les autorités compétentes.

160. Plus particulièrement, il ressort de l'article 1er, paragraphe 1, sous *a)*, et de l'article 2 de la directive PNR que celle-ci distingue les passagers empruntant des vols extra-UE, opérés entre l'Union et des pays tiers, et ceux empruntant des vols intra-UE, opérés entre différents États membres.

161. S'agissant des passagers des vols extra-UE, il y a lieu de rappeler que, s'agissant des passagers empruntant des vols entre l'Union et le Canada, la Cour a déjà jugé que le traitement automatisé de leurs données PNR, préalablement à leur arrivée 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 [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 187].

162. Or, ces considérations peuvent être transposées mutatis mutandis à la situation des passagers empruntant des vols opérés entre l'Union et l'ensemble des pays tiers, que les États membres sont obligés de soumettre au système établi par la directive PNR conformément à l'article 1er, paragraphe 1, sous *a)*, de cette directive, lu en combinaison avec l'article 3, points 2 et 4, de ladite directive. En effet, le transfert et l'évaluation préalable des données PNR des passagers aériens entrant ou sortant de l'Union ne peuvent être limités à un cercle déterminé de passagers aériens, compte tenu de la nature même des menaces pour la sécurité publique pouvant résulter d'infractions terroristes et de formes graves de criminalité qui présentent un lien objectif, à tout le moins indirect, avec le transport aérien des passagers entre l'Union et des pays tiers. Ainsi, il y a lieu de considérer que le rapport nécessaire entre ces données et l'objectif ayant trait à la lutte contre de telles infractions existe, de sorte que la directive PNR ne dépasse pas les limites du strict nécessaire du seul fait qu'elle impose aux États membres le transfert et l'évaluation préalable systématiques des données PNR de l'ensemble de ces passagers.

163. S'agissant des passagers empruntant des vols entre différents États membres de l'Union, l'article 2, paragraphe 1, de la directive PNR, lu en combinaison avec le considérant 10 de celle-ci, prévoit seulement la faculté pour les États membres d'étendre l'application du système établi par cette directive aux vols intra-UE.

164. Ainsi, le législateur de l'Union n'a pas entendu imposer aux États membres l'obligation d'étendre l'application du système établi par la directive PNR aux vols intra-UE mais, comme il ressort de l'article 19, paragraphe 3, de cette directive, a réservé sa décision sur une telle extension, tout en estimant que celle-ci devait être précédée d'une évaluation détaillée de ses incidences juridiques, notamment sur les droits fondamentaux des personnes concernées.

165. À cet égard, il convient de faire observer que, en énonçant que le rapport de réexamen de la Commission visé à l'article 19, paragraphe 1, de la directive PNR ' examine également s'il est nécessaire, proportionné et efficace d'inclure dans le champ d'application de la présente directive la collecte et le transfert des données PNR, à titre obligatoire, pour l'ensemble des vols intra-UE ou une sélection de ceux-ci ', et qu'elle doit, à cet égard, tenir 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 ', l'article 19, paragraphe 3, de cette directive met en évidence que, pour le législateur de l'Union, le système établi par ladite directive ne doit pas nécessairement être étendu à tous les vols intra-UE.

166. Dans le même ordre d'idées, l'article 2, paragraphe 3, de la directive PNR dispose que les États membres peuvent décider d'appliquer cette directive uniquement à certains vols intra-UE lorsqu'ils le jugent nécessaire afin de poursuivre les objectifs de ladite directive, tout en pouvant modifier la sélection de ces vols à tout moment.

167. En tout cas, la faculté pour les États membres d'étendre l'application du système établi par la directive PNR aux vols intra-UE doit s'exercer, ainsi qu'il ressort du considérant 22 de celle-ci, dans le plein respect des droits fondamentaux garantis aux articles 7 et 8 de la Charte. À cet égard, si, conformément au considérant 19 de ladite directive, il appartient aux États membres d'évaluer les menaces liées aux infractions terroristes et aux formes graves de criminalité, il n'en reste pas moins que l'exercice de cette faculté présuppose que, lors de cette

évaluation, les États membres concluent à l'existence d'une menace liée à de telles infractions qui est de nature à justifier l'application de la même directive également à des vols intra-UE.

168. Dans ces conditions, un État membre, lorsqu'il souhaite faire usage de la faculté prévue à l'article 2 de la directive PNR, que ce soit pour l'ensemble des vols intra-UE au titre du paragraphe 2 de cet article ou seulement pour certains de ces vols au titre du paragraphe 3 dudit article, n'est pas dispensé de vérifier que l'extension de l'application de cette directive à tout ou partie des vols intra-UE est effectivement nécessaire et proportionnée aux fins de la réalisation de l'objectif visé à l'article 1er, paragraphe 2, de ladite directive.

169. Ainsi, compte tenu des considérants 5 à 7, 10 et 22 de la directive PNR, un tel État membre doit vérifier que les traitements, prévus par cette directive, des données PNR des passagers empruntant des vols intra-UE ou certains de ces vols sont strictement nécessaires, au regard de la gravité de l'ingérence dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, pour assurer la sécurité intérieure de l'Union ou, à tout le moins, celle dudit État membre et, ainsi, pour protéger la vie et la sécurité des personnes.

170. S'agissant, en particulier, des menaces liées aux infractions terroristes, il ressort de la jurisprudence de la Cour que les activités de terrorisme sont au nombre de celles qui sont de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, et qu'il est de l'intérêt primordial de chaque État membre de prévenir et de réprimer ces activités pour protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société, dans l'objectif de sauvegarder la sécurité nationale. De telles menaces se distinguent, par leur nature, leur particulière gravité et le caractère spécifique des circonstances qui les constituent, du risque général et permanent qu'est celui d'infractions pénales graves (voir, en ce sens, arrêts du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 135 et 136, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, points 61 et 62).

171. Ainsi, dans la situation où il est constaté, sur la base de l'évaluation réalisée par un État membre, qu'il existe des circonstances suffisamment concrètes pour considérer que ce dernier fait face à une menace terroriste qui s'avère réelle et actuelle ou prévisible, le fait pour cet État membre de prévoir l'application de la directive PNR, en vertu de l'article 2, paragraphe 1, de cette directive, à tous les vols intra-UE en provenance ou à destination dudit État membre, pour une durée limitée, n'apparaît pas excéder les limites du strict nécessaire. En effet, l'existence d'une telle menace est de nature, par elle-même, à établir une relation entre, d'une part, le transfert et le traitement des données concernées et, d'autre part, la lutte contre le terrorisme (voir, par analogie, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 137).

172. La décision prévoyant cette application doit pouvoir faire l'objet d'un contrôle effectif par une juridiction ou par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence de cette situation ainsi que le respect des conditions et des garanties devant être prévues. La période d'application doit également être temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace (voir, par analogie, arrêts du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 58).

173. En revanche, en l’absence d’une menace terroriste réelle et actuelle ou prévisible à laquelle fait face l’État membre concerné, l’application sans distinction par celui-ci du système établi par la directive PNR non seulement aux vols extra-UE mais également à l’ensemble des vols intra-UE ne saurait être considérée comme étant limitée au strict nécessaire.

174. Dans une telle situation, l’application du système établi par la directive PNR à certains vols intra-UE doit être limitée au transfert et au traitement des données PNR des vols relatifs notamment à certaines liaisons aériennes ou à des schémas de voyage ou encore à certains aéroports pour lesquels il existe des indications de nature à justifier cette application. Il appartient à l’État membre concerné, dans une telle situation, de sélectionner les vols intra-UE selon les résultats de l’appréciation à laquelle il doit procéder sur le fondement des exigences exposées aux points 163 à 169 du présent arrêt et de réexaminer régulièrement celle-ci en fonction de l’évolution des conditions ayant justifié leur sélection, aux fins d’assurer que l’application du système établi par ladite directive aux vols intra-UE est toujours limitée au strict nécessaire.

175. Il résulte des considérations qui précèdent que l’interprétation ainsi retenue de l’article 2 et de l’article 3, point 4, de la directive PNR, à la lumière des articles 7 et 8 ainsi que de l’article 52, paragraphe 1, de la Charte, est de nature à assurer que ces dispositions respectent les limites du strict nécessaire ».

B.38.1. En ce qui concerne la notion de « passager » visée par la directive PNR, la Cour de justice a jugé que, si les données des « passagers » sont transférées à l’UIP de l’État membre indépendamment de tout élément objectif permettant de considérer que les passagers concernés sont susceptibles de présenter un risque d’être impliqués dans des infractions terroristes ou des formes graves de criminalité, ces données sont soumises à des traitements automatisés ayant pour finalité, ainsi qu’il ressort du considérant 7 de cette directive, d’identifier des personnes qui n’étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité avant cette évaluation et qui devraient être soumises à un examen plus approfondi par les autorités compétentes (point 161).

Compte tenu de la nature même des menaces pour la sécurité publique pouvant résulter d’infractions terroristes et de formes graves de criminalité qui présentent un lien objectif, à tout le moins indirect, avec le transport aérien des passagers, la Cour de justice considère que « le transfert et l’évaluation préalable des données PNR des passagers aériens entrant ou sortant de l’Union ne peuvent être limités à un cercle déterminé de passagers aériens » : « il y a lieu de considérer que le rapport nécessaire entre ces données et l’objectif ayant trait à la lutte contre de telles infractions existe, de sorte que la directive PNR ne dépasse pas les limites du strict

nécessaire du seul fait qu'elle impose aux États membres le transfert et l'évaluation préalable systématiques des données PNR de l'ensemble de ces passagers » (point 162).

B.38.2. Comme la Cour de justice le souligne dans l'arrêt précité, la collecte des données de tous les passagers visés par l'article 4, 10°, de la loi du 25 décembre 2016 est soumise à un traitement automatisé ultérieur visant à identifier, parmi ces passagers, ceux qui devraient être soumis à un examen plus approfondi par les autorités compétentes, dans le cadre de l'objectif de lutte contre les infractions terroristes et les formes graves de criminalité.

Un tel système se distingue ainsi d'un système de conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits en ce qui concerne 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 (comp. avec CJUE, grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, points 103-112).

B.39.1. En ce qui concerne les vols concernés, la Cour de justice a jugé que les États membres qui décident d'étendre l'application du système établi par cette directive aux vols intra-UE n'exercent qu'une faculté prévue par l'article 2, paragraphe 1, de la directive PNR.

Le rapport de la Commission « sur le réexamen de la directive 2016/681 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 », cité en B.36.4.1, établit par ailleurs que tous les États membres, à l'exception d'un seul, ont étendu le système de collecte des données PNR aux vols intra-UE.

B.39.2. Il ressort par ailleurs de l'arrêt de la Cour de justice, cité en B.37, que l'éventuelle extension du système de collecte des données PNR à tous les vols intra-UE qu'un État membre peut décider, en faisant usage de la faculté prévue par cette directive est subordonnée à la condition qu'il soit constaté, sur la base de l'évaluation réalisée par l'État membre, qu'il existe

des circonstances suffisamment concrètes pour considérer que l'État membre concerné fait face à une menace terroriste qui s'avère réelle et actuelle ou prévisible, l'existence d'une telle menace étant de nature, par elle-même, à établir une relation entre, d'une part, le transfert et le traitement des données concernées et, d'autre part, la lutte contre le terrorisme (point 171).

La décision prévoyant cette application doit par ailleurs pouvoir faire l'objet d'un contrôle effectif par une juridiction ou par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, et la période d'application doit également être temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace (point 172).

Enfin, si l'existence de cette menace n'est pas établie, il convient de limiter le système de collecte des données PNR à des vols relatifs, notamment, à certaines liaisons aériennes ou à des schémas de voyage, ou encore à certains aéroports pour lesquels il existe, selon l'appréciation de l'État membre concerné, des indications qui sont de nature à justifier cette application, et le caractère strictement nécessaire de cette application aux vols intra-UE ainsi sélectionnés doit régulièrement être réexaminé, en fonction de l'évolution des conditions ayant justifié leur sélection (point 174).

B.40.1. Comme l'indiquent ses travaux préparatoires, la loi du 25 décembre 2016, en transposant la directive PNR, tend à lutter contre la menace terroriste :

« Les attentats du 22 mars 2016 dans le hall des départs de l'aéroport national et à la station de métro Maelbeek, ceux du 13 novembre 2015 à Paris, les autres évènements dramatiques qui se sont déroulés à Bruxelles (Musée Juif, mai 2014), Paris (Charlie Hebdo, janvier 2015), Copenhague (Février 2015) et la menace à laquelle est confronté notre pays, en lien direc[t] avec la problématique des ' foreign fighter ' et des ' returnees ', nous rappellent plus que jamais qu'il est essentiel, pour les autorités qui souhaitent assurer la protection et la sécurité des citoyens, de ne pas seulement adopter une attitude réactive, mais également d'anticiper les risques liés aux déplacements criminels.

Cette anticipation est notamment possible grâce à l'analyse des fichiers contenant les données de voyage dans le cadre de la prévention et de la recherche d'infractions terroristes, des formes graves de criminalité, des atteintes à l'ordre public dans le cadre de la radicalisation violente et des activités pouvant menacer les intérêts fondamentaux de l'État » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 5).

B.40.2.1. La Belgique ayant été le siège des deux attentats terroristes évoqués dans les travaux préparatoires précités (Musée Juif en mai 2014, et station de métro Maelbeek et aéroport de Zaventem en mars 2016), le législateur a pu considérer, lorsqu'il a adopté la loi du 25 décembre 2016, que la menace terroriste était réelle et actuelle.

Il apparaît en outre que cette menace terroriste est toujours réelle et actuelle. Ainsi, l'Organe de coordination pour l'analyse de la menace (OCAM), institué par l'article 5 de la loi du 10 juillet 2006 « relative à l'analyse de la menace » (ci-après : la loi du 10 juillet 2006), faisait état, en 2022, de 215 signalements en lien avec le terrorisme et l'extrémisme, et le niveau général de la menace en Belgique est actuellement de 2 sur 4, soit une menace moyenne.

B.40.2.2. Il convient par ailleurs de tenir compte, pour évaluer la réalité de cette menace, de la situation géographique du pays, dont le territoire est restreint et les frontières aisément franchissables, sis au centre de l'Europe et siège de nombreuses institutions européennes et internationales. Cette réalité géographique, caractéristique, du pays augmente significativement les risques d'utilisation de tous les modes de transports via la Belgique pour la commission d'infractions terroristes ou relevant de la criminalité grave. Le pays se situe ainsi, géographiquement, à l'intersection de multiples voies de transports aériens, ferroviaires ou routiers pouvant être utilisés par des organisations terroristes et criminelles pour la commission d'infractions terroristes ou de formes graves de criminalité.

B.40.2.3. Il découle de ce qui précède que l'évaluation de la menace justifiant l'extension du système « PNR » à tous les vols intra-UE a fait l'objet d'un contrôle, en l'espèce juridictionnel, par la Cour, et que sa réalité et son actualité ont été constatées.

B.40.3.1. Comme le souligne la Cour de justice, la période d'application des mesures justifiées par l'évaluation de la menace doit être limitée au « strict nécessaire ».

À cet égard, il convient de rappeler que, parmi les missions de l'OCAM, figure celle « d'effectuer périodiquement une évaluation stratégique commune qui doit permettre d'apprécier si des menaces, visées à l'article 3, peuvent se manifester ou, si celles-ci ont déjà

été détectées, comment elles évoluent et, le cas échéant, quelles mesures s'avèrent nécessaires » (article 8, 1°, de la loi précitée du 10 juillet 2006), les menaces visées à l'article 3 étant « énumérées à l'article 8, 1°, *b)* et *c)*, de la loi organique des services de renseignement et de sécurité susceptibles de porter atteinte à la sûreté intérieure et extérieure de l'Etat, aux intérêts belges et à la sécurité des ressortissants belges à l'étranger ou à tout autre intérêt fondamental du pays tel que défini par le Roi sur la proposition du Conseil national de sécurité ». Il découle de ce qui précède qu'une évaluation périodique de la menace est organisée et est confiée à l'OCAM.

B.40.3.2. Pour le surplus, l'article 52, § 1er, de la loi du 25 décembre 2016 prévoit une évaluation de la loi trois ans après son entrée en vigueur.

Compte tenu de ce qui est dit en B.40.2.3 concernant la réalité et l'actualité de la menace, il appartiendra au législateur, sur la base de l'évaluation de la menace par l'OCAM, d'effectuer une évaluation périodique de la loi du 25 décembre 2016, une première évaluation devant avoir lieu au plus tard trois ans après la date du prononcé du présent arrêt.

B.40.3.3. À supposer que la réalité et l'actualité ou la prévisibilité de la menace ne soient plus établies, il appartient alors au législateur d'examiner la possibilité, au regard des objectifs poursuivis, de limiter le système de collecte des données PNR, de la manière indiquée par la Cour de justice au point 174 de son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité.

B.41. Compte tenu de ce qui est dit en B.40.3.2 et B.40.3.3, le moyen, en ce qu'il est dirigé contre l'article 4, 10°, de la loi du 25 décembre 2016, n'est pas fondé.

3. *Les finalités du traitement des données PNR (article 8)*

B.42. 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.43.1. 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 :

« 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.43.2. 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.43.3. 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.44.1. Dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, la Cour de justice a précisé, en ce qui concerne les finalités des traitements des données PNR :

« *2) Sur les finalités des traitements des données PNR*

141. Ainsi qu’il ressort de l’article 1er, paragraphe 2, de la directive PNR, les traitements des données PNR recueillies conformément à cette directive ont pour finalité la lutte contre les ‘ infractions terroristes ’ et les ‘ formes graves de criminalité ’.

142. S’agissant de la question de savoir si la directive PNR prévoit, en la matière, des règles claires et précises qui limitent l’application du système établi par cette directive à ce qui est strictement nécessaire à ces fins, il convient de relever, d’une part, que les termes ‘ infractions terroristes ’ sont définis à l’article 3, point 8, de ladite directive par référence aux ‘ infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre [2002/475] ’.

