LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

COUR CONSTITUTIONNELLE

[C − 2023/46645]

Extrait de l'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.

(...)

II. *En droit*

(...)

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, *Tele*2 *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, *Tele*2 *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, *Tele*2 *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'État, 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 nº 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 « TRÈS 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

GRONDWETTELIJK HOF

[C − 2023/46645]

Uittreksel uit arrest nr. 131/2023 van 12 oktober 2023

Rolnummer 6713

In zake : het beroep tot gehele of gedeeltelijke vernietiging van de wet van 25 december 2016 « betreffende de verwerking van passagiersgegevens », ingesteld door de vzw « Ligue des Droits de l'Homme » (thans « Ligue des droits humains »).

Het Grondwettelijk Hof,

samengesteld uit voorzitter P. Nihoul, rechter J. Moerman, waarnemend voorzitster, en de rechters T. Giet, M. Pâques, Y. Kherbache, D. Pieters, S. de Bethune, E. Bribosia, W. Verrijdt en K. Jadin, bijgestaan door de griffier F. Meersschaut, onder voorzitterschap van voorzitter P. Nihoul,

wijst na beraad het volgende arrest :

I. *Onderwerp van het beroep en rechtspleging*

Bij verzoekschrift dat aan het Hof is toegezonden bij op 24 juli 2017 ter post aangetekende brief en ter griffie is ingekomen op 26 juli 2017, heeft de vzw « Ligue des Droits de l'Homme » (thans « Ligue des droits humains »), bijgestaan en vertegenwoordigd door Mr. C. Forget, advocaat bij de balie te Brussel, beroep tot gehele of gedeeltelijke (artikelen 3, § 1, en 8, § 2, en hoofdstuk 11) vernietiging ingesteld van de wet van 25 december 2016 « betreffende de verwerking van passagiersgegevens » (bekendgemaakt in het *Belgisch Staatsblad* van 25 januari 2017).

Bij tussenarrest nr. 135/2019 van 17 oktober 2019 (ECLI:BE:GHCC:2019:ARR.135), bekendgemaakt in het *Belgisch Staatsblad* van 6 maart 2020, heeft het Hof de volgende prejudiciële vragen gesteld aan het Hof van Justitie van de Europese Unie :

« 1. Dient artikel 23 van de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 ' betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG ' (Algemene verordening gegevens — AVG), in samenhang gelezen met artikel 2, lid 2, *d)*, van die verordening, in die zin te worden geïnterpreteerd dat het van toepassing is op een nationale wetgeving zoals de wet van 25 december 2016 ' betreffende de verwerking van passagiersgegevens ', die niet enkel de richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 ' over het gebruik van persoonsgegevens van passagiers (PNR–gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit ' omzet, alsook de richtlijn 2004/82/EG van de Raad van 29 april 2004 ' betreffende de verplichting voor vervoerders om passagiersgegevens door te geven ' en de richtlijn 2010/65/EU van het Europees Parlement en de Raad van 20 oktober 2010 ' betreffende meldingsformaliteiten voor schepen die aankomen in en/of vertrekken uit havens van de lidstaten en tot intrekking van Richtlijn 2002/6/EG ' ?

2. Is bijlage I van de richtlijn (EU) 2016/681 bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin dat de erin opgesomde gegevens zeer ruim zijn — onder meer de gegevens die worden beoogd in punt 18 van bijlage I van de richtlijn (EU) 2016/681, die verder gaan dan de gegevens beoogd in artikel 3, lid 2, van de richtlijn 2004/82/EG — en doordat die gegevens, in hun geheel beschouwd, gevoelige gegevens zouden kunnen onthullen, en aldus de grenzen van het ' strikt noodzakelijke ' zou kunnen overschrijden ?

3. Zijn de punten 12 en 18 van bijlage I bij de richtlijn (EU) 2016/681 bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in zoverre, rekening houdend met de bewoordingen ' onder meer ' en ' met inbegrip van ', de erin beoogde gegevens bij wijze van voorbeeld en niet exhaustief worden vermeld, zodat de vereiste van nauwkeurigheid en duidelijkheid van de regels die leiden tot een inmenging in het recht op eerbiediging van het privéleven en in het recht op bescherming van de persoonsgegevens niet in acht zou zijn genomen ?

4. Zijn artikel 3, punt 4, van de richtlijn 2016/681/EU en bijlage I bij dezelfde richtlijn bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in zoverre het systeem van het algemeen verzamelen, doorgeven en verwerken van passagiersgegevens dat die bepalingen instellen, iedere persoon beoogt die het desbetreffende vervoersmiddel gebruikt, los van elk objectief element dat het mogelijk maakt ervan uit te gaan dat die persoon een risico voor de openbare veiligheid kan vormen ?

5. Dient artikel 6 van de richtlijn (EU) 2016/681, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus te worden uitgelegd dat het zich verzet tegen een nationale wetgeving zoals de bestreden wet, die, als doel van de ' PNR–gegevensverwerking ', het toezien op door de inlichtingen– en veiligheidsdiensten beoogde activiteiten aanvaardt, waarbij het dat doel aldus opneemt in het voorkomen, het opsporen, het onderzoeken en het vervolgen van terroristische misdrijven en ernstige criminaliteit ?

6. Is artikel 6 van de richtlijn (EU) 2016/681 bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in zoverre de voorafgaande beoordeling die daarin wordt geregeld, door een correlatie met de gegevensbanken en de vooraf bepaalde criteria, stelselmatig en op algemene wijze van toepassing is op de passagiersgegevens, los van elk objectief element dat toelaat ervan uit te gaan dat die passagiers een risico kunnen vormen voor de openbare veiligheid ?

7. Kan het begrip ' andere bevoegde nationale instantie ' bepaald in artikel 12, lid 3, van de richtlijn (EU) 2016/681 zo worden geïnterpreteerd dat het de PIE beoogt die bij de wet van 25 december 2016 is opgericht en die derhalve de toegang tot de ' PNR–gegevens ', na een termijn van zes maanden, in het kader van de gerichte opzoekingen zou kunnen toestaan ?

8. Dient artikel 12 van de richtlijn (EU) 2016/681, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zo te worden geïnterpreteerd dat het zich verzet tegen een nationale wetgeving zoals de bestreden wet die voorziet in een algemene bewaartermijn van de gegevens van vijf jaar, zonder onderscheid of de betrokken passagiers, in het kader van de voorafgaande beoordeling, al dan niet een risico kunnen vormen voor de openbare veiligheid ?

9. *a)* Is de richtlijn 2004/82/EG bestaanbaar met artikel 3, lid 2, van het Verdrag betreffende de Europese Unie en met artikel 45 van het Handvest van de grondrechten van de Europese Unie, in zoverre de daarbij ingevoerde verplichtingen van toepassing zijn op de vluchten binnen de Europese Unie ?

b) Dient de richtlijn 2004/82/EG, in samenhang gelezen met artikel 3, lid 2, van het Verdrag betreffende de Europese Unie en met artikel 45 van het Verdrag betreffende de grondrechten van de Europese Unie, zo te worden geïnterpreteerd dat zij zich verzet tegen een nationale wetgeving zoals de bestreden wet die, met het oog op de strijd tegen illegale immigratie en het verbeteren van de grenscontroles, een systeem toestaat voor de verzameling en verwerking van de passagiersgegevens ' van, naar en op doorreis over het nationaal grondgebied ', hetgeen indirect een herinvoering van de controles aan de binnengrenzen zou kunnen impliceren ?