143. Or, outre le fait que cette décision-cadre définissait, à ses articles 1er à 3, de manière claire et précise, les ‘ infractions terroristes ’, les ‘ infractions liées à un groupe terroriste ’ et les ‘ infractions liées à des activités terroristes ’, que les États membres devaient rendre

punissables en tant qu'infractions pénales au titre de ladite décision-cadre, la directive (UE) 2017/541 du Parlement européen et du Conseil, du 15 mars 2017, relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475 et modifiant la décision 2005/671/JAI du Conseil (JO 2017, L 88, p. 6), définit également, à ses articles 3 à 14, de manière claire et précise, ces mêmes infractions.

144. D'autre part, l'article 3, point 9, de la directive PNR définit les termes ' formes graves de criminalité ' par référence aux ' infractions énumérées à l'annexe II [de cette directive] 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 '.

145. Or, tout d'abord, cette annexe énumère de manière exhaustive les différentes catégories d'infractions pouvant relever des ' formes graves de criminalité ' visées à l'article 3, point 9, de la directive PNR.

146. Ensuite, compte tenu des spécificités que présentaient, lors de l'adoption de ladite directive, les systèmes pénaux des États membres en l'absence d'une harmonisation des infractions ainsi visées, le législateur de l'Union pouvait se borner à viser des catégories d'infractions sans en définir les éléments constitutifs, et ce d'autant plus que ces éléments sont, par hypothèse, nécessairement définis par le droit national auquel renvoie l'article 3, point 9, de la directive PNR, en ce que les États membres sont tenus par le respect du principe de légalité des délits et des peines en tant que composante de la valeur commune, partagée avec l'Union, de l'État de droit visée à l'article 2 TUE (voir, par analogie, arrêt du 16 février 2022, Hongrie/Parlement et Conseil, C-156/21, EU:C:2022:97, points 136, 160 et 234), principe qui est par ailleurs consacré à l'article 49, paragraphe 1, de la Charte que les États membres sont tenus d'observer lorsqu'ils mettent en œuvre un acte de l'Union tel que la directive PNR (voir, en ce sens, arrêt du 10 novembre 2011, QB, C-405/10, EU:C:2011:722, point 48 et jurisprudence citée). Ainsi, eu égard également au sens habituel des termes employés dans cette même annexe, il y a lieu de considérer que celle-ci détermine, de manière suffisamment claire et précise, les infractions susceptibles de constituer des formes graves de criminalité.

147. Il est vrai que les points 7, 8, 10 et 16 de l'annexe II visent des catégories d'infractions très générales (fraude, blanchiment du produit du crime et faux monnayage, infractions graves contre l'environnement, trafic de biens culturels), tout en se référant néanmoins à des infractions particulières relevant de ces catégories générales. Afin d'assurer une précision suffisante également requise par l'article 49 de la Charte, ces points doivent être interprétés comme se référant auxdites infractions, telles que spécifiées par le droit national et/ou le droit de l'Union en la matière. Interprétés en ce sens, lesdits points peuvent être considérés comme répondant aux exigences de clarté et de précision.

148. Enfin, il importe encore de rappeler que, si, conformément au principe de proportionnalité, l'objectif de lutte contre la criminalité grave est de nature à justifier l'ingérence grave que comporte la directive PNR dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, il en va autrement de celui de lutte contre la criminalité en général, ce dernier objectif pouvant justifier uniquement des ingérences qui ne présentent pas un caractère grave (voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 59 et jurisprudence citée). Ainsi, cette directive doit assurer, par des règles claires et précises, que l'application du système établi par ladite

directive se limite aux seules infractions relevant de la criminalité grave et exclut, de ce fait, celles relevant de la criminalité ordinaire.

149. À cet égard, comme M. l'avocat général l'a relevé au point 121 de ses conclusions, bon nombre des infractions visées à l'annexe II de la directive PNR, telles que la traite des êtres humains, l'exploitation sexuelle des enfants et la pédopornographie, le trafic d'armes, de munitions et d'explosifs, le blanchiment, la cybercriminalité, le trafic d'organes et de tissus humains, le trafic de stupéfiants et de substances psychotropes, le trafic de matières nucléaires ou radioactives, le détournement d'avion ou de navire, les infractions graves relevant de la Cour pénale internationale, le meurtre, le viol, l'enlèvement, la séquestration et la prise d'otage, revêtent, par leur nature, un niveau de gravité incontestablement élevé.

150. En outre, si d'autres infractions, également visées à cette annexe II, peuvent, a priori, moins facilement être associées à des formes graves de criminalité, il ressort néanmoins des termes mêmes de l'article 3, point 9, de la directive PNR que ces infractions ne peuvent être considérées comme relevant des formes graves de criminalité que si elles 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 de l'État membre concerné. Les exigences résultant de cette disposition, qui ont trait à la nature et à la sévérité de la peine applicable, sont, en principe, à même de limiter l'application du système établi par ladite directive à des infractions présentant un niveau suffisant de gravité susceptible de justifier l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant du système établi par la même directive.

151. Toutefois, dans la mesure où l'article 3, point 9, de la directive PNR se réfère non pas à la peine minimale applicable, mais à la peine maximale applicable, il n'est pas exclu que des données PNR puissent faire l'objet d'un traitement à des fins de lutte contre des infractions qui, bien qu'elles remplissent le critère prévu par cette disposition relatif au seuil de gravité, relèvent, compte tenu des spécificités du système pénal national, non pas des formes graves de criminalité, mais de la criminalité ordinaire.

152. Il incombe donc aux États membres d'assurer que l'application du système établi par la directive PNR est effectivement limitée à la lutte contre des formes graves de criminalité et que ce système n'est pas étendu à des infractions qui relèvent de la criminalité ordinaire.

3) Sur le lien entre les données PNR et les finalités des traitements de ces données

153. Il est vrai que, comme M. l'avocat général l'a, en substance, relevé au point 119 de ses conclusions, les termes de l'article 3, point 8, et de l'article 3, point 9, de la directive PNR, lus en combinaison avec l'annexe II de celle-ci, ne font pas expressément référence à un critère de nature à circonscrire le champ d'application de cette directive aux seules infractions susceptibles, par leur nature, d'entretenir, à tout le moins indirectement, un lien objectif avec les voyages aériens et, par conséquent, avec les catégories de données transférées, traitées et conservées en application de ladite directive.

154. Cependant, comme M. l'avocat général l'a relevé au point 121 de ses conclusions, certaines infractions visées à l'annexe II de la directive PNR, telles que la traite des êtres humains, le trafic de stupéfiants ou d'armes, l'aide à l'entrée et au séjour irréguliers ou encore le détournement d'avion, sont, par leur nature même, susceptibles de présenter un lien direct avec le transport aérien de passagers. Il en va de même de certaines infractions terroristes, telles

que le fait de causer des destructions massives à un système de transport ou à une infrastructure ou de procéder à la capture d'aéronefs, infractions qui étaient visées à l'article 1er, paragraphe 1, sous *d)* et *e)*, de la décision-cadre 2002/475, auquel renvoie l'article 3, point 8, de la directive PNR, ou encore le fait d'entreprendre des voyages à des fins de terrorisme et d'organiser ou de faciliter de tels voyages, infractions visées aux articles 9 et 10 de la directive 2017/541.

155. Dans ce contexte, il y a lieu également de rappeler que la Commission a motivé sa proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, du 2 février 2011 [COM(2011) 32 final], à l'origine de la directive PNR, en mettant l'accent sur le fait que ' [l]es attentats perpétrés aux États-Unis en 2001, le projet d'attentat déjoué en août 2006 qui visait à faire exploser plusieurs avions en vol entre le Royaume-Uni et les États-Unis et la tentative d'attentat à bord du vol Amsterdam-Détroit en décembre 2009 ont prouvé que les terroristes sont capables de monter des attaques ciblant des vols internationaux dans tous les pays ' et que ' la plupart des activités terroristes sont de nature transnationale et impliquent des déplacements internationaux, entre autres vers des camps d'entraînement situés en dehors de l'Union '. En outre, pour justifier la nécessité d'une analyse des données PNR aux fins de la lutte contre des formes graves de criminalité, la Commission s'est référée, à titre d'exemples, au cas d'un groupe de passeurs qui, aux fins de la traite d'êtres humains, avaient produit des documents falsifiés pour procéder aux formalités d'enregistrement sur un vol ainsi qu'au cas d'un réseau de traite d'êtres humains et de trafic de drogues qui, aux fins d'importer des drogues dans plusieurs régions d'Europe, faisait appel à des personnes elles-mêmes victimes de la traite, tout en ayant acheté les billets d'avion de ces personnes avec des cartes de crédit volées. Or, l'ensemble de ces cas concernaient des infractions présentant un lien direct avec le transport aérien de passagers en ce qu'il s'agissait d'infractions prenant pour cible le transport aérien des passagers ainsi que d'infractions commises à l'occasion ou à l'aide d'un voyage aérien.

156. En outre, il importe de constater que même des infractions qui ne présentent pas un tel lien direct avec le transport aérien de passagers peuvent, en fonction des circonstances de l'espèce, présenter un lien indirect avec le transport aérien des passagers. Il en va ainsi notamment lorsque le transport aérien sert de moyen pour préparer de telles infractions ou pour se soustraire aux poursuites pénales après leur commission. En revanche, les infractions dépourvues de tout lien objectif, même indirect, avec le transport aérien des passagers ne sauraient justifier l'application du système établi par la directive PNR.

157. Dans ces conditions, l'article 3, points 8 et 9, de cette directive, lu en combinaison avec l'annexe II de celle-ci et à la lumière des exigences résultant des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, exige des États membres qu'ils veillent, notamment lors du réexamen individuel par des moyens non automatisés prévu à l'article 6, paragraphe 5, de ladite directive, à ce que l'application du système établi par celle-ci soit limitée aux infractions terroristes et aux seules formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers ».

B.44.2. Il ressort de ce qui précède que, pour être compatible avec les exigences découlant notamment des articles 7 et 8, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux, les finalités de collecte et de traitement des données PNR doivent être

strictement limitées à des fins de prévention et de détection – ainsi que d'enquêtes et de poursuites – des infractions terroristes et des seules formes graves de criminalité, en référence aux catégories d'infractions énumérées de manière exhaustive dans l'annexe II de la directive PNR, et présentant un lien objectif, à tout le moins indirect, avec le transport concerné, ce système ne pouvant pas être étendu à des infractions qui relèvent de la criminalité ordinaire. En ce qui concerne ces formes graves de criminalité, l'application du système « PNR » ne peut être étendue à des infractions qui, même si elles remplissent le critère prévu par cette directive relatif au seuil de gravité et même si elles sont notamment visées à l'annexe II de celle-ci, relèvent de la criminalité ordinaire, compte tenu des spécificités du système pénal national (points 151-152).

B.45.1. L'article 8 de la loi du 25 décembre 2016 définit les finalités des traitements des données PNR.

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 ».

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.45.2.1. Comme il est dit en B.11, 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.45.2.2. 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).

B.45.2.3. 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 ».

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

B.45.3. 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.

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.

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

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 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, pp. 17-20).

B.45.4. 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.10, 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.10.2, 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 1er de la loi du 30 juillet 2018.

B.46.1. Il ressort de ce qui est dit en B.45 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°), et concernent des formes graves d’infractions selon le droit national.

Comme il est dit en B.31.1, 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.

Comme la Cour de justice l’a jugé dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres*, cité en B.44, l’application du système « PNR » à de telles finalités, strictement limitées à la prévention et à la détection des infractions terroristes et des formes graves de criminalité, ainsi que d’enquêtes et de poursuites en la matière, est compatible avec les exigences du « strict nécessaire ».

B.46.2. 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.25.

B.47.1. 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.47.2. Il convient d'examiner si ces autres finalités sont exprimées en des règles claires, précises et limitées au strict nécessaire, conformément aux exigences mentionnées en B.25, et en tenant compte de l'arrêt de la Cour de justice, rappelé en B.44.

B.48. En ce qui concerne la finalité de « 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°), la Cour, par son arrêt n° 135/2019, a jugé :

« 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 ’.

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).

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.

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 ’.

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.49.1. Comme la Cour l’a jugé par son arrêt n° 135/2019 précité, la finalité de prévention des « troubles graves » à la sécurité publique dans le cadre de la « radicalisation violente » est une notion qui vise un phénomène de groupe mettant la sécurité publique gravement en danger, et qui est en lien direct avec des infractions 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.

Il en découle que la prévention des « troubles graves » à la sécurité publique dans le cadre de la « radicalisation violente » qui ne serait liée qu’à la commission d’infractions de droit commun ne relève pas de la finalité visée à l’article 8, § 1er, 3°, de la loi du 25 décembre 2016.

Le traitement et la collecte des données PNR pour cette finalité ainsi comprise relèvent dès lors des objectifs poursuivis par la directive PNR, ainsi qu’ils ont été rappelés par la Cour de justice dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité. En outre, comme il est dit en B.53.4 de l’arrêt n° 135/2019 précité, le traitement des données PNR est, pour cette finalité, 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.

B.49.2. Comme la Cour de justice l’a indiqué par son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, rappelé en B.44, les finalités de traitement des données PNR doivent par ailleurs présenter un lien objectif, à tout le moins indirect, avec le transport concerné.

Il en découle que la prévention des « troubles graves » à la sécurité publique dans le cadre de la « radicalisation violente » qui ne nécessiterait pas l’utilisation de moyens de transport ne

peut relever du champ d'application de la finalité visée à l'article 8, § 1er, 3°, de la loi du 25 décembre 2016.

B.49.3. Sous réserve que la finalité de prévention des « troubles graves » à la sécurité publique dans le cadre de la « radicalisation violente » soit interprétée comme strictement limitée à des fins de prévention et de détection des seules infractions terroristes et des seules formes graves de criminalité, en référence aux catégories d'infractions énumérées de manière exhaustive dans l'annexe II de la directive PNR, à l'exclusion des infractions de droit commun, et présentant un lien objectif, à tout le moins indirect, avec le transport concerné, l'article 8, § 1er, 3°, de la loi du 25 décembre 2016 ne dépasse pas les limites du « strict nécessaire ».

B.50.1. 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 :

« 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 ».

B.50.2. 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.51.1. Interrogée par la Cour au sujet de la finalité de suivi d'activités par les services de renseignement et de sécurité, la Cour de justice a répondu, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité :

« 229. Par sa cinquième question, la juridiction de renvoi vise à savoir si l'article 6 de la directive PNR, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale qui autorise le traitement des données PNR recueillies conformément à cette directive aux fins du suivi d'activités par les services de renseignement et de sécurité.

230. Il ressort de la demande de décision préjudicielle que, par cette question, la juridiction de renvoi vise plus particulièrement les activités visées par la Sûreté de l'État (Belgique) et le Service général du renseignement et de la sécurité (Belgique), dans le cadre de leurs missions respectives relatives à la protection de la sécurité nationale.

231. À cet égard, afin de respecter les principes de légalité et de proportionnalité visés notamment à l'article 52, paragraphe 1, de la Charte, le législateur de l'Union a prévu des règles claires et précises régissant les finalités des mesures prévues par la directive PNR qui comportent des ingérences dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte.

232. En effet, l'article 1er, paragraphe 2, de la directive PNR énonce de façon expresse que les données PNR recueillies conformément à cette 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, [sous] *a), b)* et *c)* [de ladite directive] '. Cette dernière disposition confirme le principe énoncé à cet article 1er, paragraphe 2, en se référant de manière systématique aux notions d'' infraction terroriste' et de 'forme grave de criminalité '.

233. Il ressort ainsi clairement du libellé de ces dispositions que l'énumération qui y figure des objectifs poursuivis par le traitement des données PNR au titre de la directive PNR revêt un caractère exhaustif.

234. Cette interprétation est corroborée, notamment, par le considérant 11 de la directive PNR, selon lequel le traitement des données PNR doit être proportionné aux ' objectifs de sécurité spécifiques ' poursuivis par cette directive, et par son article 7, paragraphe 4, selon lequel les données PNR et le résultat du traitement de ces données reçus par l'UIP ne peuvent faire l'objet d'un traitement ultérieur ' qu'aux seules fins spécifiques de la prévention ou de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes ou des poursuites en la matière '.

235. Par ailleurs, le caractère exhaustif des finalités visées à l'article 1er, paragraphe 2, de la directive PNR implique également que les données PNR ne sauraient être conservées dans une base de données unique pouvant être consultée aux fins de la poursuite tant de ces finalités que d'autres finalités. En effet, la conservation de ces données dans une telle base de données comporterait le risque que lesdites données soient utilisées à des fins autres que celles visées à cet article 1er, paragraphe 2.

236. En l'occurrence, dans la mesure où, selon la juridiction de renvoi, la législation nationale en cause au principal 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, cette législation est susceptible de méconnaître le caractère exhaustif de l'énumération des objectifs poursuivis par le traitement des données PNR au titre de la directive PNR, ce qu'il incombe à la juridiction de renvoi de vérifier.

237. Partant, il convient de répondre à la cinquième question que l'article 6 de la directive PNR, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale qui autorise le traitement de données PNR recueillies conformément à cette directive à des fins autres que celles expressément visées à l'article 1er, paragraphe 2, de ladite directive ».

B.51.2. Il découle de ce qui précède que, compte tenu du caractère exhaustif des finalités visées à l'article 1er, paragraphe 2, de la directive PNR, la Cour de justice considère qu'en visant, comme une 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, une législation telle que la loi du 25 décembre 2016 est

susceptible de méconnaître le caractère exhaustif de l'énumération des objectifs du traitement des données PNR au titre de la directive PNR, ce qu'il incombe à la Cour de vérifier (point 236).

La Cour de justice souligne également que « le caractère exhaustif des finalités visées à l'article 1er, paragraphe 2, de la directive PNR implique également que les données PNR ne sauraient être conservées dans une base de données unique pouvant être consultée aux fins de la poursuite tant de ces finalités que d'autres finalités. En effet, la conservation de ces données dans une telle base de données comporterait le risque que lesdites données soient utilisées à des fins autres que celles visées à cet article 1er, paragraphe 2 » (point 235).

B.52.1. Comme la Cour l'a jugé par son arrêt n° 135/2019 précité, si les missions des services de renseignement et de sécurité, rappelées en B.50, 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 (B.54.3). On ne peut en effet considérer que les activités visées par les services de renseignement et de sécurité visent uniquement et toujours à prévenir des infractions terroristes ou des formes graves de criminalité. Contrairement à ce qu'avance le Conseil des ministres dans son mémoire complémentaire, le caractère « hybride » que présentent les infractions terroristes et les formes graves de criminalité ne permet pas de considérer que la finalité de suivi des activités visées à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016 respecte les limites du « strict nécessaire ».

La Cour constate dès lors que le « suivi des activités visées par les services de renseignement et de sécurité » ne permet pas d'établir un lien direct entre cette finalité et la prévention ou de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que les enquêtes ou des poursuites en la matière, qui sont les objectifs du traitement des données PNR au titre de la directive PNR.

En outre, cette finalité ne peut être considérée comme présentant un lien objectif, à tout le moins indirect, avec le transport de passagers, que doivent présenter les finalités de traitement des données PNR, comme la Cour de justice l'a indiqué par son arrêt, précité, en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, rappelé en B.44.

B.52.2. Compte tenu du caractère exhaustif des finalités visées à l'article 1er, paragraphe 2, de la directive PNR, il y a lieu de considérer que la finalité visée à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016 dépasse les limites du « strict nécessaire ».

B.53.1. En ce qui concerne la finalité d'amélioration des contrôles de personnes aux frontières extérieures, et plus précisément de lutte contre l'immigration illégale, visée à l'article 8, § 2, de la loi du 25 décembre 2016, la Cour, par son arrêt n° 135/2019, a jugé :

« 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.

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°).

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 ».

B.53.2. Par cet arrêt, la Cour a jugé que la finalité visée à l'article 8, § 2, de la loi attaquée était limitée au strict nécessaire, en se fondant, d'une part, sur le fait que les données visées étaient limitées aux données API et, d'autre part, sur le fait que le traitement de ces données était encadré par les différentes garanties prévues par les articles 28 à 31 de la loi du 25 décembre 2016.

La Cour n'a pas interrogé la Cour de justice sur la question de savoir si la directive PNR devait être interprétée comme s'opposant à une législation nationale telle que la loi attaquée,

qui admet, comme finalité du traitement des données PNR, la finalité d'amélioration des contrôles de personnes aux frontières extérieures, et plus précisément de lutte contre l'immigration illégale.

La Cour s'est dès lors définitivement prononcée sur la compatibilité, avec les dispositions visées au premier moyen, de la finalité visée à l'article 8, § 2, de la loi attaquée.

Les griefs dirigés contre les articles 28 à 31, combinés avec l'article 8, § 2, de la loi du 25 décembre 2016, sont examinés dans le cadre du second moyen.

B.54.1. Interrogée par la Cour au sujet de l'interprétation de la directive API (neuvième question, *sub b)*, la Cour de justice a jugé, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité :

« 287. Par ailleurs, ainsi qu'il ressort des indications figurant dans la demande de décision préjudicielle, la législation nationale en cause au principal transpose, dans un seul acte, la directive PNR, la directive API et, partiellement, la directive 2010/65. À cet effet, elle prévoit l'application du système prévu par la directive PNR à l'ensemble des vols intra-UE et des transports ferroviaires, terrestres, voire maritimes, effectués à l'intérieur de l'Union en provenance de, à destination de et transitant par la Belgique et s'applique également aux opérateurs de voyage, tout en poursuivant également d'autres objectifs que la seule lutte contre les infractions terroristes et les formes graves de criminalité. Selon ces mêmes indications, il semble que toutes les données recueillies dans le cadre du système établi par cette législation nationale soient conservées par l'UIP dans une base de données unique englobant les données PNR, y compris les données visées à l'article 3, paragraphe 2, de la directive API, pour l'ensemble des passagers des transports visés par ladite législation.

288. À cet égard, dans la mesure où la juridiction de renvoi s'est référée à l'objectif d'améliorer les contrôles aux frontières et de lutter contre l'immigration clandestine dans sa neuvième question, sous *b)*, objectif qui est celui de la directive API, il convient de rappeler que, ainsi qu'il résulte des points 233, 234 et 237 du présent arrêt, l'énumération des objectifs poursuivis par le traitement des données PNR au titre de la directive PNR revêt un caractère exhaustif, si bien qu'une législation nationale autorisant le traitement de données PNR recueillies conformément à cette directive, à des fins autres que celles prévues par celle-ci, à savoir, notamment, aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine, est contraire à l'article 6 de ladite directive, lu à la lumière de la Charte.

289. En outre, comme il ressort du point 235 du présent arrêt, les États membres ne sauraient créer une base de données unique contenant tant les données PNR recueillies au titre de la directive PNR et afférentes aux vols extra-UE et intra-UE que des données des passagers d'autres moyens de transport ainsi que les données visées à l'article 3, paragraphe 2, de la directive API, notamment lorsque cette base de données peut être consultée aux fins de la

poursuite non seulement des finalités visées à l'article 1er, paragraphe 2, de la directive PNR, mais également d'autres finalités.

290. Enfin et en tout état de cause, comme l'a relevé M. l'avocat général au point 281 de ses conclusions, les articles 28 à 31 de la loi du 25 décembre 2016 ne sauraient être compatibles avec le droit de l'Union, notamment avec l'article 67, paragraphe 2, TFUE, qu'à la condition qu'ils soient interprétés et appliqués comme visant uniquement le transfert et le traitement des données API des passagers qui franchissent les frontières extérieures de la Belgique avec des pays tiers. En effet, une mesure par laquelle un État membre étendrait les dispositions de la directive API, aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine, aux vols intra-UE et, a fortiori, à d'autres modes de transport acheminant des passagers dans l'Union en provenance et au départ de cet État membre ou encore transitant par ledit État membre, notamment l'obligation de transmission des données des passagers prévue à l'article 3, paragraphe 1, de cette directive, reviendrait à permettre aux autorités compétentes, lors du franchissement des frontières intérieures dudit État membre, de s'assurer de manière systématique que ces passagers peuvent être autorisés à entrer sur son territoire ou à le quitter et aurait ainsi un effet équivalent aux contrôles effectués aux frontières extérieures avec des pays tiers.

291. Eu égard à l'ensemble de ces considérations, il convient de répondre à la neuvième question, sous *b)*, que le droit de l'Union, en particulier l'article 2 de la directive PNR, lu à la lumière de l'article 3, paragraphe 2, TUE, de l'article 67, paragraphe 2, TFUE et de l'article 45 de la Charte, doit être interprété en ce sens qu'il s'oppose :

- à une législation nationale qui prévoit, en l'absence de menace terroriste réelle et actuelle ou prévisible à laquelle fait face l'État membre concerné, un système de transfert, par les transporteurs aériens et les opérateurs de voyage, ainsi que de traitement, par les autorités compétentes, des données PNR de l'ensemble des vols intra-UE et des transports effectués par d'autres moyens à l'intérieur de l'Union, en provenance ou à destination de cet État membre ou bien encore transitant par celui-ci, aux fins de la lutte contre les infractions terroristes et les formes graves de criminalité. Dans une telle situation, l'application du système établi par la directive PNR doit être limitée au transfert et au traitement des données PNR des vols et/ou des transports relatifs notamment à certaines liaisons ou à des schémas de voyage ou encore à certains aéroports, gares ou ports maritimes pour lesquels il existe des indications de nature à justifier cette application. Il appartient à l'État membre concerné de sélectionner les vols intra-UE et/ou les transports effectués par d'autres moyens à l'intérieur de l'Union pour lesquels de telles indications existent et de réexaminer régulièrement ladite application en fonction de l'évolution des conditions ayant justifié leur sélection, aux fins d'assurer que l'application de ce système à ces vols et/ou à ces transports est toujours limitée au strict nécessaire, et

- à une législation nationale prévoyant un tel système de transfert et de traitement desdites données aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine ».

B.54.2. Il ressort de cet arrêt que, d'une part, le traitement des données PNR à des fins autres que celles prévues par la directive PNR, notamment, aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine, méconnaît le caractère exhaustif de l'énumération des objectifs du traitement des données PNR (point 288), lequel

empêche les États membres de créer une base de données unique contenant tant les données PNR recueillies au titre de la directive PNR que les données visées à l'article 3, paragraphe 2, de la directive API, notamment lorsque cette base de données peut être consultée aux fins de la poursuite non seulement des finalités visées à l'article 1er, paragraphe 2, de la directive PNR, mais également d'autres finalités (point 289) et, d'autre part, le traitement des données API ne peut concerner que des passagers qui franchissent les frontières extérieures de l'Union avec des pays tiers, sous peine d'avoir un effet équivalent aux contrôles effectués aux frontières extérieures avec des pays tiers (point 290).

B.55.1. À la différence de ce que la Cour a jugé par son arrêt n° 135/2019, l'arrêt de la Cour de justice semble impliquer que la finalité d'amélioration des contrôles aux frontières et de lutte contre l'immigration clandestine ne peut pas être poursuivie au moyen du traitement des données PNR, même si ces dernières sont limitées aux données API et même si le traitement de ces données est encadré par les garanties prévues par les articles 28 à 31 de la loi du 25 décembre 2016, lorsque ces données sont recueillies dans une base de données unique au titre de la directive PNR et qu'elles concernent des passagers qui ne franchissent pas les frontières extérieures de l'Union.

B.55.2. Or, l'arrêt n° 135/2019 de la Cour est définitif et sans recours sur ce point (art. 116 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle). Par cet arrêt, la Cour a épuisé sa saisine en ce qui concerne le point mentionné. La Cour ne peut revenir sur ses décisions définitives, étant donné qu'« aucune circonstance ne peut [le] justifier » (voy. notamment l'arrêt n° 172/2008 du 3 décembre 2008, ECLI:BE:GHCC:2008:ARR.172, B.15). Il s'agit en effet d'« un des principes essentiels de l'État de droit » (arrêt n° 199/2009 du 17 décembre 2009, ECLI:BE:GHCC:2009:ARR.199, B.8). Le droit de l'Union n'impose pas davantage de revenir sur une décision juridictionnelle définitive, même si cela permettait de remédier à une violation d'une disposition du droit de l'Union (CJUE, grande chambre, 6 octobre 2015, C-69/14 *Târşia*, ECLI:EU:C:2015:662, points 28-29; 4 mars 2020, C-34-19, *Telecom Italia*, ECLI:EU:C:2020:148, point 69). La Cour ne pourrait trancher cette question juridique dans un sens différent sans en être à nouveau saisie. Il appartient donc au législateur d'harmoniser sur le point litigieux la loi attaquée avec l'arrêt de la Cour de justice.

B.56. En ce qu'il est dirigé contre l'article 8, § 1er, 3°, et § 2, de la loi du 25 décembre 2016, le moyen n'est pas fondé, sous réserve de l'interprétation mentionnée en B.49.

En ce qu'il est dirigé contre l'article 8, § 1er, 4°, de la loi du 25 décembre 2016, le moyen est fondé. Par conséquent, il y a lieu d'annuler l'article 8, § 1er, 4°, de la loi du 25 décembre 2016.

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

B.57. 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 peuvent se prononcer sur une requête d'accès individuelle dans le cadre de recherches ponctuelles.

B.58.1. 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.58.2. 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.

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 ».

B.59.1. Interrogée par la Cour au sujet de la validité de la directive PNR, la Cour de justice a, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, apporté plusieurs précisions concernant l'évaluation préalable des données PNR au moyen de traitements automatisés (points 176-213) – en prenant en considération (i) la confrontation des données PNR aux bases de données, (ii) le traitement des données PNR au regard de critères préétablis et (iii) les garanties entourant le traitement automatisé des données PNR – et la communication et l'évaluation ultérieures des données PNR (points 214-227) :

« *5) Sur l’évaluation préalable des données PNR au moyen de traitements automatisés*

176. Aux termes de l’article 6, paragraphe 2, sous *a)*, de la directive PNR, l’évaluation préalable qu’il prévoit a pour objectif d’identifier les personnes pour lesquelles est requis un examen plus approfondi notamment par les autorités compétentes visées à l’article 7 de cette directive, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

177. Cette évaluation préalable se déroule en deux temps. Dans un premier temps, l’UIP de l’État membre concerné procède, conformément à l’article 6, paragraphe 3, de la directive PNR, à des traitements automatisés des données PNR en les confrontant à des bases de données ou au regard de critères préétablis. Dans un second temps, dans l’hypothèse où ces traitements automatisés conduisent à une concordance positive (*hit*), ladite unité effectue, en vertu de l’article 6, paragraphe 5, de cette directive, un réexamen individuel par des moyens non automatisés, afin de vérifier si les autorités compétentes visées à l’article 7 de ladite directive doivent prendre des mesures en vertu du droit national *(match).*

178. Or, ainsi qu’il a été rappelé au point 106 du présent arrêt, des traitements automatisés présentent nécessairement un taux d’erreur assez conséquent, dans la mesure où ils sont effectués à partir de données à caractère personnel non vérifiées et se fondent sur des critères préétablis.

179. Dans ces conditions, et compte tenu de la nécessité, soulignée par le quatrième considérant du préambule de la Charte, de renforcer la protection des droits fondamentaux à la lumière notamment des développements scientifiques et technologiques, il doit être assuré, ainsi que l’énoncent le considérant 20 et l’article 7, paragraphe 6, de la directive PNR, qu’aucune décision produisant des effets juridiques préjudiciables à une personne ou l’affectant de manière significative ne saurait être prise par les autorités compétentes sur la seule base du traitement automatisé des données PNR. De plus, conformément à l’article 6, paragraphe 6, de cette directive, l’UIP elle-même ne peut transférer les données PNR à ces autorités qu’après avoir effectué un réexamen individuel par des moyens non automatisés. Enfin, en sus de ces vérifications qu’il appartient à l’UIP et aux autorités compétentes d’effectuer elles-mêmes, la licéité de l’ensemble des traitements automatisés doit pouvoir faire l’objet d’un contrôle par le délégué à la protection des données et l’autorité nationale de contrôle, en vertu respectivement de l’article 6, paragraphe 7, et de l’article 15, paragraphe 3, sous *b)*, de ladite directive, ainsi que par les juridictions nationales dans le cadre du recours juridictionnel visé à l’article 13, paragraphe 1, de la même directive.

180. Or, ainsi que M. l’avocat général l’a, en substance, relevé au point 207 de ses conclusions, l’autorité nationale de contrôle, le délégué à la protection des données et l’UIP doivent être dotés des moyens matériels et personnels nécessaires aux fins d’exercer le contrôle leur incombant en vertu de la directive PNR. En outre, il importe que la réglementation nationale transposant cette directive dans le droit interne et autorisant les traitements automatisés que celle-ci prévoit fixe des règles claires et précises encadrant la détermination des bases de données ainsi que des critères d’analyse utilisés, sans pouvoir recourir, aux fins de l’évaluation préalable, à d’autres méthodes non prévues expressément à l’article 6, paragraphe 2, de cette directive.

181. Par ailleurs, il découle de l’article 6, paragraphe 9, de la directive PNR que les conséquences de l’évaluation préalable au titre de l’article 6, paragraphe 2, sous *a)*, de celle-ci

ne compromettent pas le droit d'entrée des personnes jouissant du droit à la libre circulation sur le territoire de l'État membre concerné prévu par la directive 2004/38 et doivent, par ailleurs, respecter le règlement n° 562/2006. Ainsi, le système établi par la directive PNR ne permet pas aux autorités compétentes de limiter ce droit au-delà de ce qui est prévu par la directive 2004/38 et le règlement n° 562/2006.

i) *Sur la confrontation des données PNR aux bases de données*

182. Selon l'article 6, paragraphe 3, sous *a)*, de la directive PNR, l'UIP ' peut ', lorsqu'elle réalise l'évaluation visée à l'article 6, paragraphe 2, sous *a)*, de cette directive, 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 '.

183. S'il découle du libellé même de cet article 6, paragraphe 3, sous *a)*, de la directive PNR, en particulier des termes ' y compris ', que les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement figurent au nombre des ' bases de données utiles ' visées par cette disposition, celle-ci ne précise en revanche pas quelles autres bases de données pourraient également être considérées comme étant ' utiles ' au regard des objectifs poursuivis par cette directive. En effet, et ainsi que M. l'avocat général l'a relevé au point 217 de ses conclusions, ladite disposition ne précise pas expressément la nature des données pouvant être contenues dans de telles bases et leur rapport avec ces objectifs, ni n'indique si les données PNR doivent être confrontées exclusivement aux bases de données gérées par des autorités publiques ou si elles peuvent également l'être à des bases de données gérées par des personnes privées.

184. Dans ces conditions, l'article 6, paragraphe 3, sous *a)*, de la directive PNR pourrait, à première vue, se prêter à une interprétation selon laquelle les données PNR peuvent être utilisées comme simples critères de recherche aux fins de réaliser des analyses à partir de bases de données diverses, y compris de bases de données que les agences de sécurité et de renseignement des États membres gèrent et exploitent dans la poursuite d'objectifs autres que ceux visés par cette directive, et que de telles analyses peuvent prendre la forme d'une exploration de données *(data mining)*. Or, la possibilité de conduire de telles analyses et de confronter les données PNR à de telles bases de données serait de nature à générer dans l'esprit des passagers du transport aérien le sentiment que leur vie privée fait l'objet d'une forme de surveillance. Ainsi, bien que l'évaluation préalable prévue à cette disposition parte d'un ensemble de données relativement limité que sont les données PNR, une telle interprétation de cet article 6, paragraphe 3, sous *a)*, ne saurait être retenue, dès lors que celle-ci serait susceptible de donner lieu à une utilisation disproportionnée de ces données, fournissant les moyens d'établir le profil précis des personnes concernées pour la seule raison que celles-ci ont l'intention de voyager par avion.

185. Partant, conformément à la jurisprudence rappelée aux points 86 et 87 du présent arrêt, il y a lieu d'interpréter l'article 6, paragraphe 3, sous *a)*, de la directive PNR de manière à garantir le plein respect des droits fondamentaux consacrés aux articles 7 et 8 de la Charte.

186. À cet égard, il ressort des considérants 7 et 15 de la directive PNR que le traitement automatisé prévu à l'article 6, paragraphe 3, sous *a)*, de cette directive doit être limité à ce qui est strictement nécessaire aux fins de la lutte contre les infractions terroristes et les formes graves de criminalité, tout en assurant un niveau élevé de protection de ces droits fondamentaux.