10. Zou het Grondwettelijk Hof, indien het op grond van de antwoorden op de hiervoor weergegeven prejudiciële vragen, tot de conclusie zou komen dat de bestreden wet, die met name de richtlijn (EU) 2016/681 omzet, één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van de wet van 25 december 2016 ' betreffende de verwerking van passagiersgegevens ' tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen worden gebruikt voor de door de wet beoogde doelstellingen ? ».

Bij arrest van 21 juni 2022 in de zaak C—817/19 (ECLI:EU:C:2022:491) heeft het Hof van Justitie van de Europese Unie op de vragen geantwoord.

Bij beschikking van 13 juli 2022 heeft het Hof, na de rechters–verslaggevers T. Giet en W. Verrijdt te hebben gehoord, beslist :

- de debatten te heropenen,

- de partijen uit te nodigen, in een uiterlijk op 30 september 2022 in te dienen aanvullende memorie, waarvan ze binnen dezelfde termijn een kopie laten toekomen aan de andere partijen, hun standpunt mee te delen over de weerslag van het voormelde arrest van het Hof van Justitie van de Europese Unie op het beroep tot vernietiging, meer bepaald :

a) wat betreft de gevolgen, voor de voortzetting van het onderzoek van het beroep tot vernietiging voor het Hof, van de overwegingen met betrekking tot onder meer :

- de samenhang tussen de PNR–richtlijn en de AVG;

- het toepassingsgebied van het verzamelen en het verwerken van de PNR–gegevens (geïdentificeerde gegevens, doeleinden en beoogde misdrijven, betrokken vluchten);

- de waarborgen met betrekking tot de verwerking van de PNR–gegevens (voorafgaande beoordeling, geautomatiseerde verwerking, toegang tot de PNR–gegevens, begrip « onafhankelijke nationale autoriteit », bewaartermijn van de PNR–gegevens);

- de onmogelijkheid om de gevolgen te handhaven in geval van gedeeltelijke vernietiging van de wet van 25 december 2016 « betreffende de verwerking van passagiersgegevens »;

b) wat betreft de verantwoordingen en voorwaarden, die concreet onderbouwd zijn, in verband met het tot het « strikt noodzakelijke » beperkte karakter en de overeenstemming met de interpretatie van de PNR–richtlijn van elk van de hiervoor aangegeven elementen, zoals die te dezen zijn bepaald in de wet van 25 december 2016 « betreffende de verwerking van passagiersgegevens »;

- dat geen terechtzitting zal worden gehouden, tenzij een partij binnen zeven dagen na ontvangst van de kennisgeving van die beschikking een verzoek heeft ingediend om te worden gehoord, en

- dat, behoudens zulk een verzoek, de debatten zullen worden gesloten op 5 oktober 2022 en de zaak in beraad zal worden genomen.

(...)

II. *In rechte*

(...)

Ten aanzien van de bestreden wet en de context ervan

B.1. Het beroep tot vernietiging, ingesteld door de vzw « Ligue des Droits de l'Homme » (thans « Ligue des droits humains »), is gericht tegen de wet van 25 december 2016 « betreffende de verwerking van passagiersgegevens » (hierna : de wet van 25 december 2016), die de vervoerders en reisoperatoren de verplichting oplegt om de passagiersgegevens, de zogenoemde PNR-gegevens (*Passenger Name Record*) door te geven.

B.2.1. Overeenkomstig artikel 2 ervan, zet de wet van 25 december 2016 drie Europese richtlijnen om.

B.2.2. De wet van 25 december 2016 zet vooreerst de richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 « over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit » (hierna : de PNR-richtlijn) om.

De PNR-richtlijn voorziet in het verzamelen en doorgeven, door de luchtvaartmaatschappijen, van de persoonsgegevens van passagiers naar of vanuit derde landen om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen alsook te onderzoeken en te vervolgen. Die richtlijn is van toepassing op de verwerking van de PNR-gegevens betreffende de luchtvaart maar, overeenkomstig overweging 33 ervan, sluit zij voor de lidstaten niet de mogelijkheid uit om, krachtens hun nationaal recht, het PNR-mechanisme waarin zij voorziet uit te breiden tot andere vervoermiddelen of tot marktdeelnemers die geen luchtvaartmaatschappij zijn. Bovendien kan de PNR-richtlijn, overeenkomstig artikel 2 ervan, ook worden toegepast op vluchten binnen de EU.

B.2.3. De wet van 25 december 2016 zet eveneens de richtlijn 2004/82/EG van de Raad van 29 april 2004 « betreffende de verplichting voor vervoerders om passagiersgegevens door te geven » (hierna : de API-richtlijn) om.

Zij regelt dus het gebruik van passagiersgegevens voor de doelstellingen waarin de richtlijn 2004/82/EG voorziet, waarbij de inhoud van het koninklijk besluit van 11 december 2006 « betreffende de verplichting voor luchtvervoerders om passagiersgegevens door te geven » (hierna : het koninklijk besluit van 11 december 2006) wordt overgenomen.

B.2.4. De wet van 25 december 2016 zet ten slotte, gedeeltelijk, de richtlijn 2010/65/EU van het Europees Parlement en de Raad van 20 oktober 2010 « betreffende meldingsformaliteiten voor schepen die aankomen in en/of vertrekken uit havens van de lidstaten en tot intrekking van Richtlijn 2002/6/EG » (hierna : de richtlijn 2010/65/EU) om. Die richtlijn heeft tot doel de administratieve procedures die van toepassing zijn op het zeevervoer te vereenvoudigen en te harmoniseren door de algemene invoering van de elektronische overdracht van gegevens en door rationalisering van de meldingsformaliteiten (artikel 1, lid 1).

B.3.1. De wet van 25 december 2016 beoogt « een wettelijk kader te scheppen om de vervoerders van passagiers in verschillende internationale transportsectoren (luchtvervoer, treinverkeer, internationaal wegvervoer en maritiem transport), alsook reisoperatoren, te verplichten de gegevens van hun passagiers door te sturen naar een gegevensbank, beheerd door de FOD Binnenlandse Zaken » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, p. 6) :

« De verwerking van de passagiersgegevens, het vergelijken ervan met databanken en het aftoetsen ervan aan vooraf bepaalde criteria zijn noodzakelijk om deze modi operandi te ontdekken, om nieuwe trends en fenomenen in kaart te brengen, maar ook om te bepalen welke passagiers aan een nader onderzoek dienen onderworpen te worden, aangezien zij, op basis van het resultaat van de verwerking, kunnen betrokken zijn bij een terroristisch misdrijf, bij vormen van ernstige criminaliteit, bij inbreuken op de openbare orde in het kader van gewelddadige radicalisering en bij activiteiten die de fundamentele belangen van de Staat kunnen bedreigen

[...]

Als omzetting van de Europese Richtlijn over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige misdrijven, houdt dit voorontwerp van wet maximaal rekening met alle vastgelegde bepalingen op Europees niveau. Dit is essentieel om een doeltreffende mechanisme voor de verwerking van passagiersgegevens op te zetten dat streeft naar een maximale interoperabiliteit met de passagiers informatie eenheden van de andere lidstaten.