187. En outre, ainsi que la Commission l'a, en substance, relevé en réponse à une question de la Cour, les termes de cette disposition, selon laquelle l'UIP ' peut ' confronter les données PNR aux bases de données qu'elle vise, permettent à l'UIP de choisir une modalité de traitement qui est limitée au strict nécessaire, en fonction de la situation concrète. Or, eu égard au respect nécessaire des exigences de clarté et de précision requis pour assurer la protection des droits fondamentaux consacrés aux articles 7 et 8 de la Charte, l'UIP est tenue de limiter le traitement automatisé prévu à l'article 6, paragraphe 3, sous *a)*, de la directive PNR aux seules bases de données que cette disposition permet d'identifier. À cet égard, si la référence, figurant à cette dernière disposition, aux ' bases de données utiles ' ne se prête pas à une interprétation précisant de manière suffisamment claire et précise les bases de données ainsi visées, il en va autrement de la référence aux ' 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 '.

188. Dès lors, comme M. l'avocat général l'a, en substance, relevé au point 219 de ses conclusions, l'article 6, paragraphe 3, sous *a)*, de la directive PNR doit, à la lumière de ces droits fondamentaux, être interprété en ce sens que ces dernières bases de données sont les seules bases de données auxquelles l'UIP peut confronter les données PNR.

189. S'agissant des exigences auxquelles doivent satisfaire ces bases de données, il convient de relever que, selon l'article 6, paragraphe 4, de la directive PNR, l'évaluation préalable menée au regard des critères préétablis doit, au titre de l'article 6, paragraphe 3, sous *b)*, de cette directive, être réalisée de façon non discriminatoire, ces critères doivent être ciblés, proportionnés et spécifiques et ils doivent être fixés et réexaminés à intervalles réguliers par les UIP en coopération avec les autorités compétentes visées à l'article 7 de ladite directive. Si, en faisant référence à l'article 6, paragraphe 3, sous *b)*, de cette même directive, les termes de cet article 6, paragraphe 4, visent uniquement le traitement des données PNR au regard de critères préétablis, cette dernière disposition doit être interprétée, à la lumière des articles 7, 8 et 21 de la Charte, en ce sens que les exigences qu'elle prescrit doivent s'appliquer *mutatis mutandis* à la confrontation de ces données aux bases de données visées au point précédent du présent arrêt, et ce d'autant plus que ces exigences correspondent, en substance, à celles retenues pour le recoupement des données PNR avec des bases de données par la jurisprudence issue de l'avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 172).

190. À cet égard, il convient de préciser que l'exigence ayant trait au caractère non discriminatoire desdites bases de données implique, notamment, que l'inscription dans les bases de données concernant les personnes recherchées ou faisant l'objet d'un signalement soit fondée sur des éléments objectifs et non discriminatoires, définis par les règles nationales, internationales et de l'Union applicables à de telles bases de données (voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 78).

191. En outre, pour répondre à l'exigence relative au caractère ciblé, proportionné et spécifique des critères préétablis, les bases de données visées au point 188 du présent arrêt

doivent être exploitées en rapport avec la lutte contre des infractions terroristes et des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers.

192. Par ailleurs, les bases de données utilisées au titre de l'article 6, paragraphe 3, sous *a)*, de la directive PNR doivent, eu égard aux considérations figurant aux points 183 et 184 du présent arrêt, être gérées par les autorités compétentes visées à l'article 7 de cette directive ou, s'agissant des bases de données de l'Union ainsi que des bases de données internationales, être exploitées par ces autorités dans le cadre de leur mission de lutte contre les infractions terroristes et les formes graves de criminalité. Or, tel est le cas des 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.

ii) *Sur le traitement des données PNR au regard de critères préétablis*

193. L'article 6, paragraphe 3, sous *b)*, de la directive PNR prévoit que l'UIP peut également traiter les données PNR au regard de critères préétablis. Il ressort de l'article 6, paragraphe 2, sous *a)*, de cette directive que l'évaluation préalable, et, partant, le traitement des données PNR au regard de critères préétablis, vise, en substance, à identifier les personnes qui peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

194. S'agissant des critères que l'UIP peut utiliser à cet effet, il convient de relever, tout d'abord, que, selon les termes mêmes de l'article 6, paragraphe 3, sous *b)*, de la directive PNR, ces critères doivent être ' préétablis '. Ainsi que M. l'avocat général l'a relevé au point 228 de ses conclusions, cette exigence s'oppose à l'utilisation de technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage *(machine learning)*, susceptibles de modifier, sans intervention et contrôle humains, le processus de l'évaluation et, en particulier, les critères d'évaluation sur lesquels se fonde le résultat de l'application de ce processus ainsi que la pondération de ces critères.

195. Il importe d'ajouter que le recours à de telles technologies risquerait de priver d'effet utile le réexamen individuel des concordances positives ainsi que le contrôle de licéité requis par les dispositions de la directive PNR. En effet, comme M. l'avocat général l'a relevé, en substance, au point 228 de ses conclusions, compte tenu de l'opacité caractérisant le fonctionnement des technologies d'intelligence artificielle, il peut s'avérer impossible de comprendre la raison pour laquelle un programme donné est parvenu à une concordance positive. Dans ces conditions, l'utilisation de telles technologies serait susceptible de priver les personnes concernées également de leur droit à un recours juridictionnel effectif consacré à l'article 47 de la Charte que la directive PNR vise, selon son considérant 28, à garantir à un niveau élevé, en particulier pour contester le caractère non discriminatoire des résultats obtenus.

196. En ce qui concerne, ensuite, les exigences résultant de l'article 6, paragraphe 4, de la directive PNR, cette disposition énonce, à sa première phrase, que l'évaluation préalable au regard de critères préétablis est réalisée de façon non discriminatoire et précise, à sa quatrième phrase, que ces 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.

197. Ainsi, les États membres ne sauraient retenir, en tant que critères préétablis, des critères reposant sur des caractéristiques visées au point précédent du présent arrêt et dont l'utilisation peut être de nature à donner lieu à des discriminations. À cet égard, il résulte des termes de l'article 6, paragraphe 4, quatrième phrase, de la directive PNR, selon lesquels les critères préétablis ne sont ' en aucun cas ' fondés sur ces caractéristiques, que cette disposition vise tant des discriminations directes que des discriminations indirectes. Cette interprétation est, par ailleurs, confirmée par l'article 21, paragraphe 1, de la Charte, à la lumière duquel ladite disposition doit être lue, qui interdit ' toute ' discrimination fondée sur lesdites caractéristiques. Dans ces conditions, les critères préétablis doivent être déterminés de manière à ce que, bien que formulés de manière neutre, leur application ne puisse être de nature à désavantager particulièrement les personnes possédant les caractéristiques protégées.

198. S'agissant des exigences ayant trait au caractère ciblé, proportionné et spécifique des critères préétablis, prévues à l'article 6, paragraphe 4, deuxième phrase, de la directive PNR, il découle de ces exigences que les critères utilisés aux fins de l'évaluation préalable doivent être déterminés de manière à cibler, spécifiquement, les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou à des formes graves de criminalité visées par cette directive. Cette lecture est corroborée par les termes mêmes de l'article 6, paragraphe 2, sous *a)*, de celle-ci, qui mettent l'accent sur le ' fait ' que les personnes concernées ' peuvent ' être impliquées dans ' une ' infraction terroriste ou ' une ' forme grave de criminalité. Dans le même ordre d'idées, le considérant 7 de ladite directive précise que 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 '.

199. Afin de cibler de la sorte les personnes ainsi visées et compte tenu du risque de discrimination que comportent des critères reposant sur les caractéristiques mentionnées à l'article 6, paragraphe 4, quatrième phrase, de la directive PNR, l'UIP et les autorités compétentes ne sauraient, en principe, se fonder sur ces caractéristiques. En revanche, comme le gouvernement allemand l'a relevé lors de l'audience, elles peuvent notamment prendre en compte des particularités dans le comportement factuel de personnes en lien avec la préparation et la réalisation de voyages aériens, qui pourraient, selon les constatations opérées et l'expérience acquise par les autorités compétentes, indiquer que les personnes se comportant de la sorte peuvent être impliquées dans des infractions terroristes ou des formes graves de criminalité.

200. Dans ce contexte, ainsi que la Commission l'a fait remarquer en réponse à une question de la Cour, les critères préétablis doivent être déterminés de manière à tenir compte tant des éléments ' à charge ' que des éléments ' à décharge ', cette exigence étant susceptible de contribuer à la fiabilité de ces critères et, notamment, d'assurer qu'ils sont proportionnés, comme l'exige l'article 6, paragraphe 4, deuxième phrase, de la directive PNR.

201. Enfin, aux termes de l'article 6, paragraphe 4, troisième phrase, de cette directive, les critères préétablis doivent être réexaminés à intervalles réguliers. Dans le cadre de ce réexamen, ces critères doivent être actualisés en fonction de l'évolution des conditions ayant justifié leur prise en compte aux fins de l'évaluation préalable, permettant ainsi notamment de réagir aux évolutions de la lutte contre les infractions terroristes et les formes graves de criminalité visées au point 157 du présent arrêt [voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 82]. En particulier, ledit réexamen doit prendre en compte l'expérience acquise dans le cadre de l'application des critères préétablis,

aux fins de réduire, dans toute la mesure du possible, le nombre des résultats ‘ faux positifs ’ et, ce faisant, de contribuer au caractère strictement nécessaire de l’application de ces critères.

iii) *Sur les garanties entourant le traitement automatisé des données PNR*

202. Le respect des exigences auxquelles l’article 6, paragraphe 4, de la directive PNR soumet le traitement automatisé des données PNR s’impose non seulement dans le cadre de la détermination et du réexamen des bases de données ainsi que des critères préétablis prévus à cette disposition, mais également, comme M. l’avocat général l’a relevé au point 230 de ses conclusions, tout au long du processus de traitement de ces données.

203. S’agissant plus particulièrement des critères préétablis, il convient, tout d’abord, de préciser que, si l’UIP doit, comme l’énonce le considérant 7 de la directive PNR, définir les critères d’évaluation d’une manière qui réduise au minimum le nombre d’identifications erronées de personnes innocentes par le système établi par cette directive, cette même unité doit tout de même, conformément à l’article 6, paragraphes 5 et 6, de ladite directive, procéder à un réexamen individuel de toute concordance positive par des moyens non automatisés, aux fins de déceler, dans toute la mesure du possible, l’existence éventuelle de résultats ‘ faux positifs ’. En outre, nonobstant le fait qu’elle doive fixer les critères d’évaluation de manière non discriminatoire, l’UIP est tenue d’effectuer un tel réexamen aux fins d’exclure d’éventuels résultats discriminatoires. L’UIP doit respecter cette même obligation de réexamen à l’égard de la confrontation des données PNR aux bases de données.

204. Ainsi, l’UIP doit s’abstenir de transférer les résultats de ces traitements automatisés aux autorités compétentes visées à l’article 7 de la directive PNR lorsque, eu égard aux considérations figurant au point 198 du présent arrêt, elle ne dispose pas, à la suite de ce réexamen, d’éléments de nature à fonder, à suffisance de droit, un soupçon raisonnable de participation à des infractions terroristes ou à des formes graves de criminalité à l’égard des personnes identifiées au moyen de ces traitements automatisés ou lorsqu’elle dispose d’éléments indiquant que lesdits traitements conduisent à des résultats discriminatoires.

205. S’agissant des vérifications auxquelles l’UIP doit procéder à cet effet, il découle de l’article 6, paragraphes 5 et 6, de la directive PNR, lu en combinaison avec les considérants 20 et 22 de celle-ci, que les États membres doivent prévoir des règles claires et précises de nature à guider et à encadrer l’analyse effectuée par les agents en charge du réexamen individuel, aux fins d’assurer le plein respect des droits fondamentaux consacrés aux articles 7, 8 et 21 de la Charte et, notamment, de garantir une pratique administrative cohérente au sein de l’UIP respectant le principe de non-discrimination.

206. En particulier, compte tenu du nombre assez conséquent de résultats ‘ faux positifs ’, évoqué au point 106 du présent arrêt, les États membres doivent s’assurer que l’UIP établit, de manière claire et précise, des critères de réexamen objectifs permettant à ses agents de vérifier, d’une part, si et dans quelle mesure une concordance positive *(hit)* concerne effectivement un individu qui est susceptible d’être impliqué dans les infractions terroristes ou les formes graves de criminalité visées au point 157 du présent arrêt et doit, de ce fait, faire l’objet d’un examen plus approfondi par les autorités compétentes visées à l’article 7 de cette directive, ainsi que, d’autre part, le caractère non discriminatoire des traitements automatisés prévus par ladite directive et, notamment, des critères préétablis et des bases de données utilisées.

207. Dans ce contexte, les États membres sont tenus de veiller à ce que, conformément à l'article 13, paragraphe 5, de la directive PNR, lu en combinaison avec le considérant 37 de celle-ci, l'UIP garde une trace documentaire de tout traitement des données PNR effectué dans le cadre de l'évaluation préalable, y compris dans le cadre du réexamen individuel par des moyens non automatisés, aux fins de la vérification de sa licéité et d'un autocontrôle.

208. Ensuite, les autorités compétentes ne peuvent prendre, en vertu de l'article 7, paragraphe 6, première phrase, de la directive PNR, aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR, ce qui implique, dans le cadre de l'évaluation préalable, qu'elles doivent prendre en compte et, le cas échéant, faire prévaloir le résultat du réexamen individuel opéré par des moyens non automatisés par l'UIP sur celui obtenu par les traitements automatisés. La seconde phrase de cet article 7, paragraphe 6, précise que de telles décisions ne doivent pas être discriminatoires.

209. Dans ce cadre, les autorités compétentes doivent s'assurer du caractère licite tant de ces traitements automatisés, notamment de leur caractère non discriminatoire, que du réexamen individuel.

210. En particulier, les autorités compétentes doivent s'assurer que l'intéressé, sans lui permettre nécessairement, lors de la procédure administrative, de prendre connaissance des critères d'évaluation préétablis et des programmes appliquant ces critères, peut comprendre le fonctionnement de ces critères et de ces programmes, de manière à ce qu'il puisse décider, en pleine connaissance de cause, s'il exerce ou non son droit à un recours juridictionnel garanti à l'article 13, paragraphe 1, de la directive PNR, aux fins de mettre en cause, le cas échéant, le caractère illicite et, notamment, discriminatoire desdits critères (voir, par analogie, arrêt du 24 novembre 2020, Minister van Buitenlandse Zaken, C-225/19 et C-226/19, EU:C:2020:951, point 43 et jurisprudence citée). Il doit en aller de même des critères de réexamen visés au point 206 du présent arrêt.

211. Enfin, dans le cadre d'un recours introduit au titre de l'article 13, paragraphe 1, de la directive PNR, le juge chargé du contrôle de la légalité de la décision adoptée par les autorités compétentes ainsi que, hormis les cas de menaces pour la sûreté de l'État, l'intéressé lui-même doivent pouvoir prendre connaissance tant de l'ensemble des motifs que des éléments de preuve sur la base desquels cette décision a été prise (voir, par analogie, arrêt du 4 juin 2013, ZZ, C-300/11, EU:C:2013:363, points 54 à 59), y compris des critères d'évaluation préétablis et du fonctionnement des programmes appliquant ces critères.

212. Par ailleurs, en vertu respectivement de l'article 6, paragraphe 7, et de l'article 15, paragraphe 3, sous *b)*, de la directive PNR, il incombe au délégué à la protection des données et à l'autorité nationale de contrôle d'assurer le contrôle de la licéité des traitements automatisés effectués par l'UIP dans le cadre de l'évaluation préalable, contrôle qui s'étend notamment au caractère non discriminatoire de ces traitements. Si la première de ces dispositions précise, à cet effet, que le délégué à la protection des données a accès à toutes les données traitées par l'UIP, cet accès doit nécessairement s'étendre aux critères préétablis et aux bases de données utilisées par cette unité, aux fins d'assurer l'efficacité et le niveau élevé de la protection des données que doit assurer ce délégué conformément au considérant 37 de cette directive. De même, les enquêtes, les inspections et les audits que l'autorité nationale de contrôle effectue au titre de la seconde de ces dispositions peuvent également porter sur ces critères préétablis et ces bases de données.

213. Il résulte de l'ensemble des considérations qui précèdent que les dispositions de la directive PNR régissant l'évaluation préalable des données PNR au titre de l'article 6, paragraphe 2, sous *a)*, de cette directive se prêtent à une interprétation conforme aux articles 7, 8 et 21 de la Charte, respectant les limites du strict nécessaire.

6) Sur la communication et l'évaluation postérieures des données PNR

214. En vertu de l'article 6, paragraphe 2, sous *b)*, de la directive PNR, les données PNR peuvent également, sur demande des autorités compétentes, être communiquées à ces dernières et faire l'objet d'une évaluation postérieurement à l'arrivée prévue dans l'État membre ou au départ prévu de celui-ci.

215. S'agissant des conditions dans lesquelles une telle communication et une telle évaluation peuvent être effectuées, il ressort des termes de cette disposition que l'UIP peut traiter les données PNR aux fins de répondre ' au cas par cas ' aux ' demandes dûment motivées fondées sur des motifs suffisants ' des autorités compétentes, visant à ce que ces données leur soient communiquées et 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 '. En outre, lorsqu'une demande est introduite plus de six mois après le transfert des données PNR à l'UIP, période à l'expiration de laquelle toutes les données PNR sont dépersonnalisées par un masquage de certains éléments, conformément à l'article 12, paragraphe 2, de cette directive, l'article 12, paragraphe 3, de ladite directive dispose que la communication de l'intégralité des données PNR et, partant, d'une version non dépersonnalisée de celles-ci n'est autorisée qu'à la double condition que, d'une part, il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, sous *b)*, de ladite directive et, d'autre part, elle soit approuvée par une autorité judiciaire ou par une autre autorité nationale compétente en vertu du droit national.

216. À cet égard, il ressort, tout d'abord, des termes mêmes de l'article 6, paragraphe 2, sous *b)*, de la directive PNR que l'UIP ne peut procéder systématiquement à une communication et à une évaluation postérieures des données PNR de l'ensemble des passagers aériens et qu'elle peut seulement répondre ' au cas par cas ' à des demandes visant de tels traitements ' dans des cas spécifiques '. Cela étant, dans la mesure où cette disposition se réfère à des ' cas spécifiques ', ces traitements ne doivent pas nécessairement se limiter aux données PNR d'un seul passager aérien, mais ils peuvent, ainsi que la Commission l'a relevé en réponse à une question de la Cour, également porter sur une pluralité de personnes, pourvu que les personnes concernées partagent un certain nombre de caractéristiques permettant de les considérer comme constituant ensemble un 'cas spécifique' aux fins de la communication et de l'évaluation recherchées.

217. En ce qui concerne, ensuite, les conditions matérielles requises pour que les données PNR de passagers aériens puissent faire l'objet d'une communication et d'une évaluation postérieures, si l'article 6, paragraphe 2, sous *b)*, et l'article 12, paragraphe 3, sous *a)*, de la directive PNR se réfèrent respectivement à des ' motifs suffisants ' et à des ' motifs raisonnables ' sans préciser expressément la nature de ces motifs, il découle néanmoins des termes mêmes de la première de ces dispositions, qui se réfère aux finalités visées à l'article 1er, paragraphe 2, de ladite directive, que la communication des données PNR et

l'évaluation postérieures ne peuvent être effectuées qu'aux fins de vérifier l'existence d'indices quant à une possible implication des personnes concernées dans des infractions terroristes ou des formes graves de criminalité présentant, ainsi qu'il ressort du point 157 du présent arrêt, un lien objectif, à tout le moins indirect, avec le transport aérien des passagers.

218. Or, dans le cadre du système établi par la directive PNR, la communication et le traitement des données PNR en application de l'article 6, paragraphe 2, sous *b)*, de cette directive concernent des données de personnes qui ont déjà fait l'objet d'une évaluation préalable avant leur arrivée prévue dans l'État membre concerné ou leur départ prévu de celui-ci. En outre, une demande d'évaluation postérieure est susceptible de viser, notamment, les personnes dont les données PNR n'ont pas été transférées aux autorités compétentes à la suite de l'évaluation préalable, dans la mesure où celle-ci n'a pas révélé d'éléments indiquant que ces personnes pouvaient être impliquées dans des infractions terroristes ou des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers. Dans ces conditions, la communication et le traitement de ces données aux fins de leur évaluation postérieure doivent se fonder sur des circonstances nouvelles justifiant cette utilisation [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 200 et jurisprudence citée].

219. S'agissant de la nature des circonstances susceptibles de justifier la communication et le traitement des données PNR aux fins de leur évaluation postérieure, il est de jurisprudence constante que, dès lors qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme étant limité au strict nécessaire, la réglementation concernée, que ce soit la réglementation de l'Union ou une règle nationale visant à transposer cette dernière, doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités compétentes l'accès aux données en cause. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes peut également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités [arrêts du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 50 et jurisprudence citée, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 105].

220. Ainsi, les termes ' motifs suffisants ' et ' motifs raisonnables ', figurant respectivement à l'article 6, paragraphe 2, sous *b)*, et à l'article 12, paragraphe 3, sous *a)*, de la directive PNR, doivent être interprétés, à la lumière des articles 7 et 8 de la Charte, comme se référant à des éléments objectifs de nature à fonder un soupçon raisonnable d'implication de la personne concernée, d'une manière ou d'une autre, dans des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers, tandis que, s'agissant des infractions terroristes présentant un tel lien, cette exigence est satisfaite lorsqu'il existe des éléments objectifs permettant de considérer que les données PNR pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles infractions.

221. Enfin, s’agissant des conditions procédurales auxquelles sont soumis la communication et le traitement des données PNR aux fins de leur évaluation postérieure, l’article 12, paragraphe 3, sous *b)*, de la directive PNR exige, dans le cas où la demande est introduite plus de six mois après leur transfert à l’UIP, c’est-à-dire alors que, conformément au paragraphe 2 de cet article, lesdites données ont été dépersonnalisées par le masquage des éléments visés à ce paragraphe 2, que la communication de l’intégralité des données PNR, et, partant, d’une version non dépersonnalisée de celles-ci, soit approuvée par une autorité judiciaire ou par une autre autorité nationale compétente en vertu du droit national. Dans ce contexte, il appartient à ces autorités d’examiner intégralement le bien-fondé de la demande et, notamment, de vérifier si les éléments apportés au soutien de ladite demande sont de nature à étayer la condition matérielle tenant à l’existence de ‘ motifs raisonnables ’ visée au point précédent du présent arrêt.

222. Il est vrai que, dans le cas où la demande de communication et d’évaluation postérieures des données PNR est introduite avant l’expiration du délai de six mois suivant le transfert de ces données, l’article 6, paragraphe 2, sous *b)*, de la directive PNR ne prévoit pas expressément une telle condition procédurale. Toutefois, l’interprétation de cette dernière disposition doit prendre en compte le considérant 25 de cette directive, dont il ressort que, en prévoyant ladite condition procédurale, le législateur de l’Union a entendu ‘ garantir le niveau le plus élevé de protection des données ’ en ce qui concerne l’accès aux données PNR sous une forme permettant une identification directe de la personne concernée. Or, toute demande de communication et d’évaluation postérieures implique un tel accès à ces données, indépendamment du point de savoir si cette demande est introduite avant l’expiration de la période de six mois suivant le transfert des données PNR à l’UIP ou si elle l’est après l’expiration de cette période.

223. En particulier, afin de garantir, en pratique, le plein respect des droits fondamentaux dans le système mis en place par la directive PNR et, notamment, les conditions énoncées aux points 218 et 219 du présent arrêt, il est essentiel que la communication des données PNR aux fins d’une évaluation postérieure soit, en principe, sauf en cas d’urgence dûment justifiée, subordonnée à un contrôle préalable effectué soit par une juridiction soit par une autorité administrative indépendante et que la décision de cette juridiction ou de cette autorité intervienne à la suite d’une demande motivée des autorités compétentes, présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales. En cas d’urgence dûment justifiée, ledit contrôle doit intervenir dans de brefs délais [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 202 et jurisprudence citée, ainsi que arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 110].

224. Dans ces conditions, l’exigence d’un contrôle préalable prévu à l’article 12, paragraphe 3, sous *b)*, de la directive PNR, pour les demandes de communication des données PNR introduites après l’expiration du délai de six mois suivant le transfert de ces données à l’UIP, doit également s’appliquer, mutatis mutandis, dans le cas où la demande de communication est introduite avant l’expiration de ce délai.

225. Par ailleurs, si l’article 12, paragraphe 3, sous *b)*, de la directive PNR ne précise pas expressément les exigences auxquelles doit satisfaire l’autorité chargée du contrôle préalable, il est de jurisprudence constante que, afin d’assurer que l’ingérence dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte qui résulte d’un accès aux données à

caractère personnel soit limitée au strict nécessaire, cette autorité doit disposer de toutes les attributions et présenter toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et des droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette autorité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 107 ainsi que jurisprudence citée).

226. À cet effet, une telle autorité doit jouir d'un statut lui permettant d'agir lors de l'exercice de ses missions de manière objective et impartiale et doit être, de ce fait, à l'abri de toute influence extérieure. Cette exigence d'indépendance impose que celle-ci ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer son contrôle à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique que ladite autorité, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité à l'égard des parties à la procédure pénale (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 108 ainsi que jurisprudence citée).

227. Partant, les dispositions de la directive PNR régissant la communication et l'évaluation postérieures des données PNR au titre de l'article 6, paragraphe 2, sous *b)*, de cette directive se prêtent à une interprétation conforme aux articles 7 et 8 ainsi qu'à l'article 52, paragraphe 1, de la Charte, respectant les limites du strict nécessaire ».

B.59.2. Il ressort de cet arrêt que la Cour de justice apporte plusieurs précisions au sujet de l'interprétation des différents traitements des données PNR, afin que ceux-ci soient conformes aux articles 7 et 8, ainsi qu'à l'article 52, paragraphe 1, de la Charte, dans le respect des limites du « strict nécessaire ».

Tout d'abord, en ce qui concerne l'évaluation préalable des données PNR, qui a pour objectif d'identifier les personnes pour lesquelles est requis un examen plus approfondi avant leur arrivée ou leur départ et qui est, dans un premier temps, effectuée au moyen de traitements automatisés, l'UIP ne peut confronter ces données qu'aux seules bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement. Ces bases de données doivent être non discriminatoires et exploitées, par les autorités compétentes, en rapport avec la lutte contre des infractions terroristes et des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers (points 186-191).

En ce qui concerne ensuite les critères préétablis sur lesquels se fonde l'évaluation préalable, l'UIP ne saurait utiliser des technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (*machine learning*), susceptibles de modifier, sans intervention et contrôle humains, le processus d'évaluation et, en particulier, les critères d'évaluation sur lesquels se fonde le résultat de l'application de ce processus ainsi que la pondération de ces critères. Lesdits critères doivent être déterminés de manière à ce que leur application cible, spécifiquement, les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou à des formes graves de criminalité et à tenir compte tant des éléments « à charge » que des éléments « à décharge », tout en ne donnant pas lieu à des discriminations directes ou indirectes (points 194-200).

Afin de limiter le taux d'erreur par des « faux positifs », générés nécessairement par un traitement automatisé, il est essentiel que l'UIP effectue, dans un deuxième temps, un réexamen individuel par des moyens non automatisés, selon des règles claires et précises de nature à guider et à encadrer l'analyse effectuée par les agents de l'UIP en charge de ce réexamen individuel, aux fins de garantir une pratique administrative cohérente au sein de l'UIP respectant le principe de non-discrimination (points 178-180). En particulier, les États membres doivent s'assurer que l'UIP établit des critères de réexamen objectifs permettant à ses agents de vérifier, d'une part, si et dans quelle mesure une concordance positive (*hit*) concerne effectivement un individu qui est susceptible d'être impliqué dans les infractions terroristes ou les formes graves de criminalité, ainsi que, d'autre part, le caractère non discriminatoire des traitements automatisés (points 203-209). L'UIP doit garder une trace documentaire de tout traitement des données PNR effectué dans le cadre de l'évaluation préalable, y compris dans le cadre du réexamen individuel par des moyens non automatisés, aux fins de la vérification de sa licéité et d'un autocontrôle (point 207).

Les autorités compétentes doivent également s'assurer que l'intéressé puisse comprendre le fonctionnement des critères d'évaluation préétablis et des programmes appliquant ces critères, de manière à ce qu'il puisse décider, en pleine connaissance de cause, s'il exerce ou non son droit à un recours juridictionnel, dans le cadre duquel le juge chargé du contrôle de la légalité de la décision adoptée par les autorités compétentes ainsi que, hormis les cas de menaces pour la sûreté de l'État, l'intéressé lui-même doivent pouvoir prendre connaissance tant de l'ensemble des motifs que des éléments de preuve sur la base desquels cette décision a

été prise, y compris des critères d'évaluation préétablis et du fonctionnement des programmes appliquant ces critères (points 210-211).

En ce qui concerne enfin la communication et l'évaluation postérieures des données PNR, c'est-à-dire après l'arrivée ou le départ de la personne concernée, la Cour de justice considère qu'elles ne peuvent être effectuées que sur la base de circonstances nouvelles et d'éléments objectifs qui soit sont de nature à fonder un soupçon raisonnable d'implication de cette personne dans des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers, soit permettent de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre des infractions terroristes présentant un tel lien (points 217-220). La communication des données PNR aux fins d'une telle évaluation postérieure doit, en principe, sauf en cas d'urgence dûment justifiée, être subordonnée à un contrôle préalable effectué soit par une juridiction soit par une autorité administrative indépendante, sur demande motivée des autorités compétentes, et ce, indépendamment du point de savoir si cette demande a été introduite avant ou après l'expiration du délai de six mois suivant le transfert de ces données à l'UIP (points 221-226).

B.59.3. Il ressort de ce qui précède que la compatibilité de la directive PNR avec les articles 7 et 8 de la Charte des droits fondamentaux et avec les exigences du strict nécessaire est conditionnée par le respect des différentes garanties énumérées en B.59.2, découlant de l'interprétation conforme délivrée par la Cour de justice dans l'arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité. La compatibilité des règlementations nationales transposant la directive PNR avec les articles 7 et 8 de la Charte des droits fondamentaux et avec les exigences du strict nécessaire est dès lors conditionnée dans la même mesure.

B.59.4. La compatibilité du système mis en place par la loi du 25 décembre 2016 avec les différentes normes de référence visées au moyen impose dès lors d'interpréter la loi du 25 décembre 2016 comme intégrant les garanties énumérées en B.59.2, relevant de la transposition de la directive PNR, telle qu'elle a été interprétée par la Cour de justice.

Il appartient à l'UIP et aux différentes autorités concernées de veiller au respect de ces garanties, dans la mise en œuvre de la loi du 25 décembre 2016.

a) La gestion de la banque de données des passagers par l'UIP (articles 12 à 16)

B.60.1. 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 de cette loi. 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 de la même loi.

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).

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 » (ci-après : l'arrêté royal du 21 décembre 2017) définit, entre autres, les modalités de composition et d'organisation de l'UIP.

B.60.2. 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 26, 8°, de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de

données à caractère personnel » (article 15, § 2, de la loi du 25 décembre 2016, modifié par la loi du 2 mai 2019).

Les traitements des données des passagers effectués en vertu de la loi attaquée sont soumis à la loi du 30 juillet 2018 précitée (article 15, § 4, de la loi du 25 décembre 2016, modifié par la loi du 2 mai 2019).

Dans le cadre des finalités visées à l'article 8, § 1er, de la loi du 25 décembre 2016, la banque de données des passagers est directement accessible par l'UIP pour les traitements visés aux articles 24 à 27 de la même loi, 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.

Un protocole d'accord mettant en œuvre 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.60.3. 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.61.1. 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 B.60, constitue un élément essentiel du système mis en place par la directive PNR, que la loi du 25 décembre 2016 transpose.

B.61.2.1. Comme il est dit en B.60.1, l'UIP est composée d'un fonctionnaire dirigeant, assisté par un service d'appui, et de membres détachés issus des services compétents, énumérés à l'article 14, § 1er, alinéa 1er, 2°, de la loi du 25 décembre 2016, à savoir *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 et *d)* des 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.

Le fonctionnaire dirigeant de l'UIP a la responsabilité finale pour les tâches et les missions que la loi confie à l'UIP, et prend à cet effet les décisions nécessaires (article 3 de l'arrêté royal du 21 décembre 2017); il doit être titulaire d'une habilitation de sécurité nationale et UE de niveau « TRES SECRET », telle que visée par la loi du 11 décembre 1998 (article 11, alinéa 1er, de l'arrêté royal du 21 décembre 2017).

Dès leur entrée en fonction, les membres du service d'appui doivent être titulaires d'une habilitation de sécurité nationale et UE de niveau au moins « SECRET », telle que visée par la loi du 11 décembre 1998 (article 11, alinéa 2, de l'arrêté royal du 21 décembre 2017).

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 (article 14, § 1er, alinéa 2, de la loi du 25 décembre 2016). Ces membres détachés sont sélectionnés sur la base de leur profil et soumis à un entretien devant une commission de trois personnes, présidée par le fonctionnaire dirigeant de l'UIP, qui établit, à l'issue de l'entretien, un classement motivé des candidats, sur la base duquel les membres détachés sont désignés (article 12 de l'arrêté royal du 21 décembre 2017). Au moment de sa désignation, le membre détaché doit notamment posséder, au regard des missions de l'UIP, une expérience utile d'au moins trois ans, et se montrer prêt à s'investir dans l'analyse de données des passagers et dans la coopération avec les services compétents (article 13, 3°, de l'arrêté royal du 21 décembre 2017) et être titulaire d'une habilitation de sécurité nationale et UE de niveau au moins « SECRET » telle que visée par la loi du 11 décembre 1998 (article 14 de l'arrêté royal du 21 décembre 2017).

B.61.2.2. La composition de l'UIP et la définition des « services compétents » offrent des garanties d'expertise et de confidentialité concernant la gestion de la banque de données des passagers, au regard des seules finalités strictement limitées à des fins de prévention et de détection, ainsi que d'enquêtes et de poursuites, des infractions terroristes et des seules formes graves de criminalité, en référence aux catégories d'infractions énumérées de manière exhaustive dans l'annexe II de la directive PNR et présentant un lien objectif, à tout le moins indirect, avec le transport concerné. Cela vaut également dans la mesure où sont détachés à l'UIP des membres de la Sûreté de l'État et du Service général de Renseignement et de Sécurité. Ce qui a été jugé en B.52 concernant la finalité de suivi des activités visées par les services de renseignement et de sécurité, visée à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016, ne change rien à ce constat.

Les membres des services précités peuvent en effet être présumés disposer d'une expertise globale en matière de lutte contre la criminalité et disposer dès lors des compétences requises pour poursuivre les finalités exhaustivement énumérées dans la directive PNR. Il ressort en

outre de ce qui précède que les agents détachés sont sélectionnés et désignés sur la base d'un profil directement lié à la gestion de la banque de données des passagers, et qu'ils exercent leurs missions, dans ce cadre, sous la seule autorité fonctionnelle et hiérarchique du fonctionnaire dirigeant de l'UIP.

Lorsque ces agents exercent leurs missions de gestion de la banque de données des passagers, ils ne peuvent dès lors exercer leurs missions que pour le traitement des seules finalités autorisées par la directive PNR.

B.61.3. Compte tenu de ce qui est dit en B.61.2.2, et au regard des différentes garanties, énumérées en B.60, 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.62.1. 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.62.2. 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.62.3.1. 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.

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.62.3.2. En ce qui concerne la corrélation avec les banques de données, les travaux préparatoires de la loi du 25 décembre 2016 exposent :

« 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 internationales 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.

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.62.4.1. 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 (§ 3).

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 (§ 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.62.4.2. 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.

Il[s] 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 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 31).

B.63.1. 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 pour identifier les personnes devant être soumises à un examen plus approfondi.

Il ressort des éléments qui précèdent, interprétés à la lumière de ce qui est dit en B.59, que les articles 24 à 26 de la loi du 25 décembre 2016 respectent les limites du « strict nécessaire ».

B.63.2.1. Les banques de données avec lesquelles les données PNR peuvent être confrontées sont définies avec précision et énumérées à l'article 24 de la loi du 25 décembre 2016. Sont visées les 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, mais il peut s'agir aussi, comme il est précisé dans les travaux préparatoires cités en B.62.3.2, d'une corrélation avec des banques de données internationales telles que SIS II, Interpol (SLTD), auxquels les services compétents ont accès dans le cadre de l'exercice de leurs missions.