[...]

De analyse van de passagiersgegevens zal uitsluitend worden toevertrouwd aan een Passagiersinformatie-eenheid (PIE), die wordt opgericht binnen de FOD Binnenlandse Zaken en onder meer, onder het functioneel toezicht van een leidend ambtenaar van de PIE zal worden samengesteld uit gedetacheerden van de politiediensten, de Veiligheid van de Staat, de Algemene Directie Inlichtingen en Veiligheid en de Douane (wat betreft de Douane is de verwerking van de passagiersgegevens noodzakelijk met het oog op het opsporen en vervolgen van fraude zoals voorzien in bijlage 2, punt 7 van Richtlijn 2016/681) » (*ibid.*, pp. 5-6).

B.3.2. Het door de PNR-richtlijn ingevoerde systeem voor het verzamelen van gegevens vult het systeem voor het verzamelen van gegevens aan dat door de API-richtlijn werd gecreëerd, doordat PNR-gegevens ruimer zijn dan API-gegevens :

« De API-gegevens (*Advanced Passenger Information*), zijn authentieke gegevens. Ze zijn afkomstig uit authentieke documenten (o.a. uit de identiteitskaarten) en zijn voldoende accuraat om een persoon te identificeren. Dit betreffen de gegevens die doorgegeven worden in het kader van de check-in en het instappen. Bij de bestrijding van terrorisme en ernstige criminaliteit is de informatie in de API-gegevens voldoende om bekende terroristen en criminelen met behulp van waarschuwingssystemen te identificeren.

De PNR-gegevens, zijnde de reservatiegegevens, bevatten meer gegevenselementen en zijn sneller beschikbaar dan API-gegevens. Deze gegevenselementen vormen een zeer belangrijk instrument voor het uitvoeren van risicobeoordelingen van personen en het leggen van verbanden tussen bekende en onbekende personen. Ook voor de gerichte opzoekingen bieden de PNR gegevens een zeer belangrijke meerwaarde » (*ibid.*, p. 6-7).

B.3.3. De verplichting om passagiersgegevens door te sturen geldt « voor internationale vluchten, internationale hogesnelheidstreinen, geregeld internationaal busvervoer en maritiem transport zowel naar en vanuit de Europese Unie, als inkomend en uitgaand binnen de Europese Unie » (*ibid.*, p. 7), krachtens de mogelijkheid waarin artikel 2 van de PNR-richtlijn voorziet.

De wettelijke verplichting om passagiersgegevens door te sturen geldt overigens niet alleen voor de door de PNR-richtlijn beoogde luchtvaartmaatschappijen, maar ook voor de reisoperatoren, krachtens de door de PNR-richtlijn geboden mogelijkheid om die verplichting op te leggen aan marktdeelnemers die geen luchtvaartmaatschappij zijn (*ibid.*, p. 8).

B.4.1. Artikel 4, 9°, van de wet van 25 december 2016 definieert de « PNR » als « het bestand met de reisgegevens van iedere passagier, dat de in artikel 9 bedoelde informatie bevat, die de boekende en de deelnemende vervoerders en reisoperatoren nodig hebben om reserveringen te kunnen verwerken en controleren bij elke reis die door of namens iemand wordt geboekt; dit bestand kan zich bevinden in een reserveringssysteem, een vertrekcontrolesysteem (voor de controle van vertrekkende passagiers) of een soortgelijk systeem dat dezelfde functies vervult ».

Wat de gegevens van de *check-in*-status en het instappen betreft, zijn de voorafgaande gegevens (API-gegevens — *Advanced Passenger Information*) bedoeld in artikel 9, § 1, 18°, exhaustief opgesomd in de zestien punten van artikel 9, § 2, van de wet van 25 december 2016.

Wat de reservatiegegevens betreft, bevatten de passagiersgegevens (PNR–gegevens — *Passenger Name Record*) maximaal de negentien elementen die exhaustief zijn opgesomd in artikel 9, § 1, van de wet van 25 december 2016, waaronder de API-gegevens bedoeld in artikel 9, § 1, 18°.

B.4.2. Krachtens artikel 5 van de wet van 25 december 2016 worden de PNR-gegevens verzameld door de vervoerders en reisoperatoren en doorgestuurd met het oog op de registratie ervan in de passagiersgegevensbank bedoeld in artikel 15, die wordt beheerd door de « Passagiersinformatie-eenheid » (hierna : de PIE), die is opgericht binnen de Federale Overheidsdienst Binnenlandse Zaken (artikelen 12 en volgende). De passagiers worden geïnformeerd over het feit dat hun gegevens worden doorgestuurd naar de PIE en dat die gegevens achteraf kunnen worden verwerkt voor de in artikel 8 beoogde doelen (artikel 6).

De doeleinden van de verwerking van PNR-gegevens zijn opgesomd in artikel 8 van de wet van 25 december 2016 : het gaat, enerzijds, om het opsporen en vervolgen van misdrijven (artikel 8, § 1) en, anderzijds, onder de voorwaarden bepaald in hoofdstuk 11, om de verbetering van de controles van personen aan de buitengrenzen en de bestrijding van illegale immigratie (artikel 8, § 2).

In het kader van de doeleinden beoogd in artikel 8, § 1, bepaalt artikel 16 van de wet van 25 december 2016 dat de passagiersgegevensbank rechtstreeks toegankelijk is door de PIE voor de verwerkingen bedoeld in de artikelen 24 tot 27, overeenkomstig de bepalingen waarin hoofdstuk 9 voorziet.

In het kader van de in artikel 8, § 2 beoogde doeleinden worden enkel de in artikel 9, § 1, 18° (API-gegevens) bedoelde passagiersgegevens doorgegeven die betrekking hebben op de categorieën van passagiers die worden beoogd in artikel 29, § 2, van de wet van 25 december 2016.

De bewaartermijn van de gegevens is vastgesteld bij de artikelen 18 en volgende van de wet van 25 december 2016.

Ten aanzien van de omvang van het beroep

B.5.1. Het Hof dient de omvang van het beroep tot vernietiging te bepalen door zich te baseren op de inhoud van het verzoekschrift.

Het Hof kan slechts uitdrukkelijk bestreden wetskrachtige bepalingen vernietigen waartegen middelen worden aangevoerd en, in voorkomend geval, bepalingen die niet worden bestreden maar die onlosmakelijk zijn verbonden met de bepalingen die moeten worden vernietigd.

B.5.2. Hoewel de verzoekende partij, met haar eerste middel, de vernietiging vordert van de volledige wet van 25 december 2016, blijkt uit de uiteenzetting van het middel dat de grieven enkel gericht zijn tegen de artikelen 3, § 2, 4, 9° en 10°, 7 tot 9, 12 tot 16, 18, 24 tot 27, 50 en 51 van de wet van 25 december 2016. Bijgevolg is het beroep tot vernietiging slechts in die mate ontvankelijk.

Het tweede middel, dat in ondergeschikte orde wordt geformuleerd, is gericht tegen de artikelen 3, § 1, 8, § 2, en tegen hoofdstuk 11, dat de artikelen 28 tot 31, van de wet van 25 december 2016 bevat.

B.5.3. Wanneer evenwel uit het nader onderzoek van de middelen zou blijken dat enkel bepaalde onderdelen van de bestreden bepalingen worden bekritiseerd, zal het onderzoek in voorkomend geval tot die onderdelen worden beperkt.

B.6. De bestreden artikelen bepalen :

« HOOFDSTUK 2. - *Toepassingsgebied*

Art. 3. § 1. Deze wet bepaalt de verplichtingen van de vervoerders en de reisoperatoren inzake de doorgifte van gegevens van passagiers van, naar en op doorreis over het nationaal grondgebied.

§ 2. De Koning bepaalt bij een in Ministerraad overlegd besluit, per vervoerssector en voor de reisoperatoren, de passagiersgegevens die moeten worden doorgestuurd en de nadere regels voor het doorsturen, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

HOOFDSTUK 3. - *Definities*

Art. 4. Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder :

[...]

9° ' PNR ' : het bestand met de reisgegevens van iedere passagier, dat de in artikel 9 bedoelde informatie bevat, die de boekende en de deelnemende vervoerders en reisoperatoren nodig hebben om reserveringen te kunnen verwerken en controleren bij elke reis die door of namens iemand wordt geboekt; dit bestand kan zich bevinden in een reserveringssysteem, een vertrekcontrolesysteem (voor de controle van vertrekkende passagiers) of een soortgelijk systeem dat dezelfde functies vervult;

10° ' passagier ' : iedere persoon, met inbegrip van de transferpassagiers en transitpassagiers en met uitsluiting van de bemanningsleden, die wordt vervoerd of moet worden vervoerd door een vervoerder, met de toestemming van deze laatste, wat zich vertaalt door de inschrijving van deze persoon op de passagierslijst;

[...]

HOOFDSTUK 4. - *Verplichtingen van de vervoerders en reisoperatoren*

[...]

Art. 7. § 1. De vervoerders sturen de passagiersgegevens bedoeld in artikel 9, § 1, waarover zij beschikken, door en verzekeren zich ervan dat de passagiersgegevens bedoeld in artikel 9, § 1, 18°, waarover zij beschikken, volledig, juist en actueel zijn. Hiervoor controleren zij de overeenstemming tussen de reisdocumenten en de identiteit van de betrokken passagier.

§ 2. De reisoperatoren sturen de passagiersgegevens bedoeld in artikel 9, § 1, waarover zij beschikken, door en verzekeren zich ervan dat de passagiersgegevens bedoeld in artikel 9, § 1, 18°, waarover zij beschikken, volledig, juist en actueel zijn. Hiervoor nemen ze alle noodzakelijke maatregelen om de overeenstemming tussen de reisdocumenten en de identiteit van de betrokken passagier te controleren.

§ 3. De Koning bepaalt bij een in Ministerraad overlegd besluit, per vervoerssector en voor de reisoperatoren, de nadere regels met betrekking tot de verplichting bepaald in §§ 1 en 2.

HOOFDSTUK 5. - *Doelen van de gegevensverwerking*

Art. 8. § 1. De passagiersgegevens worden verwerkt met het oog op :

1° het opsporen en vervolgen, met inbegrip van de uitvoering van straffen of vrijheidsbeperkende maatregelen, met betrekking tot misdrijven bedoeld in artikel 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° en § 3, van het Wetboek van Strafvordering;

2° het opsporen en vervolgen, met inbegrip van de uitvoering van straffen of vrijheidsbeperkende maatregelen, met betrekking tot misdrijven bedoeld in de artikelen 196, voor wat betreft valsheid in authentieke en openbare geschriften, 198, 199, 199*bis*, 207, 213, 375 en 505 van het Strafwetboek;

3° de preventie van ernstige inbreuken op de openbare veiligheid in het kader van gewelddadige radicalisering door het toezien op fenomenen en groeperingen overeenkomstig artikel 44/5, § 1, 2° en 3° en § 2, van de wet van 5 augustus 1992 op het politieambt;

4° het toezien op activiteiten bedoeld in de artikelen 7, 1° en 3°/1, en 11, § 1, 1° tot 3° en 5°, van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst;

5° het opsporen en vervolgen met betrekking tot de misdrijven bedoeld in artikel 220, § 2, van de algemene wet van 18 juli 1977 inzake douane en accijnzen en artikel 45, derde lid, van de wet van 22 december 2009 betreffende de algemene regeling inzake accijnzen.

§ 2. Onder de voorwaarden bepaald in hoofdstuk 11, worden de passagiersgegevens eveneens verwerkt ter verbetering van de controles van personen aan de buitengrenzen en ter bestrijding van illegale immigratie.

HOOFDSTUK 6. - *Passagiersgegevens*

Art. 9. § 1. Wat de reservatiegegevens betreft, bevatten de passagiersgegevens maximaal :

1° de PNR-bestandslocatiecode;

2° de datum van reservering en afgifte van het biljet;

3° de geplande reisdata;

4° de namen, voornamen en geboortedatum;

5° het adres en de contactgegevens (telefoonnummer, e-mailadres);

6° de betalingsinformatie, met inbegrip van het factureringsadres;

7° de volledige reisroute voor de betrokken passagier;

8° de informatie over de ' geregistreerde reizigers ', met name de reizigers die gebruikmaken van een loyauteitsprogramma voor frequent reizen;

9° het reisbureau of de reisagent;

10° de status van de reiziger, met inbegrip van de bevestigingen, *check-in*-status, no-*show*- of *go-show*-informatie;

11° de aanwijzingen over de opgesplitste of opgedeelde PNR-informatie;

12° de algemene opmerkingen, met inbegrip van alle beschikbare informatie over de niet-begeleide minderjarigen onder 18 jaar, zoals de naam en het geslacht van de minderjarige, zijn leeftijd, de taal/talen die hij spreekt, de naam en de contactgegevens van de voogd die de minderjarige begeleidt bij het vertrek en de aard van zijn relatie met de minderjarige, de naam en de contactgegevens van de voogd aanwezig bij de aankomst en de aard van zijn relatie met de minderjarige, de ambtenaar die bij het vertrek en de aankomst aanwezig is;

13° de informatie betreffende de biljetuitgifte, waaronder het biljetnummer, de uitgiftedatum, de biljetten voor enkele reizen en de geautomatiseerde prijsnotering van de biljetten;

14° het zitplaatsnummer en andere informatie over de zitplaats;

15° de informatie over gezamenlijke vluchtnummers;

16° alle bagage-informatie;

17° het aantal en de namen van de andere reizigers in het PNR;

18° alle voorafgaande passagiersgegevens (API-gegevens) die werden verzameld en worden opgesomd in § 2;

19° alle vroegere wijzigingen van de onder 1° tot 18° opgesomde gegevens;

§ 2. Wat de gegevens van de check-in-status en het instappen betreft, zijn de voorafgaande gegevens bedoeld in § 1, 18°, de volgende :

1° soort reisdocument;

2° nummer van het document;

3° nationaliteit;

4° land van afgifte van het document;

5° vervaldatum van het document;

6° familienaam, voornaam, geslacht, geboortedatum;

7° vervoerder/reisoperator;

8° nummer van het vervoer;

9° datum van vertrek, datum van aankomst;

10° plaats van vertrek, plaats van aankomst;

11° tijdstip van vertrek, tijdstip van aankomst;

12° totaal aantal vervoerde personen;

13° zitplaatsnummer;

14° PNR-bestandslocatiecode;

15° aantal, gewicht en identificatie van de bagagestukken;

16° grensdoorlaatpost van binnenkomst op het nationaal grondgebied.