L'article 24, § 2, 1°, de la loi du 25 décembre 2016 permet également une corrélation avec des « listes de personnes élaborées par les services compétents dans le cadre de leurs missions ». Comme il est dit en B.61.2.2, les membres des services précités peuvent en effet être présumés disposer d'une expertise globale en matière de lutte contre la criminalité, et disposer dès lors des compétences requises pour poursuivre les finalités exhaustivement énumérées dans la directive PNR.

B.63.2.2. Il ressort des travaux préparatoires cités en B.62.3.2 que l'objectif poursuivi n'est 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 strictement limitées à la lutte contre des infractions terroristes et des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers.

Le législateur avait dès lors pour objectif de limiter clairement les corrélations techniques dans le cadre de l'évaluation préalable, afin d'identifier uniquement les profils appelant un examen plus approfondi au regard des seuls objectifs exhaustivement énumérés dans la directive PNR.

B.63.2.3. Il y a dès lors lieu, compte tenu de l'arrêt de la Cour de justice en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, rappelé en B.59, d'interpréter la confrontation des données PNR aux banques de données et aux listes visées à l'article 24, § 2, 1°, de la loi du 25 décembre 2016 comme étant strictement limitée, techniquement, aux seules bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, ces bases de données étant exploitées de manière non discriminatoire, par les autorités compétentes, en rapport avec la lutte contre des infractions terroristes et des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers.

Il appartient à l'UIP de veiller à ce que, d'un point de vue technique, le traitement automatisé permettant ces corrélations ne dépasse pas les limites du strict nécessaire.

B.63.3.1. 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 ».

L'article 25 de la loi du 25 décembre 2016 garantit expressément que l'évaluation des passagers avant leur arrivée, leur transit ou leur départ au regard des critères préétablis est réalisée de façon non discriminatoire et que ces critères ne peuvent viser l'identification d'un

individu et doivent être ciblés, proportionnés et spécifiques (§ 2). Les travaux préparatoires cités en B.62.4.2 précisent qu'ils ne sont pas nominatifs. En outre, 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 (§ 3).

De manière analogue aux corrélations avec les banques de données, l'élaboration de critères préétablis est conçue comme limitée techniquement à l'identification de personnes devant faire l'objet d'un examen plus approfondi au regard des finalités strictement limitées à la lutte contre des infractions terroristes et des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers.

B.63.3.2. Il y a dès lors lieu, compte tenu de l'arrêt de la Cour de justice en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, rappelé en B.59, d'interpréter l'élaboration de critères préétablis visés à l'article 25 de la loi du 25 décembre 2016 comme empêchant l'UIP d'utiliser des technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (*machine learning*), susceptibles de modifier, sans intervention et contrôle humains. En outre, les critères d'évaluation sur lesquels se fonde le résultat de l'application de ce processus, ainsi que la pondération de ces critères doivent être déterminés de manière à ce que leur application cible, spécifiquement, les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou à des formes graves de criminalité, et à tenir compte tant des éléments « à charge » que des éléments « à décharge », tout en ne donnant pas lieu à des discriminations directes ou indirectes.

Il appartient à l'UIP de veiller à ce que, d'un point de vue technique, l'élaboration des critères préétablis n'excède pas les limites du strict nécessaire.

B.63.4.1. En ce qui concerne le souci de limiter le taux d'erreur par des « faux positifs », il convient de constater que l'article 24, §§ 4 et 5, de la loi du 25 décembre 2016 prévoit que l'UIP effectue un réexamen individuel en validant la correspondance positive dans les vingt-quatre heures, garantissant ainsi 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.

En outre, l'article 21, § 3, alinéa 2, de la loi du 25 décembre 2016 garantit que, lorsque, à la suite du réexamen individuel visé à l'article 24, § 4, le résultat du traitement s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées sur la base de l'article 18, de manière à éviter de fausses correspondances positives.

Il convient, compte tenu de l'arrêt de la Cour de justice en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, rappelé en B.59, d'interpréter ce réexamen individuel comme étant effectué selon des règles claires et précises permettant de garantir une pratique administrative cohérente au sein de l'UIP respectant le principe de non-discrimination et permettant de vérifier si et dans quelle mesure une concordance positive (*hit*) concerne effectivement un individu qui est susceptible d'être impliqué dans les infractions terroristes ou les formes graves de criminalité.

Il appartient à l'UIP de veiller au respect de ces exigences.

B.63.4.2. Par ailleurs, l'article 23, § 1er, de la loi du 25 décembre 2016 garantit que le traitement des données fait l'objet d'une « journalisation », définie par l'article 4, 11°, de la même loi comme « le mécanisme visé à l'article 23, § 2, permettant le traçage des traitements de données effectués afin qu'il soit possible d'identifier la personne qui a consulté des données, les données consultées, le moment et la finalité de cette consultation ».

L'article 23, § 2, de la loi du 25 décembre 2016 garantit que l'UIP conserve pendant cinq ans une trace documentaire de tous les systèmes et procédures de traitement sous sa responsabilité. Cette trace documentaire comprend au minimum : le nom et les coordonnées de l'organisation et du personnel chargés du traitement des données des passagers au sein de l'UIP ainsi que leurs demandes et les différents niveaux d'autorisation d'accès (1°), un registre des opérations de traitement qui indique au minimum l'identité de la personne qui a traité les données des passagers (2°), les demandes formulées par les autorités compétentes et les UIP

d'autres États membres de l'Union européenne (3°) et toutes les demandes et tous les transferts de données vers un pays tiers (4°). L'UIP met ces traces documentaires à la disposition de l'autorité compétente de contrôle des traitements de données à caractère personnel, à la demande de celle-ci (article 23, § 2, alinéa 2).

Cette disposition garantit ainsi que l'UIP conserve une trace documentaire de tout traitement des données PNR effectué dans le cadre de l'évaluation préalable, y compris dans le cadre du réexamen individuel par des moyens non automatisés, aux fins de la vérification de sa licéité et d'un autocontrôle.

B.63.5. Enfin, en ce qui concerne les droits et l'information des personnes intéressées, la Cour de justice, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, cité en B.59, a précisé que les autorités compétentes doivent également s'assurer que l'intéressé puisse comprendre le fonctionnement des critères d'évaluation préétablis et des programmes appliquant ces critères, de manière à ce qu'il puisse décider, en pleine connaissance de cause, s'il exerce ou non son droit à un recours juridictionnel garanti par l'article 13, paragraphe 1, de la directive PNR, dans le cadre duquel le juge chargé du contrôle de la légalité de la décision adoptée par les autorités compétentes, ainsi que, hormis les cas de menaces pour la sûreté de l'État, l'intéressé lui-même doivent pouvoir prendre connaissance tant de l'ensemble des motifs que des éléments de preuve sur la base desquels cette décision a été prise, y compris des critères d'évaluation préétablis et du fonctionnement des programmes appliquant ces critères (points 210-211).

Il appartient aux autorités compétentes de veiller au respect de ces exigences.

c) Les recherches ponctuelles (articles 27, 50 et 51)

B.64.1. 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°, de la même loi 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. L'article 6 de la loi du 2 mai 2019, non attaqué, a modifié l'article 27 de la loi du 25 décembre 2016 pour

permettre ces recherches ponctuelles aux conditions prévues par l'article 281, § 4, de la loi générale sur les douanes et accises, coordonnée le 18 juillet 1977.

Conformément à l'article 20 de la loi du 25 décembre 2016, les conditions d'application de l'article 27 de la même loi valent également pour la communication de l'intégralité des données des passagers à l'expiration du délai de six mois prévu à l'article 19 de ladite loi.

B.64.2. 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.

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 des finalités visées 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.64.3. 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.

B.64.4. 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).

B.65.1. La partie requérante estime par ailleurs 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.65.2. 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).

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.65.3. 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.65.4. Comme il est dit en B.61.2, 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 [...] ».

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 de la même loi).

B.65.5.1. En ce qui concerne l'accès aux données PNR après un délai de six mois, l'article 12, paragraphe 3, de la directive PNR dispose :

« 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.65.5.2. Conformément à l'article 20 de la loi du 25 décembre 2016, les conditions d'application de l'article 27 de la même loi valent également pour la communication de l'intégralité des données des passagers à l'expiration du délai de six mois prévu à l'article 19. En étendant le régime des recherches ponctuelles visé par l'article 27 de ladite loi à la communication de l'intégralité des données des passagers à l'expiration du délai de six mois, l'article 20 déroge au principe posé par l'article 19 de la loi du 25 décembre 2016, selon lequel, 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.

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

« Après 6 mois, les données passagers peuvent encore être rendue[s] visibles dans leur intégralité uniquement lorsqu'il existe des motifs raisonnables de penser qu'elles sont nécessaires aux fins de l'article 27 et uniquement dans les conditions prévues à l'article 27.

Ce mode de traitement exclut donc la finalité 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'autorisation du procureur du Roi est nécessaire » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-2069/001, p. 26).

Il résulte dès lors de la combinaison des articles 20 et 27 de la loi du 25 décembre 2016 que les conditions d'accès aux données PNR dans le cadre de recherches ponctuelles sont transposées à la communication de données à l'expiration d'un délai de six mois suivant le transfert de ces données à l'UIP, délai après lequel ces données devraient être dépersonnalisées.

B.66.1. Dès lors que, comme il est jugé en B.52, la finalité visée à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016 excède les exigences du « strict nécessaire », il en va de même des dispositions qui autoriseraient les services de renseignement et de sécurité à accéder, par simple décision motivée, aux données de la banque de données des passagers, pour cette finalité qui excède celles qui sont énumérées de manière exhaustive dans la directive PNR.

B.66.2. Pour les mêmes motifs que ceux qui sont énoncés en ce qui concerne l'article 8, § 1er, 4°, de la loi du 25 décembre 2016, l'article 51 de la loi du 25 décembre 2016 excède les exigences du « strict nécessaire ».

B.67. La Cour doit maintenant examiner si le régime de communication des données PNR établi par les articles 27 et 50 de la loi du 25 décembre 2016 respecte les exigences du strict nécessaire, ainsi que les garanties d'indépendance de l'autorité chargée d'autoriser cet accès.

B.68.1. Comme il est dit en B.59, en ce qui concerne la communication et l'évaluation ultérieures des données PNR, c'est-à-dire après l'arrivée ou le départ de la personne concernée, la Cour de justice considère qu'elles ne peuvent être effectuées que sur la base de circonstances nouvelles et d'éléments objectifs qui soit sont de nature à fonder un soupçon raisonnable d'implication de cette personne dans des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers, soit permettent de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre des infractions terroristes présentant un tel lien.

La communication des données PNR aux fins d'une telle évaluation ultérieure doit, en principe, sauf en cas d'urgence dûment justifiée, être subordonnée à un contrôle préalable effectué soit par une juridiction soit par une autorité administrative indépendante, sur demande motivée des autorités compétentes, et ce, indépendamment du point de savoir si cette demande a été introduite avant ou après l'expiration du délai de six mois suivant le transfert de ces données à l'UIP.

Plus précisément, la Cour de justice précise que l'exigence d'un contrôle préalable prévu à l'article 12, paragraphe 3, *b)*, de la directive PNR, pour les demandes de communication des données PNR introduites après l'expiration du délai de six mois suivant le transfert de ces données à l'UIP, doit également s'appliquer, *mutatis mutandis*, dans le cas où la demande de communication est introduite avant l'expiration de ce délai (point 224).

B.68.2. Interrogée par la Cour sur l'interprétation d'une « autre autorité nationale compétente » au sens de l'article 12, paragraphe 3, de la directive PNR, la Cour de justice a

jugé, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité :

« 241. Sur le fond, il convient de relever que le libellé de l'article 12, paragraphe 3, sous *b)*, de la directive PNR, qui mentionne respectivement, à ses points i) et ii), ' une autorité judiciaire ' et ' une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies ', met sur le même plan ces deux autorités, ainsi qu'il ressort de l'emploi de la conjonction ' ou ' entre ces points i) et ii). Il découle ainsi de ce libellé que l' ' autre ' autorité nationale compétente ainsi visée constitue une alternative à l'autorité judiciaire et doit, partant, présenter un niveau d'indépendance et d'impartialité comparable à cette dernière.

242. Cette analyse est confortée par l'objectif de la directive PNR, visé au considérant 25 de celle-ci, de garantir le niveau le plus élevé de protection des données en ce qui concerne l'accès à l'intégralité des données PNR, qui permettent l'identification directe de la personne concernée. Ce même considérant précise d'ailleurs qu'un tel accès ne devrait être accordé que dans des conditions très strictes après le délai de six mois suivant le transfert des données PNR à l'UIP.

243. Ladite analyse est également corroborée par la genèse de la directive PNR. En effet, alors que la proposition de directive mentionnée au point 155 du présent arrêt, à l'origine de la directive PNR, se limitait à prévoir que ' [l]'accès à l'intégralité des données PNR n'est autorisé que par le responsable de l'unité de renseignement passagers ', la version de l'article 12, paragraphe 3, sous *b)*, de cette directive finalement retenue par le législateur de l'Union désigne, en les plaçant sur le même plan, l'autorité judiciaire et une ' autre autorité nationale ' compétente pour vérifier si les conditions de communication de l'intégralité des données PNR sont remplies et approuver une telle communication.

244. En outre et surtout, conformément à une jurisprudence constante rappelée aux points 223, 225 et 226 du présent arrêt, il est essentiel que l'accès des autorités compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne 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. L'exigence d'indépendance à laquelle doit satisfaire l'entité chargée d'exercer le contrôle préalable impose également que celle-ci ait la qualité de tiers par rapport à l'autorité qui demande l'accès aux données, de sorte que ladite entité soit en mesure d'exercer ce contrôle de manière objective et impartiale, en étant protégée de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale.

245. Or, ainsi que l'a relevé M. l'avocat général au point 271 de ses conclusions, l'article 4 de la directive PNR prévoit, à ses paragraphes 1 et 3, que l'UIP mise en place ou désignée dans chaque État membre est 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, et que les membres de son personnel peuvent être des agents détachés par les autorités compétentes visées à l'article 7 de cette directive, de sorte que l'UIP apparaît

nécessairement liée à ces autorités. L'UIP peut également procéder, en vertu de l'article 6, paragraphe 2, sous *b)*, de ladite directive, à des traitements de données PNR dont elle communique le résultat auxdites autorités. Au vu de ces éléments, l'UIP ne saurait être regardée comme présentant la qualité de tiers par rapport à ces mêmes autorités et, partant, comme disposant de toutes les qualités d'indépendance et d'impartialité requises pour exercer le contrôle préalable mentionné au point précédent du présent arrêt et vérifier si les conditions de communication de l'intégralité des données PNR sont remplies, tel que prévu à l'article 12, paragraphe 3, sous *b)*, de la même directive.

246. Par ailleurs, le fait que cette dernière disposition exige, à son point ii), en cas d'approbation de la communication de l'intégralité de ces données par une ' autre autorité nationale compétente ', que le délégué à la protection des données de l'UIP ' en soit informé et procède à un examen ex post ', alors que tel n'est pas le cas lorsque cette approbation est donnée par l'autorité judiciaire, n'est pas de nature à remettre en cause cette appréciation. En effet, selon une jurisprudence bien établie, un contrôle ultérieur, comme celui opéré par le délégué à la protection des données, ne permet pas de répondre à l'objectif du contrôle préalable, qui consiste à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 110 ainsi que jurisprudence citée).

247. Eu égard à l'ensemble de ces considérations, il convient de répondre à la septième question que l'article 12, paragraphe 3, sous *b)*, de la directive PNR doit être interprété en ce sens qu'il s'oppose à une législation nationale selon laquelle l'autorité mise en place en tant qu'UIP a également la qualité d'autorité nationale compétente habilitée à approuver la communication des données PNR à l'expiration de la période de six mois suivant le transfert de ces données à l'UIP ».

B.68.3. Il ressort de ce qui précède que la communication et l'évaluation ultérieures des données PNR sont encadrées par des exigences tant organiques que substantielles.

D'une part, au niveau organique, l'UIP ne peut être considérée comme ayant la qualité d' « autorité nationale compétente » habilitée à approuver la communication des données PNR que ce soit avant ou après l'expiration de la période de six mois suivant le transfert de ces données à l'UIP. Selon la Cour de justice, une telle autorité nationale compétente doit présenter un niveau d'indépendance et d'impartialité comparable à une autorité judiciaire, ce qui implique que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale (point 244). Un contrôle ultérieur, comme celui opéré par le délégué à la protection des données, ne permet pas de répondre à l'objectif du contrôle préalable (point 246).

D’autre part, au niveau substantiel, cette communication ne peut, en outre, être décidée que sur la base de circonstances nouvelles et d’éléments objectifs qui soit sont de nature à fonder un soupçon raisonnable d’implication de cette personne dans des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers, soit permettent de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre des infractions terroristes présentant un tel lien.

B.69.1. Comme il est dit en B.64.1 et B.64.2, l’article 27 de la loi du 25 décembre 2016 permet la communication des données PNR en vue de procéder à des recherches ponctuelles aux conditions prévues, notamment, par l’article 46*septies* du Code d’instruction criminelle, inséré par l’article 50 de la loi du 25 décembre 2016.

Cette disposition limite le recours à l’article 27 précité aux finalités visées à l’article 8, § 1er, 1°, 2° et 5°, de la loi du 25 décembre 2016, et prévoit l’autorisation préalable du procureur du Roi, par une décision motivée et écrite, qui reflète le caractère proportionné de la mesure eu égard au respect de la vie privée et subsidiaire à tout autre devoir d’enquête; cette mesure ne peut excéder un mois à dater de la décision, sans préjudice de renouvellement.

D’un point de vue substantiel, il convient d’interpréter le régime d’autorisation préalable prévu par l’article 27 de la loi du 25 décembre 2016 en tenant compte de l’arrêt de la Cour de justice en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, rappelé en B.59, comme exigeant que l’autorité qui effectuera le contrôle préalable de la nécessité de la communication des données PNR, sur demande motivée des autorités compétentes, évalue au cas par cas l’existence de circonstances nouvelles et d’éléments objectifs qui soit sont de nature à fonder un soupçon raisonnable d’implication de cette personne dans des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport des passagers, soit permettent de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre des infractions terroristes présentant un tel lien.