[...]

HOOFDSTUK 7. - *De Passagiersinformatie-eenheid*

Art. 12. Binnen de Federale Overheidsdienst Binnenlandse Zaken wordt een Passagiersinformatie-eenheid opgericht.

Art. 13. § 1. De PIE is belast met :

1° het verzamelen, het bewaren en het verwerken van de passagiersgegevens die door de vervoerders en reisoperatoren zijn doorgestuurd, evenals met het beheer van de passagiersgegevensbank;

2° de uitwisseling met de PIE's van andere lidstaten van de Europese Unie, met Europol, en met derde landen van zowel de passagiersgegevens als de resultaten van hun verwerking, overeenkomstig hoofdstuk 12.

§ 2. Onverminderd andere wettelijke bepalingen, mag de PIE de gegevens die krachtens hoofdstuk 9 zijn bewaard, niet voor andere dan de in artikel 8 bedoelde doelen gebruiken.

Art. 14. § 1. De PIE is samengesteld uit :

1° een leidend ambtenaar, bijgestaan door een ondersteunende dienst. Deze is verantwoordelijk voor :

a) de organisatie en de werking van de PIE;

b) het toezicht op de naleving door de vervoerders en de reisoperatoren van hun verplichtingen bepaald in hoofdstuk 4;

c) het beheer en het gebruik van de passagiersgegevensbank;

d) de verwerking van de passagiersgegevens;

e) de naleving van de wettigheid en de regelmatigheid van de in hoofdstuk 10 bedoelde verwerkingen;

f) de ondersteuning van de bevoegde diensten voor de uitoefening van hun bevoegdheden binnen de PIE.

2° uit de volgende bevoegde diensten gedetacheerde leden :

a) de politiediensten, bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

b) de Veiligheid van de Staat, bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst;

c) de Algemene Inlichtingen– en Veiligheidsdienst, bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst;

d) de Administratie Onderzoek en Opsporing en de Administratie Toezicht, Controle en Vaststelling van de Algemene Administratie van de Douane en Accijnzen, bedoeld in het besluit van de Voorzitter van het Directiecomité van 16 oktober 2014 tot oprichting van de nieuwe diensten van de Algemene Administratie van de Douane en Accijnzen.

De leden van de bevoegde diensten worden gedurende de periode van hun detachering onder het functioneel en hiërarchisch toezicht geplaatst van de leidend ambtenaar van de PIE. Zij behouden evenwel het statuut van hun oorspronkelijke dienst.

§ 2. Na overleg met de functionaris voor de gegevensbescherming en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, sluiten de leidend ambtenaar van de PIE en de bevoegde diensten het protocolakkoord bedoeld in artikel 17, teneinde de nadere regels te bepalen met betrekking tot de doorgifte van de gegevens. Het protocol vermeldt minstens de volgende garanties :

- de nadere regels met betrekking tot de uitwisseling van de gegevens;

- de door de wet bepaalde maximumtermijnen voor de verwerking van de gegevens;

- het informeren van de PIE door de bevoegde diensten over het gevolg gegeven aan de gevalideerde positieve overeenstemmingen.

§ 3. Overeenkomstig de wettelijke verplichtingen van iedere bevoegde dienst homologeert de Nationale Veiligheidsoverheid een beveiligd en gecodeerd communicatie– en informatiesysteem voor het automatisch versturen van de positieve overeenstemmingen.

§ 4. De Koning bepaalt bij een in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, de nadere regels voor de samenstelling en de organisatie van de PIE, het statuut van de leidend ambtenaar en de leden van de PIE, evenals de directies of afdelingen die binnen de bevoegde diensten instaan voor de verwerking van de passagiersgegevens.

HOOFDSTUK 8. - *De passagiersgegevensbank*

Art. 15. § 1. Er wordt een passagiersgegevensbank opgericht die door de Federale Overheidsdienst Binnenlandse Zaken wordt beheerd en waarin de passagiersgegevens worden geregistreerd.

§ 2. De leidend ambtenaar van de PIE is de verantwoordelijke voor de verwerking van de passagiersgegevensbank in de zin van artikel 1, § 4, van de wet tot bescherming van de persoonlijke levenssfeer.

§ 3. Het recht op toegang en rechtzetting inzake de passagiersgegevens, bepaald in respectievelijk de artikelen 10 en 12 van de wet tot bescherming van de persoonlijke levenssfeer, wordt rechtstreeks uitgeoefend bij de functionaris voor de gegevensbescherming.

In afwijking van het eerste lid worden deze rechten uitgeoefend bij de Commissie voor de bescherming van de persoonlijke levenssfeer voor de positieve overeenstemmingen en de resultaten van de gerichte opzoekingen bedoeld in de artikelen 24 tot 27.

§ 4. De verwerkingen van de passagiersgegevens uitgevoerd volgens deze wet worden onderworpen aan de wet bescherming van de persoonlijke levenssfeer met betrekking tot de verwerking van gegevens met een persoonlijk karakter. De Commissie voor de bescherming van de persoonlijke levenssfeer oefent haar bevoegdheden uit die de wet tot bescherming van de persoonlijke levenssfeer bepaalt.

Art. 16. In het kader van de doelen beoogd in artikel 8, § 1, is de passagiersgegevensbank rechtstreeks toegankelijk door de PIE voor de verwerkingen bedoeld in de artikelen 24 tot 27 volgens de in hoofdstuk 9 voorziene regels.

[...]

HOOFDSTUK 9. - *Bewaartermijnen*

Art. 18. De passagiersgegevens worden in de passagiersgegevensbank bewaard gedurende een maximale termijn van vijf jaar, te rekenen vanaf de registratie ervan. Aan het eind van deze termijn worden ze vernietigd.

[...]

HOOFDSTUK 10. - *De gegevensverwerking*

Afdeling 1. - De verwerking van passagiersgegevens in het kader van de voorafgaande beoordeling van de passagiers

Art. 24. § 1. De passagiersgegevens worden verwerkt met het oog op het uitvoeren van een voorafgaande beoordeling van de passagiers vóór hun geplande aankomst in, vertrek uit of doorreis over het nationaal grondgebied om te bepalen welke personen moeten worden onderworpen aan een nader onderzoek.

§ 2. In het kader van de doelen beoogd in artikel 8, § 1, 1°, 4° en 5°, of met betrekking tot de bedreigingen vermeld in de artikelen 8, 1°, *a)*, *b)*, *c)*, *d)*, *f)*, *g)* en 11, § 2, van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst, berust de voorafgaande beoordeling van de passagiers op een positieve overeenstemming, voortvloeiende uit een correlatie van de passagiersgegevens met :

1° de gegevensbanken die door de bevoegde diensten worden beheerd of die voor hen rechtstreeks beschikbaar of toegankelijk zijn in het kader van hun opdrachten of met lijsten van personen die worden opgesteld door de bevoegde diensten in het kader van hun opdrachten.

2° de door de PIE vooraf bepaalde beoordelingscriteria, bedoeld in artikel 25.

§ 3. In het kader van de doeleinden beoogd in artikel 8, § 1, 3°, berust de voorafgaande beoordeling van de passagiers op een positieve overeenstemming, voortvloeiende uit een correlatie van de passagiersgegevens met de gegevensbanken bedoeld in § 2, 1°.

§ 4. De positieve overeenstemming wordt gevalideerd door de PIE binnen de vierentwintig uur na ontvangst van het geautomatiseerd bericht van de positieve overeenstemming.

§ 5. Vanaf het moment van validatie geeft de bevoegde dienst die aan de basis ligt van de positieve overeenstemming een nuttig gevolg binnen de kortst mogelijke termijn.

Art. 25. § 1. De passagiersgegevens kunnen door de PIE worden gebruikt voor het bijstellen van bestaande criteria of het formuleren van nieuwe criteria die bestemd zijn om zich te richten op individuen bij de voorafgaande beoordelingen van de passagiers, bedoeld in artikel 24, § 2, 2°.

§ 2. Het beoordelen van de passagiers voor hun geplande aankomst, doorreis of vertrek op grond van vooraf bepaalde criteria wordt op niet-discriminerende wijze verricht. Deze criteria mogen niet gericht zijn op de identificatie van een individu en moeten doelgericht, evenredig en specifiek zijn.

§ 3. Deze criteria mogen niet gebaseerd zijn op gegevens die de raciale of etnische oorsprong van een persoon, zijn religieuze of levensbeschouwelijke overtuigingen, zijn politieke opvattingen, zijn vakbondslidmaatschap, zijn gezondheidstoestand, zijn seksleven of zijn seksuele geaardheid onthullen.

Art. 26. § 1. Voor het in artikel 8, § 1, 3°, bedoelde doel zullen enkel de passagiersgegevens bedoeld in artikel 9, § 1, 18° met betrekking tot de persoon of personen voor wie een positieve overeenstemming werd gegenereerd, toegankelijk zijn.

§ 2. Voor het doel beoogd in artikel 8, § 1, 1°, 4° en 5°, of met betrekking tot de bedreigingen vermeld in de artikelen 8, 1°, *a)*, *b)*, *c)*, *d)*, *f)*, *g)*, en 11, § 2, van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst, zijn alle passagiersgegevens bedoeld in artikel 9 toegankelijk.

Afdeling 2. - De verwerking van gegevens in het kader van gerichte opzoekingen

Art. 27. De passagiersgegevens worden gebruikt om gerichte opzoekingen te verrichten voor de doelen beoogd in artikel 8, § 1, 1°, 2°, 4° en 5°, en onder de voorwaarden bepaald in artikel 46*septies* van het Wetboek van Strafvordering of in artikel 16/3 van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst.

HOOFDSTUK 11. - *De verwerking van de passagiersgegevens ter verbetering van de grenscontroles en ter bestrijding van de illegale immigratie*

Art. 28. § 1. Dit hoofdstuk is van toepassing op de verwerking van de passagiersgegevens door de politiediensten belast met de grenscontroles en door de Dienst Vreemdelingenzaken, met het oog op de verbetering van de controles van personen aan de buitengrenzen en met het oog op de bestrijding van de illegale immigratie.

§ 2. Dit hoofdstuk is van toepassing onverminderd de verplichtingen van de politiediensten belast met de grenscontroles en van de Dienst Vreemdelingenzaken om persoonsgegevens of inlichtingen door te geven krachtens wettelijke of reglementaire bepalingen.

Art. 29. § 1. Met het oog op de in artikel 28, § 1, beoogde doelen worden de passagiersgegevens doorgegeven aan de politiediensten belast met de grenscontroles en aan de Dienst Vreemdelingenzaken, om hen in staat te stellen hun wettelijke opdrachten te vervullen, binnen de in dit artikel bepaalde grenzen.

§ 2. Enkel de passagiersgegevens bedoeld in artikel 9, § 1, 18°, worden doorgegeven voor de volgende categorieën van passagiers :

1° de passagiers die van plan zijn om het grondgebied via de buitengrenzen van België te betreden of het grondgebied via de buitengrenzen van België betreden hebben;

2° de passagiers die van plan zijn om het grondgebied via de buitengrenzen van België te verlaten of het grondgebied via de buitengrenzen van België verlaten hebben;

3° de passagiers die van plan zijn om via een in België gelegen internationale transitzone te passeren, die zich in een in België gelegen internationale transitzone bevinden of die via een in België gelegen transitzone gepasseerd zijn.

§ 3. De passagiersgegevens bedoeld in § 2 worden onmiddellijk na hun registratie in de passagiersgegevensbank doorgestuurd naar de politiediensten die belast zijn met de controle aan de buitengrenzen van België. Deze bewaren de gegevens in een tijdelijk bestand en vernietigen ze binnen de vierentwintig uur na doorsturing.

§ 4. Wanneer de Dienst Vreemdelingenzaken de gegevens nodig heeft voor de vervulling van zijn wettelijke opdrachten, worden de passagiersgegevens bedoeld in § 2 onmiddellijk na hun registratie in de passagiersgegevensbank doorgestuurd. De Dienst Vreemdelingenzaken bewaart deze gegevens in een tijdelijk bestand en vernietigt ze binnen de vierentwintig uur na doorsturing.

Indien, na het verstrijken van deze termijn, de toegang tot de passagiersgegevens bedoeld in § 2 voor de Dienst Vreemdelingenzaken noodzakelijk is in het kader van de uitvoering van zijn wettelijke opdrachten, richt hij hiertoe een afdoende gemotiveerde aanvraag tot de PIE.

De Dienst Vreemdelingenzaken stuurt maandelijks een verslag naar de Commissie voor de bescherming van de persoonlijke levenssfeer betreffende de toepassing van het tweede lid.

De Koning bepaalt bij een in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, de toegangsvoorwaarden bedoeld in het tweede lid.

Art. 30. § 1. De technische beveiligings- en toegangsregels, alsook de nadere regels voor de doorgifte van de passagiersgegevens aan de politiediensten belast met de grenscontroles en aan de Dienst Vreemdelingenzaken, worden gepreciseerd in een protocol dat afgesloten wordt, in overleg met de functionaris voor de gegevensbescherming en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, tussen, enerzijds, de leidend ambtenaar van de PIE en, anderzijds, de Commissaris-generaal van de federale politie en de leidend ambtenaar van de Dienst Vreemdelingenzaken.

§ 2. Deze nadere regels hebben tenminste betrekking op :

1° de behoefte van de Dienst Vreemdelingenzaken om op de hoogte te zijn van de gegevens;

2° de categorieën van personeelsleden die op basis van de uitvoering van hun opdrachten over een rechtstreekse toegang beschikken tot de doorgestuurde gegevens;

3° de verplichting voor alle personen die rechtstreeks of onrechtstreeks kennis nemen van de passagiersgegevens om het beroepsgeheim te respecteren;

4° de veiligheidsmaatregelen in verband met hun doorgifte.

Art. 31. De vervoerders en de reisoperatoren vernietigen, binnen de vierentwintig uur na het einde van het in artikel 4, 3° tot 6° bedoelde vervoer, alle in artikel 9, § 2, bedoelde passagiersgegevens, die ze overeenkomstig artikel 7 doorsturen.

[...]