Ainsi interprété, le régime prévu par l'article 27 de la loi du 25 décembre 2016 est, d'un point de vue substantiel, conforme aux dispositions visées au moyen.

B.69.2. D'un point de vue organique, en revanche, le régime organisé par l'article 27 de la loi du 25 décembre 2016, applicable pour les recherches ponctuelles et étendu, comme il est dit en B.65.5, par l'article 20 de la même loi à la communication de données après l'expiration d'un délai de six mois, ne permet pas de considérer qu'un contrôle préalable de la décision de communication est confié à une « autorité nationale indépendante ».

Tout d'abord, comme il est dit en B.68.3, l'UIP ne peut être considérée comme une « autorité nationale indépendante », lorsqu'elle communique des données des passagers, à la demande d'autorités compétentes.

Ensuite, l'article 46*septies* du Code d'instruction criminelle, qui a été inséré par l'article 50 de la loi du 25 décembre 2016 et auquel renvoie l'article 27 de la même loi prévoit certes une intervention préalable du procureur du Roi, mais, conformément à l'article 46*septies* précité, c'est ce dernier qui décide lui-même, par une décision écrite et motivée, de 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. En outre, le Procureur du Roi étant chargé de la recherche des infractions, il ne peut être considéré comme une autorité nationale indépendante pouvant exercer le contrôle préalable à la communication des données tel que l'exige la Cour de justice dans le point 244 de son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité.

Pour le surplus, il convient de constater que l'article 281, § 4, de la loi générale sur les douanes et accises, coordonnée le 18 juillet 1977, qui a été inséré par l'article 6 de la loi du 2 mai 2019 et auquel renvoie l'article 27 de la loi du 25 décembre 2016, tel qu'il a été modifié par cette même loi du 2 mai 2019, prévoit que le conseiller-général désigné pour l'administration en charge des contentieux peut, par une décision écrite et motivée, charger un agent des douanes et accises de requérir l'UIP afin de communiquer les données des passagers. Quant au régime prévu par l'article 16/3 de la loi du 30 novembre 1998 « organique des services

de renseignement et de sécurité », inséré par l'article 51 de la loi du 25 décembre 2016 – lequel excède les exigences du strict nécessaire, comme la Cour l'a jugé en B.66 –, il prévoyait que les services de renseignement et de sécurité pouvaient, 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.

De telles procédures, auxquelles renvoie l'article 27 de la loi du 25 décembre 2016, ne respectent dès lors pas l'exigence d'un contrôle préalable à la communication des données, par une autorité administrative indépendante, telle qu'elle a été définie par la Cour de justice dans les points 244 à 246 de son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité.

B.69.3. En ce qu'il ne subordonne pas, sauf en cas d'urgence dûment justifiée, la communication des données PNR aux fins d'une évaluation ultérieure, à un contrôle préalable effectué soit par une juridiction soit par une « autorité administrative indépendante », sur demande motivée des autorités compétentes, l'article 27 de la loi du 25 décembre 2016 viole les dispositions visées au moyen.

B.69.4. C'est au législateur qu'il appartient de déterminer l'organe chargé d'exercer ce contrôle préalable, compte tenu de ce que la Cour de justice a jugé par son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, en ce qui concerne tant l'étendue du contrôle que les conditions d'impartialité et d'indépendance de l'organe chargé de ce contrôle.

B.69.5. Dans l'attente de cette intervention du législateur censée permettre la communication des données PNR en vue d'une évaluation ultérieure, il y a lieu de considérer que l'Autorité de protection des données – qui dispose, conformément à l'article 4, § 2, alinéa 2, de la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données », d'une compétence résiduaire à l'égard des traitements de données à caractère personnel – constitue une « autorité administrative indépendante » répondant aux exigences d'impartialité et d'indépendance posées par la Cour de justice.

Avant toute communication des données PNR en vue d'une évaluation ultérieure, il y a dès lors lieu, pour l'application de l'article 27 de la loi du 25 décembre 2016, de saisir au préalable l'Autorité de protection des données, en tenant compte de ce qui est dit en B.69.1 et en s'inspirant, le cas échéant, du régime prévu à l'article 46*septies* du Code d'instruction criminelle.

B.70. En ce qu'il est dirigé contre l'article 51 de la loi du 25 décembre 2016 et contre l'article 27 de la loi du 25 décembre 2016, en ce que ce dernier ne subordonne pas, sauf en cas d'urgence dûment justifiée, la communication des données PNR aux fins d'une évaluation ultérieure, à un contrôle préalable effectué soit par une juridiction soit par une « autorité administrative indépendante », sur demande motivée des autorités compétentes, le moyen est fondé.

Pour le surplus, sous réserve des interprétations mentionnées en B.63.2.3, B.63.3.2, B.63.4.1, B.69.1 et compte tenu de ce qui est dit en B.61.2.2, le moyen, en ce qu'il est dirigé contre les articles 12 à 16 et 24 à 26 et 50 de la loi du 25 décembre 2016, n'est pas fondé.

5. *La durée de conservation des données PNR (article 18)*

B.71. 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.72.1. 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.72.2. 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.72.3. 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.72.4.1. 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.72.4.2. 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;

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.72.4.3. Comme il est dit en B.64.1 et B.65.5, 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.72.4.4. 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.73.1. Interrogée par la Cour au sujet de durée de conservation des données PNR, la Cour de justice a jugé, dans son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité :

« 249. Il y a lieu de rappeler que, selon l'article 12, paragraphes 1 et 4, de cette directive, l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol concerné conserve les données PNR fournies par les transporteurs aériens dans une base de données pendant une période de cinq ans suivant leur transfert à cette unité et efface ces données de manière définitive à l'issue de cette période de cinq ans.

250. Ainsi que le rappelle le considérant 25 de la directive PNR, 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 '.

251. Par conséquent, la conservation des données PNR en application de l'article 12, paragraphe 1, de la directive PNR ne saurait être justifiée en l'absence de rapport objectif entre cette conservation et les objectifs poursuivis par cette directive, à savoir la lutte contre les infractions terroristes et les formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers.

252. À cet égard, ainsi qu'il ressort de ce considérant 25 de la directive PNR, il y a lieu d'opérer une distinction entre, d'une part, la période de conservation initiale de six mois, visée à l'article 12, paragraphe 2, de cette directive, et, d'autre part, la période ultérieure, visée à l'article 12, paragraphe 3, de ladite directive.

253. L'interprétation de l'article 12, paragraphe 1, de la directive PNR doit prendre en compte les dispositions figurant aux paragraphes 2 et 3 de cet article, qui fixent le régime de conservation et d'accès aux données PNR conservées après l'expiration de la période de conservation initiale de six mois. Ainsi qu'il découle du considérant 25 de cette directive, ces dispositions traduisent, d'une part, l'objectif d'assurer ' que les données PNR soient conservées pendant une période suffisamment longue pour permettre leur analyse et leur utilisation dans le cadre d'enquêtes ', celles-ci pouvant déjà être effectuées au cours de la période de conservation initiale de six mois. D'autre part, elles cherchent, selon ce même considérant 25, à ' éviter toute utilisation disproportionnée ' par un masquage de ces données et à ' garantir le niveau le plus élevé de protection de données ' en n'autorisant l'accès à ces données sous une forme permettant l'identification directe de la personne concernée ' que dans des conditions très strictes et limitées après ce délai initial ', tenant ainsi compte du fait que plus la conservation des données PNR est longue, plus l'ingérence en résultant est grave.

254. Or, la distinction entre la période de conservation initiale de six mois, visée à l'article 12, paragraphe 2, de la directive PNR, et la période ultérieure, visée à l'article 12, paragraphe 3, de cette directive, s'applique également au respect nécessaire de l'exigence visée au point 251 du présent arrêt.

255. Ainsi, eu égard aux finalités de la directive PNR et aux besoins des enquêtes et des poursuites en matière d'infractions terroristes et de formes graves de criminalité, il y a lieu de considérer que la conservation, au cours de la période initiale de six mois, des données PNR de l'ensemble des passagers aériens soumis au système instauré par cette directive, sans qu'il existe la moindre indication de leur implication dans des infractions terroristes ou des formes graves de criminalité, ne paraît pas, par principe, excéder les limites du strict nécessaire, dans la mesure où elle permet les recherches nécessaires aux fins d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité.

256. En revanche, s'agissant de la période ultérieure, visée à l'article 12, paragraphe 3, de la directive PNR, la conservation des données PNR de l'ensemble des passagers aériens soumis au système instauré par cette directive, outre le fait qu'elle comporte, en raison de la quantité importante de données susceptibles d'être conservées de manière continue, des risques inhérents d'utilisation disproportionnée et d'abus (voir, par analogie, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 119), se heurte à l'exigence visée au considérant 25 de ladite directive, selon lequel ces données ne devraient être conservées que pour la durée nécessaire et proportionnée aux objectifs poursuivis, le législateur de l'Union ayant entendu établir le niveau le plus élevé de protection des données PNR qui permettent une identification directe des personnes concernées.

257. En effet, s'agissant des passagers aériens pour lesquels ni l'évaluation préalable visée à l'article 6, paragraphe 2, sous *a)*, de la directive PNR, ni les éventuelles vérifications effectuées au cours de la période de six mois visée à l'article 12, paragraphe 2, de cette directive, ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le voyage aérien effectué par ces passagers, il n'apparaît pas exister, dans de telles circonstances, de rapport, ne serait-ce qu'indirect, entre les données PNR de ces passagers et l'objectif poursuivi par ladite directive, qui justifierait la conservation de ces mêmes données [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 204 et 205].

258. Le stockage continu des données PNR de l'ensemble des passagers après la période initiale de six mois n'apparaît donc pas limité au strict nécessaire [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 206].

259. Dans la mesure où, toutefois, sont identifiés, dans des cas particuliers, des éléments objectifs, tels que les données PNR des passagers ayant donné lieu à une concordance positive vérifiée, qui permettent de considérer que certains passagers pourraient présenter un risque en matière d'infractions terroristes ou de formes graves de criminalité, un stockage de leurs données PNR paraît admissible au-delà de cette période initiale [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 207 et jurisprudence citée].

260. En effet, l'identification de ces éléments objectifs serait de nature à établir un rapport avec les objectifs poursuivis par les traitements au titre de la directive PNR, de sorte que la conservation des données PNR relatives à ces passagers serait justifiée pendant le délai maximal admis par ladite directive, à savoir pendant cinq ans.

261. En l'occurrence, dans la mesure où la législation en cause au principal paraît prévoir une durée générale de conservation des données PNR de cinq ans, applicable indifféremment à tous les passagers, y compris à ceux pour lesquels ni l'évaluation préalable visée à l'article 6, paragraphe 2, sous *a)*, de la directive PNR, ni les éventuelles vérifications effectuées au cours de la période initiale de six mois, ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité, cette législation est susceptible de méconnaître l'article 12, paragraphe 1, de cette directive, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, à moins qu'elle ne puisse faire l'objet d'une interprétation conforme à ces dispositions, ce qu'il incombe à la juridiction de renvoi de vérifier.

262. Eu égard aux considérations qui précèdent, il y a lieu de répondre à la huitième question que l'article 12, paragraphe 1, de la directive PNR, lu en combinaison avec les articles 7 et 8 ainsi qu'avec l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale qui prévoit une durée générale de conservation des données PNR de cinq ans, applicable indifféremment à tous les passagers aériens, y compris à ceux pour lesquels ni l'évaluation préalable visée à l'article 6, paragraphe 2, sous *a)*, de cette directive, ni les éventuelles vérifications effectuées au cours de la période de six mois visée à l'article 12, paragraphe 2, de ladite directive, ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers ».

B.73.2. Il découle de cet arrêt qu'en ce qui concerne la durée de conservation des données PNR, il y a lieu d'opérer une distinction entre, d'une part, la période de conservation initiale de six mois, visée à l'article 12, paragraphe 2, de cette directive, et, d'autre part, la période ultérieure, visée à l'article 12, paragraphe 3, de ladite directive (point 252) : si la conservation, au cours de la période initiale de six mois, des données PNR de l'ensemble des passagers soumis au système instauré par cette directive, sans qu'il existe la moindre indication

de leur implication dans des infractions terroristes ou des formes graves de criminalité, ne paraît pas, par principe, excéder les limites du strict nécessaire, dans la mesure où elle permet les recherches nécessaires aux fins d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité (point 255), la conservation des données PNR de l'ensemble des passagers soumis au système instauré par cette directive, au-delà de cette période initiale de six mois, excède les limites du strict nécessaire, notamment en raison de la quantité importante de données susceptibles d'être conservées de manière continue et des risques inhérents d'utilisation disproportionnée et d'abus (point 256).

En effet, en ce qui concerne les passagers pour lesquels ni l'évaluation préalable visée à l'article 6, paragraphe 2, *a)*, de la directive PNR ni les éventuelles vérifications effectuées au cours de la période de six mois visée à l'article 12, paragraphe 2, de cette directive ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs étant de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le voyage effectué par ces passagers, il n'apparaît pas exister, dans de telles circonstances, de rapport, ne serait-ce qu'indirect, entre les données PNR de ces passagers et l'objectif poursuivi par ladite directive, qui justifierait la conservation de ces mêmes données (point 257).

La Cour de justice laisse à la juridiction qui pose les questions le soin de vérifier si la loi du 25 décembre 2016 peut être interprétée de manière conforme aux exigences des articles 7 et 8 de la Charte des droits fondamentaux, combinés avec l'article 52, paragraphe 1, de la Charte (point 261).

B.74.1. Comme il est dit en B.72.2, 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.

Cette disposition se limite à fixer une durée maximale de conservation, sans identifier les données appelées à être conservées pendant cette durée maximale.

L’article 18 de la loi du 25 décembre 2016 peut dès lors être interprété en ce sens qu’après la période initiale de six mois à compter de l’enregistrement des données des passagers dans la banque de données des passagers, seules sont conservées dans la banque de données des passagers, pendant une durée de cinq ans, les données des personnes pour lesquelles soit l’évaluation préalable visée à l’article 6, paragraphe 2, *a)*, de la directive PNR, soit les éventuelles vérifications effectuées au cours de la période de six mois visée à l’article 12, paragraphe 2, de cette directive, soit d’autres circonstances ont révélé l’existence d’éléments objectifs qui sont de nature à établir un risque en matière d’infractions terroristes ou de formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le voyage effectué par ces passagers.

Les données qui ne respecteraient pas cette interprétation doivent être détruites.

B.74.2. Dans l’interprétation mentionnée en B.74.1, l’article 18 de la loi du 25 décembre 2016 n’excède pas les exigences du strict nécessaire.

B.75. Sous réserve de l’interprétation mentionnée en B.74.1, le moyen, en ce qu’il est dirigé contre l’article 18 de la loi du 25 décembre 2016, n’est pas fondé.

Quant au second moyen

B.76. 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.77.1. 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 ».

B.77.2. 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).

B.77.3. 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.

Par son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, la Cour de justice a rappelé à cet égard que l'extension du système « PNR » aux vols intra-UE relève d'une faculté pour les États membres d'étendre l'application du système établi par cette directive aux vols intra-UE (point 162), et, comme il est dit en B.36.4.1, la Commission a constaté que tous les États membres, à une exception près, ont fait usage de cette faculté.

B.77.4. En ce qui concerne la mise en œuvre de cette faculté, la Cour de justice a, par son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, jugé :

« 274. Tout d'abord, l'article 45 de la Charte consacre la libre circulation des personnes, laquelle constitue, par ailleurs, l'une des libertés fondamentales du marché intérieur [voir, en

ce sens, arrêt du 22 juin 2021, Ordre des barreaux francophones et germanophone e.a. (Mesures préventives en vue d'éloignement), C-718/19, EU:C:2021:505, point 54].

275. Cet article garantit, à son paragraphe 1, le droit de tout citoyen de l'Union de circuler et de séjourner librement sur le territoire des États membres, droit qui, selon les explications relatives à la Charte des droits fondamentaux (JO 2007, C 303, p. 17), correspond à celui garanti à l'article 20, paragraphe 2, premier alinéa, sous *a)*, TFUE et s'exerce, conformément à l'article 20, paragraphe 2, second alinéa, TFUE et à l'article 52, paragraphe 2, de la Charte, dans les conditions et les limites définies par les traités et par les mesures adoptées en application de ceux-ci.

276. Ensuite, selon l'article 3, paragraphe 2, TUE, l'Union offre à ses citoyens un espace de liberté, de sécurité et de justice sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes, en liaison avec des mesures appropriées en matière, notamment, de contrôle des frontières extérieures ainsi que de prévention de la criminalité et de lutte contre ce phénomène. De même, conformément à l'article 67, paragraphe 2, TFUE, l'Union assure l'absence de contrôles des personnes aux frontières intérieures et développe une politique commune en matière, notamment, de contrôle des frontières extérieures.

277. Conformément à la jurisprudence constante de la Cour, une législation nationale qui désavantage certains ressortissants nationaux en raison du seul fait qu'ils ont exercé leur liberté de circuler et de séjourner dans un autre État membre constitue une restriction aux libertés reconnues par l'article 45, paragraphe 1, de la Charte à tout citoyen de l'Union (voir en ce sens, en ce qui concerne l'article 21, paragraphe 1, TFUE, arrêts du 8 juin 2017, Freitag, C-541/15, EU:C:2017:432, point 35 et jurisprudence citée, ainsi que du 19 novembre 2020, ZW, C-454/19, EU:C:2020:947, point 30).

278. Or, une législation nationale telle que celle en cause au principal, qui applique le système prévu par la directive PNR non seulement aux vols extra-UE mais également, conformément à l'article 2, paragraphe 1, de cette directive, aux vols intra-UE ainsi que, au-delà de ce qui est prévu à cette disposition, à des transports effectués par d'autres moyens à l'intérieur de l'Union, a pour conséquence le transfert ainsi que le traitement systématiques et continus des données PNR de tout passager se déplaçant par ces moyens à l'intérieur de l'Union en exerçant sa liberté de circulation.