HOOFDSTUK 15. - *Wijzigingsbepalingen*

Afdeling 1. - Wijziging van het Wetboek van Strafvordering

Art. 50. In het Wetboek van Strafvordering wordt een artikel 46*septies* ingevoegd, luidende :

‘ Art. 46*septies*. Bij het opsporen van de misdaden en wanbedrijven bedoeld in artikel 8, § 1, 1°, 2° en 5°, van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, kan de procureur des Konings, bij een schriftelijke en met redenen omklede beslissing, de officier van gerechtelijke politie opdragen om de PIE te vorderen tot het meedelen van de passagiersgegevens overeenkomstig artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

De maatregel kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek onderzoek. In dit geval preciseert de procureur des Konings de duur van de maatregel die niet langer kan zijn dan een maand, te rekenen vanaf de beslissing, onverminderd hernieuwing.

In geval van uiterst dringende noodzakelijkheid kan iedere officier van gerechtelijke politie, na mondelinge en voorafgaande instemming van de procureur des Konings, en bij een gemotiveerde en schriftelijke beslissing, de leidend ambtenaar van de PIE vorderen tot het meedelen van de passagiersgegevens. De officier van de gerechtelijke politie deelt deze gemotiveerde en schriftelijke beslissing en de verkregen informatie binnen vierentwintig uur mee aan de procureur des Konings en motiveert tevens de uiterst dringende noodzakelijkheid. ’

Afdeling 2. - Wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst

Art. 51. In hoofdstuk III, afdeling 1, onderafdeling 2, van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst, wordt een artikel 16/3 ingevoegd, luidende :

‘ Art. 16/3. § 1. De inlichtingen– en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, mits afdoende motivering, beslissen om toegang te hebben tot de passagiersgegevens bedoeld in artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

§ 2. De in § 1 bedoelde beslissing, wordt door een diensthoofd genomen en schriftelijk overgemaakt aan de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van voormelde wet. De beslissing wordt met de motivering van deze beslissing aan het Vast Comité I betekend.

Het Vast Comité I verbiedt de inlichtingen– en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.

De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt de lijst van de raadplegingen van de passagiersgegevens een keer per maand aan het Vast Comité I doorgegeven. ' ».

Ten aanzien van de inwerkingtreding en het toepassingsgebied van de wet van 25 *december* 2016

B.7. Krachtens artikel 54 van de wet van 25 december 2016 bepaalt de Koning, bij een in Ministerraad overlegd besluit, per vervoerssector en voor de reisoperatoren, de datum van inwerkingtreding van deze wet.

B.8. De wet van 25 december 2016 is in werking getreden op 7 augustus 2017, wat betreft de luchtvaartmaatschappijen, overeenkomstig artikel 12 van het koninklijk besluit van 18 juli 2017 « ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van de passagiersgegevens, houdende de verplichtingen opgelegd aan de luchtvaartmaatschappijen » (hierna : het koninklijk besluit van 18 juli 2017).

Sinds 22 februari 2019 is de wet van 25 december 2016 eveneens in werking getreden wat betreft de HST–vervoerders (*High speed train* – internationale dienst voor reizigersvervoer over het spoor) en de HST–ticketverdelers, overeenkomstig het koninklijk besluit van 3 februari 2019 « ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende de verplichtingen opgelegd aan de HST–vervoerders en de HST–ticketverdelers », evenals wat betreft de busvervoerders, overeenkomstig het koninklijk besluit van 3 februari 2019 « ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende de verplichtingen opgelegd aan de busvervoerders ».

Ten aanzien van de wijzigingen aangebracht in de wet van 25 *december* 2016

B.9. De wet van 25 december 2016 is gewijzigd bij de wet van 30 juli 2018 « betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens » (hierna : de wet van 30 juli 2018), bij de wet van 15 juli 2018 « houdende diverse bepalingen Binnenlandse Zaken » (hierna : de wet van 15 juli 2018) en bij de wet van 2 mei 2019 « tot wijziging van diverse bepalingen betreffende de verwerking van passagiersgegevens » (hierna : de wet van 2 mei 2019).

B.10.1. Artikel 280, vierde lid, van de wet van 30 juli 2018 heeft, met ingang van 5 september 2018, artikel 15, § 3, van de wet van 25 december 2016 opgeheven.

Daar geen enkel beroep tot vernietiging is ingesteld tegen artikel 280, vierde lid, van de wet van 30 juli 2018, is het thans voorliggende beroep tot vernietiging, in zoverre het betrekking heeft op artikel 15, § 3, van de wet van 25 december 2016, definitief zonder voorwerp geworden.

B.10.2. De wet van 30 juli 2018 omlijnt overigens de verwerkingen van persoonsgegevens, meer bepaald wat betreft de doelstellingen die zijn opgesomd in artikel 8 van de wet van 25 december 2016.

De parlementaire voorbereiding van de wet van 30 juli 2018 zet in dat verband uiteen :

« De verwerkingen ter verbetering van de grenscontroles en bestrijding van de illegale immigratie, bedoeld in artikel 8, § 2, van voornoemde wet van 25 december 2016, die een omzetting betreft van de API-Richtlijn, worden ingedeeld onder titel 1 van deze wet.

De verwerkingen in het kader van de finaliteiten opgenomen in artikel 8, § 1, 1°, 2°, 3° en 5°, van voornoemde wet van 25 december 2016 worden ingedeeld onder titel 2 aangezien dit verwerkingen betreffen van persoonsgegevens (passagiersgegevens) door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

De verwerkingen in het kader van de finaliteit bedoeld in artikel 8, § 1, 4°, van voornoemde wet van 25 december 2016 worden ingedeeld onder titel 3 daar dit verwerkingen [betreft] van persoonsgegevens (passagiersgegevens), uitgevoerd in het kader van de opdrachten van de inlichtingen– en veiligheidsdiensten als bedoeld in artikelen 7 en 11 van de wet van 30 november 1998.

Voornoemde wet van 25 december 2016 bevat reeds verscheidene bepalingen inzake gegevensbescherming zoals het aanstellen van een functionaris voor gegevensbescherming, het voorzien van een manuele validatie of het verbod om gevoelige gegevens te verwerken. Bepaalde punten die reeds opgenomen zijn in de wet van 25 december 2016 dienen bijgevolg niet opgenomen worden in de huidige wet » (*ibid.*, pp. 188-189).

Daaruit volgt dat, om de draagwijdte van het bestreden artikel 8 van de wet van 25 december 2016 te beoordelen, het Hof rekening dient te houden met de wet van 30 juli 2018.

B.11.1. De artikelen 62 tot 70 van de wet van 15 juli 2018 « houdende diverse bepalingen Binnenlandse Zaken » (hierna : de wet van 15 juli 2018), bekendgemaakt in het *Belgisch Staatsblad* op 25 september 2018, hebben eveneens de wet van 25 december 2016 gewijzigd.