279. Ainsi qu'il a été constaté aux points 98 à 111 du présent arrêt, le transfert ainsi que le traitement des données des passagers des vols extra-UE et intra-UE résultant du système établi par la directive PNR impliquent des ingérences d'une gravité certaine dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte des personnes concernées. La gravité de cette ingérence est encore accrue dans le cas où l'application de ce système est étendue à d'autres moyens de transports intérieurs à l'Union. De telles ingérences sont, pour les mêmes raisons que celles exposées à ces points, également de nature à désavantager et, partant, à dissuader d'exercer leur liberté de circulation, au sens de l'article 45 de la Charte, les ressortissants des États membres ayant adopté une telle législation ainsi que, de manière générale, les citoyens de l'Union se déplaçant par ces moyens de transport dans l'Union en provenance ou à destination de ces États membres, de sorte que ladite législation comporte une restriction à cette liberté fondamentale.

280. Conformément à une jurisprudence constante, une restriction à la libre circulation des personnes ne peut être justifiée que si elle se fonde sur des considérations objectives et est

proportionnée à l'objectif légitimement poursuivi par le droit national. Une mesure est proportionnée lorsque, tout en étant apte à la réalisation de l'objectif poursuivi, elle ne va pas au-delà de ce qui est nécessaire pour l'atteindre (voir, en ce sens, arrêt du 5 juin 2018, Coman e.a., C-673/16, EU:C:2018:385, point 41 ainsi que jurisprudence citée).

281. Il importe d'ajouter qu'une mesure nationale qui est de nature à entraver l'exercice de la libre circulation des personnes ne peut être justifiée que lorsque cette mesure est conforme aux droits fondamentaux garantis par la Charte dont la Cour assure le respect (arrêt du 14 décembre 2021, Stolichna obshtina, rayon ' Pancharevo ', C-490/20, EU:C:2021:1008, point 58 et jurisprudence citée).

282. En particulier, conformément à la jurisprudence rappelée aux points 115 et 116 du présent arrêt, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, et ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause. À cet égard, la possibilité pour les États membres de justifier une limitation du droit fondamental garanti à l'article 45, paragraphe 1, de la Charte doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité.

283. Ainsi qu'il a été rappelé au point 122 du présent arrêt, l'objectif de lutte contre les infractions terroristes et les formes graves de criminalité que poursuit la directive PNR est indubitablement un objectif d'intérêt général de l'Union.

284. S'agissant de la question de savoir si une législation nationale adoptée aux fins de transposer la directive PNR et qui étend le système prévu par cette directive aux vols intra-UE et à d'autres modes de transport intérieurs à l'Union est apte à la réalisation de l'objectif poursuivi, il ressort des indications figurant dans le dossier dont dispose la Cour que l'utilisation des données PNR permet d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité et qui devraient être soumises à un examen plus approfondi, de sorte qu'une telle législation paraît appropriée pour atteindre l'objectif de lutte contre les infractions terroristes et les formes graves de criminalité recherché.

285. En ce qui concerne le caractère nécessaire d'une telle législation, l'exercice par les États membres de la faculté prévue à l'article 2, paragraphe 1, de la directive PNR, lu à la lumière des articles 7 et 8 de la Charte, doit se limiter à ce qui est strictement nécessaire à la réalisation de cet objectif au regard des exigences visées aux points 163 à 174 du présent arrêt.

286. Ces exigences s'appliquent, à plus forte raison, dans le cas où le système prévu par la directive PNR est appliqué à d'autres moyens de transports intérieurs à l'Union ».

B.77.5. Comme la Cour l'a jugé en B.40, la réalité de la menace terroriste, au regard notamment de la situation géographique du pays, justifie l'application du système PNR à différents moyens de transport à l'intérieur des frontières de l'Union.

Pour les mêmes motifs, il y a lieu de considérer que la restriction de la liberté de circulation qu'emporterait la loi du 25 décembre 2016 est justifiée par le fait que le système PNR, appliqué aux vols intra-UE et étendu à d'autres moyens de transport, participe à l'objectif de lutte contre les infractions terroristes et les formes graves de criminalité que poursuit la directive PNR et qui est indubitablement un objectif d'intérêt général de l'Union, et que ce système PNR n'excède pas les limites du strict nécessaire.

B.77.6. Le moyen, en ce qu'il est dirigé contre l'article 3, § 1er, de la loi du 25 décembre 2016, n'est pas fondé.

B.78.1. 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.78.2.1. Interrogée par la Cour sur le champ d'application de la directive « API », la Cour de justice a jugé, par son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité :

« 263. Par sa neuvième question, sous *a)*, la juridiction de renvoi s'interroge, en substance, sur la validité de la directive API au regard de l'article 3, paragraphe 2, TUE et de l'article 45 de la Charte, en partant de la prémisse que les obligations que cette directive institue s'appliquent aux vols intra-UE.

264. Or, ainsi que l'a relevé M. l'avocat général au point 277 de ses conclusions et comme l'ont fait observer le Conseil, la Commission et plusieurs gouvernements, cette prémisse est erronée.

265. En effet, l'article 3, paragraphe 1, de la directive API prévoit que les États membres doivent prendre les mesures nécessaires afin d'établir l'obligation, pour les transporteurs, de transmettre, à la demande des autorités chargées du contrôle des personnes aux frontières extérieures, avant la fin de l'enregistrement, les renseignements relatifs aux passagers qu'ils vont transporter vers un point de passage frontalier autorisé par lequel ces personnes entreront sur le territoire d'un État membre. Ces données sont transmises, selon l'article 6, paragraphe 1, de ladite directive, aux autorités chargées d'effectuer le contrôle aux frontières extérieures par lesquelles le passager entrera sur ce territoire et font l'objet d'un traitement dans les conditions prévues à cette dernière disposition.

266. Or, il ressort clairement de ces dispositions, lues à la lumière de l'article 2, sous *a)*, *b)* et *d)*, de la directive API, où sont définies les notions respectivement de ' transporteur ', de ' frontières extérieures ' et de ' point de passage frontalier ', que cette directive n'impose l'obligation, pour les transporteurs aériens, de transmettre les données visées à son article 3, paragraphe 2, aux autorités chargées des contrôles aux frontières extérieures que dans le cas des vols acheminant des passagers vers un point de passage autorisé pour le franchissement des frontières extérieures des États membres avec des pays tiers et prévoit seulement le traitement des données relatives à ces vols.

267. En revanche, ladite directive n'impose aucune obligation concernant les données des passagers voyageant sur des vols ne franchissant que des frontières intérieures entre les États membres.

268. Il convient d'ajouter que la directive PNR, en incluant au nombre des données PNR, ainsi qu'il ressort de son considérant 9 et de son article 8, paragraphe 2, les données visées à l'article 3, paragraphe 2, de la directive API recueillies conformément à cette directive et conservées par certains transporteurs aériens, et en conférant aux États membres la faculté d'appliquer la directive PNR, en vertu de son article 2, aux vols intra-UE qu'ils définissent, n'a modifié ni la portée des dispositions de la directive API ni les limitations résultant de cette directive.

269. Eu égard à ce qui précède, il y a lieu de répondre à la neuvième question, sous a), que la directive API doit être interprétée en ce sens qu'elle ne s'applique pas aux vols intra-UE ».

B.78.2.2. Il ressort de ce qui précède que la Cour de justice confirme que le fait pour la directive PNR d'inclure au nombre des données PNR les données API ne modifie ni la portée des dispositions de la directive API ni les limitations résultant de cette directive, laquelle doit être interprétée en ce sens qu'elle ne s'applique pas aux vols intra-UE (points 268-269). Comme il est dit en B.54.2, la Cour de justice juge en effet que le traitement des données API ne peut concerner que des passagers qui franchissent les frontières extérieures de l'Union avec des pays tiers, sous peine d'avoir un effet équivalent aux contrôles effectués aux frontières extérieures avec des pays tiers (point 290).

B.78.3. Il convient par ailleurs de tenir compte du point 235 de l'arrêt *en cause de Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, par lequel la Cour de justice juge que « le caractère exhaustif des finalités visées à l'article 1er, paragraphe 2, de la directive PNR implique également que les données PNR ne sauraient être conservées dans une base de données unique pouvant être consultée aux fins de la poursuite tant de ces finalités que d'autres finalités. En effet, la conservation de ces données dans une telle base de données comporterait le risque que lesdites données soient utilisées à des fins autres que celles visées à cet article 1er, paragraphe 2 ».

C’est d’ailleurs en se fondant sur l’incompatibilité d’une base de données unique avec les exigences du strict nécessaire que la Cour de justice a jugé, comme il est dit en B.54.2, que le traitement des données PNR à des fins autres que celles prévues par la directive PNR, notamment aux fins de l’amélioration des contrôles aux frontières et de la lutte contre l’immigration clandestine, méconnaît le caractère exhaustif de l’énumération des objectifs poursuivis par le traitement des données PNR (point 288), lequel empêche les États membres de créer une base de données unique contenant tant les données PNR recueillies au titre de la directive PNR que les données visées à l’article 3, paragraphe 2, de la directive API, notamment lorsque cette base de données peut être consultée aux fins de la poursuite non seulement des finalités visées à l’article 1er, paragraphe 2, de la directive PNR, mais également d’autres finalités (point 289).

B.78.4. Au regard de l’existence d’une base de données unique contenant tant les données PNR que les données API, il n’est pas possible d’interpréter le champ d’application des articles 28 à 31 de la loi du 25 décembre 2016 d’une manière qui soit compatible avec le droit de l’Union.

B.78.5. En autorisant, dans le cadre du système PNR, le traitement des données API, visées à l’article 9, § 1er, 18°, de la loi du 25 décembre 2016, pour des vols intra-UE, les articles 28 à 31, qui composent le chapitre 11, de la loi du 25 décembre 2016, méconnaissent les dispositions visées au moyen et doivent être annulés. L’article 8, § 2, de la loi du 25 décembre 2016, qui est indissociablement lié à ces dispositions, doit également être annulé.

B.78.6. Il appartient au législateur d’organiser la collecte des données API dans une banque de données distincte de la banque de données PNR et selon les conditions qui respectent les finalités, les limitations et le champ d’application des obligations découlant de la directive API.

B.79. Le moyen, en ce qu’il est dirigé contre les articles 8, § 2, et 28 à 31 de la loi du 25 décembre 2016, est fondé.

Quant à la portée de l'annulation

B.80.1. La Cour a jugé les moyens fondés en ce qu'ils visent :

- l'article 8, § 1er, 4°, et l'article 8, § 2, de la loi du 25 décembre 2016;

- l'article 27 de la loi du 25 décembre 2016, en ce qu'il ne subordonne pas, sauf en cas d'urgence dûment justifiée, la communication des données PNR aux fins d'une évaluation ultérieure, à un contrôle préalable effectué soit par une juridiction soit par une « autorité administrative indépendante », sur demande motivée des autorités compétentes;

- les articles 28 à 31 de la loi du 25 décembre 2016 et

- l'article 51 de la loi du 25 décembre 2016.

B.80.2. Il y a par conséquent lieu d'annuler les dispositions précitées, dans la mesure du caractère fondé des moyens.

B.81.1. Cette annulation a pour conséquence que les dispositions de la loi du 25 décembre 2016 ou d'autres dispositions légales qui renverraient aux dispositions annulées perdent, dans cette mesure, leur objet.

B.81.2. Cette annulation a également pour conséquence que les traitements des données qui ont été effectués sur la base des finalités annulées ou les communications de données effectuées sans contrôle préalable doivent être considérés comme illégaux.

L'identification des traitements illégaux est possible dès lors que l'article 23, § 1er, de la loi du 25 décembre 2016 prévoit une « journalisation » définie à l'article 4, 11°, de la même loi comme étant « le mécanisme visé à l'article 23, § 2, permettant le traçage des traitements de données effectués afin qu'il soit possible d'identifier la personne qui a consulté des données, les données consultées, le moment et la finalité de cette consultation ».

Cette journalisation permet ainsi d'identifier les traitements qui excéderaient le « strict nécessaire ».

B.81.3. Pour le surplus, cette annulation partielle de la loi du 25 décembre 2016 n'affecte pas les autres traitements de données des passagers.

Quant au maintien des effets

B.82.1. L'article 8, alinéa 3, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle dispose :

« Si la Cour l'estime nécessaire, elle indique, par voie de disposition générale, ceux des effets des dispositions annulées qui doivent être considérés comme définitifs ou maintenus provisoirement pour le délai qu'elle détermine ».

B.82.2. En la matière, la Cour doit tenir compte des limitations qui découlent du droit de l'Union européenne quant au maintien des effets des normes nationales qui doivent être annulées parce qu'elles sont contraires à ce droit (CJUE, grande chambre, 8 septembre 2010, C-409/06, *Winner Wetten*, ECLI:EU:C:2010:503, points 53-69; CJUE, grande chambre, 28 février 2012, C-41/11, *Inter-Environnement Wallonie et Terre wallonne*, ECLI:EU:C:2012:103, points 56-63).

En règle générale, ce maintien des effets ne peut avoir lieu qu'aux conditions qui sont fixées par la Cour de justice en réponse à une question préjudicielle.

B.83.1. Interrogée par la Cour quant à un éventuel maintien des effets de la loi attaquée, la Cour de justice, par son arrêt en cause de *Ligue des droits humains c. Conseil des ministres* du 21 juin 2022, précité, a jugé :

« 293. Le principe de primauté du droit de l'Union consacre la prééminence du droit de l'Union sur le droit des États membres. Ce principe impose dès lors à toutes les instances des États membres de donner leur plein effet aux différentes dispositions du droit de l'Union, le droit des États membres ne pouvant affecter l'effet reconnu à ces dispositions sur le territoire desdits États. En vertu de ce principe, à défaut de pouvoir procéder à une interprétation de la législation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation

d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel (arrêts du 15 juillet 1964, Costa, 6/64, EU:C:1964:66, p. 1159 et 1160; du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 214 et 215, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 118).

294. Seule la Cour peut, à titre exceptionnel et pour des considérations impérieuses de sécurité juridique, accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci. Une telle limitation dans le temps des effets de l'interprétation de ce droit donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée. Il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 119 ainsi que jurisprudence citée).

295. Contrairement à l'omission d'une obligation procédurale telle que l'évaluation préalable des incidences d'un projet sur l'environnement, en cause dans l'affaire ayant donné lieu à l'arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen (C-411/17, EU:C:2019:622, points 175, 176, 179 et 181), dans lequel la Cour a accepté une suspension provisoire de cet effet d'éviction, une méconnaissance des dispositions de la directive PNR, lue à la lumière des articles 7, 8 et 45 ainsi que de l'article 52, paragraphe 1, de la Charte, ne saurait faire l'objet d'une régularisation par voie d'une procédure comparable à celle admise dans cette affaire. En effet, le maintien des effets d'une législation nationale, telle que la loi du 25 décembre 2016, signifierait que cette législation continue à imposer aux transporteurs aériens comme à d'autres transporteurs et aux opérateurs de voyage des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été transférées, conservées et traitées ainsi que des restrictions à la liberté de circulation de ces personnes allant au-delà de ce qui est nécessaire (voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 122 et jurisprudence citée).

296. Partant, la juridiction de renvoi ne saurait limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu du droit national, quant à la législation nationale en cause au principal (voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 123 et jurisprudence citée).

297. Enfin, pour autant que la juridiction de renvoi s'interroge sur l'incidence du constat de l'éventuelle incompatibilité de la loi du 25 décembre 2016 avec les dispositions de la directive PNR, lue à la lumière de la Charte, sur la recevabilité et l'exploitation des éléments de preuve et des informations obtenus au moyen des données transférées par les transporteurs et les opérateurs de voyage concernés dans le cadre de procédures pénales, il suffit de renvoyer à la jurisprudence de la Cour y afférente, en particulier aux principes rappelés aux points 41 à 44 de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), dont il découle que cette recevabilité relève, conformément au principe d'autonomie procédurale des États membres, du

droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité (voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 127).

298. Eu égard aux considérations qui précèdent, il convient de répondre à la dixième question que le droit de l'Union doit être interprété en ce sens qu'il s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'illégalité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux transporteurs aériens, ferroviaires et terrestres ainsi qu'aux opérateurs de voyage, le transfert des données PNR et prévoyant un traitement et une conservation de ces données incompatibles avec les dispositions de la directive PNR, lues à la lumière de l'article 3, paragraphe 2, TUE, de l'article 67, paragraphe 2, TFUE, des articles 7, 8 et 45 ainsi que de l'article 52, paragraphe 1, de la Charte. La recevabilité des éléments de preuve obtenus par ce moyen relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité ».

B.83.2. Il ressort de l'arrêt précité que la Cour ne peut maintenir provisoirement les effets des dispositions annulées.

Comme il est dit en B.81, cette annulation limitée ne remet pas en cause les traitements qui ont été effectués conformément aux dispositions constitutionnelles et conventionnelles invoquées dans les moyens.

B.83.3. Il appartient au juge pénal compétent de statuer, le cas échéant, sur l'admissibilité des preuves qui ont été recueillies lors de la mise en œuvre des dispositions annulées, conformément à l'article 32 du titre préliminaire du Code de procédure pénale et à la lumière des précisions apportées par la Cour de justice dans l'arrêt du 21 juin 2022 précité.

Par ces motifs,

la Cour

- annule l'article 8, § 1er, 4°, et § 2, de la loi du 25 décembre 2016 « relative au traitement des données des passagers »;

- annule l'article 27 de la loi du 25 décembre 2016 précitée, en ce qu'il ne subordonne pas, sauf en cas d'urgence dûment justifiée, la communication des données PNR aux fins d'une évaluation ultérieure à un contrôle préalable effectué soit par une juridiction soit par une autorité administrative indépendante, sur demande motivée des autorités compétentes;

- annule les articles 28 à 31 de la loi du 25 décembre 2016 précitée;

- annule l'article 16/3 de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité », tel qu'il a été inséré par l'article 51 de la loi du 25 décembre 2016 précitée;

- sous réserve des interprétations mentionnées en B.33.2 à B.33.5, B.49, B.63.2.3, B.63.3.2, B.63.4.1, B.69.1 et B.74.1, et compte tenu de ce qui est dit en B.40.3.2, en B.40.3.3 et en B.61.2.2, rejette le recours pour le surplus.

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 12 octobre 2023.

Le greffier, Le président,

F. Meersschaut P. Nihoul