De artikelen 62 tot 68 wijzigen meerdere bestreden artikelen van de wet van 25 december 2016 als volgt :

« Art. 62. In artikel 8 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens worden de volgende wijzigingen aangebracht :

1° in paragraaf 1 wordt de bepaling onder 1° vervangen als volgt :

' 1° het opsporen en vervolgen, met inbegrip van de uitvoering van straffen of vrijheidsbeperkende maatregelen, met betrekking tot misdrijven bedoeld in artikel 90*ter*, § 2, 2°, 3°, 7°, 8°, 11°, 14°, 17° tot 20°, 22°, 24° tot 28°, 30°, 32°, 33°, 34°, 36° tot 39°, 43° tot 45° en § 3, van het Wetboek van strafvordering; '

2° in paragraaf 1 wordt de bepaling onder 5° vervangen als volgt :

' 5° het opsporen en vervolgen van de misdrijven bedoeld in artikel 220, § 2, van de algemene wet van 18 juli 1977 inzake douane en accijnzen, in artikel 45, derde lid, van de wet van 22 december 2009 betreffende de algemene regeling inzake accijnzen, in artikel 5 van de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, in artikel 26 van het decreet van de Duitstalige gemeenschap van 20 februari 2017 ter bescherming van roerende cultuurgoederen van uitzonderlijk belang alsook in artikel 24 van het decreet van de Vlaamse gemeenschap van 24 januari 2003 houdende bescherming van het roerend cultureel erfgoed van uitzonderlijk belang, het ministerieel besluit tot wijziging van het ministerieel besluit van 7 februari 2012 waarbij de invoer van goederen van oorsprong of van herkomst uit Syrië, aan een vergunning onderworpen wordt, zoals gewijzigd bij het ministerieel besluit van 1 juli 2014, het ministerieel besluit van 23 maart 2004 tot opheffing van het ministerieel besluit van 17 januari 2003 waarbij de in–, uit– en doorvoer van goederen van oorsprong of van herkomst uit of met bestemming Irak, aan een voorafgaande machtiging onderworpen wordt en waarbij de in–, uit– en doorvoer van zekere goederen van oorsprong, van herkomst uit of met bestemming Irak aan een vergunning onderworpen wordt alsook het opsporen van misdrijven bedoeld in artikel 5 van de wet van 28 juli 1981 houdende goedkeuring van de Overeenkomst inzake de internationale handel in bedreigde in het wild levende dier– en plantensoorten, en van de Bijlagen, opgemaakt te Washington op 3 maart 1973, alsmede van de Wijziging van de Overeenkomst, aangenomen te Bonn op 22 juni 1979. '.

Art. 63. In artikel 14 van dezelfde wet worden de volgende wijzigingen aangebracht :

1° in paragraaf 1, 2°, wordt de bepaling onder *d)* vervangen als volgt :

' *d)* De onderzoeksdiensten, opsporingsdiensten en diensten belast met toezicht, controle en vaststelling van de Algemene Administratie van de Douane en Accijnzen. ';

2° paragraaf 4 wordt vervangen als volgt :

' § 4. De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens, de nadere regels voor de samenstelling en de organisatie van de PIE alsook het statuut van de leidend ambtenaar en de leden van de PIE. '.

Art. 64. In artikel 15, § 2, van dezelfde wet wordt het woord ' passagiersgegevensbank ' vervangen door het woord ' passagiersgegevens '.

Art. 65. Artikel 17 van dezelfde wet wordt vervangen als volgt :

' Art. 17. Na overleg met de functionaris voor de gegevensbescherming en na advies van de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens, sluiten de leidend ambtenaar van de PIE en de bevoegde diensten een protocol af dat de technische beveiligings– en toegangsregels uitwerkt.

Dit protocol :

1° garandeert dat de verwerkte gegevens aan dezelfde beveiligings– en beschermingsvereisten worden onderworpen;

2° zorgt ervoor dat de noodzakelijke beveiligingsmaatregelen genomen worden teneinde :

- te voldoen aan de verplichtingen die voortvloeien uit de regels betreffende de in deze wet bepaalde termijnen, de bewaring en de vernietiging van de gegevens die in de passagiersgegevensbank zijn bewaard;

- de gegevens ontoegankelijk te maken voor elke persoon die niet gemachtigd is om hiertoe toegang te hebben;

- te verzekeren dat de verwerkingen uitgevoerd door de leden van de PIE, gebeuren overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

3° bepaalt dat machtigingen om toegang tot de passagiersgegevens en gemeenschappelijke gebruikersprofielen worden toegekend aan elke persoon die toegang zou kunnen hebben tot de passagiersgegevens;

4° garandeert dat de gegevens op het grondgebied van de Europese Unie worden bewaard. '.

Art. 66. In artikel 24, § 2, van dezelfde wet, wordt de inleidende zin van het eerste lid vervangen als volgt :

' In het kader van de doelen beoogd in artikel 8, § 1, 1°, 2°, 4° en 5°, of met betrekking tot de bedreigingen vermeld in de artikelen 8, 1°, *a)*, *b)*, *c)*, *d)*, *f)*, *g)*, en 11, § 2, van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst, berust de voorafgaande beoordeling van de passagiers op een positieve overeenstemming, voortvloeiende uit een correlatie van de passagiersgegevens met : '.

Art. 67. In artikel 26 van dezelfde wet wordt paragraaf 2 vervangen als volgt :

' § 2. Voor het doel beoogd in artikel 8, § 1, 1°, 2°, 4° en 5°, of met betrekking tot de bedreigingen vermeld in de artikelen 8, 1°, *a)*, *b)*, *c)*, *d)*, *f)*, *g)*, en 11, § 2, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, zijn alle passagiersgegevens bedoeld in artikel 9 toegankelijk. '.

Art. 68. In artikel 31 van dezelfde wet worden de woorden ' in artikel 9, § 2 ' vervangen door de woorden ' in artikel 9, § 1, 18°. ' ».

Die wijzigingen zijn in werking getreden op 5 oktober 2018.

B.11.2. De artikelen 62, 63, 65, 66 en 67 van de wet van 15 juli 2018 vervangen, respectievelijk, de artikelen 8, § 1, 1° en 5°, 14, § 1, 2°, *d)*, en § 4, 17, 24, § 2, eerste lid, inleidende zin, en 26, § 2, van de wet van 25 december 2016.

Daar geen enkel beroep tot vernietiging is ingesteld tegen de voormelde artikelen van de wet van 15 juli 2018, is het thans voorliggende beroep tot vernietiging in beginsel zonder voorwerp geworden in zoverre het is gericht tegen de vervangen artikelen van de wet van 25 december 2016.

Het thans voorliggende beroep tot vernietiging is gericht tegen de wet van 25 december 2016 in de oorspronkelijke versie ervan. Ook al zijn de artikelen 8, § 1, 1° en 5°, 14, § 1, 2°, *d)*, en § 4, 17, 24, § 2, eerste lid, inleidende zin, en 26, § 2, van de wet van 25 december 2016 vervangen door de voormelde artikelen van de wet van 15 juli 2018, het beroep tot vernietiging behoudt, in zoverre het is gericht tegen de artikelen 8, § 1, 1° en 5°, 14, § 1, 2°, *d)*, en § 4, 17, 24, § 2, eerste lid, inleidende zin, en 26, § 2, van de wet van 25 december 2016, een voorwerp in zoverre de wet van 15 juli 2018 die bestreden artikelen van de wet van 25 december 2016 niet wezenlijk wijzigt.

Het Hof onderzoekt bijgevolg, voor elk van die bepalingen en voor elke grief, in welke mate het beroep tot vernietiging al dan niet een voorwerp heeft behouden.

B.11.3. Artikel 64 van de wet van 15 juli 2018 vervangt, in artikel 15, § 2, van de wet van 25 december 2016, het woord « passagiersgegevensbank » door het woord « passagiersgegevens ».

Artikel 68 van de wet van 15 juli 2018 vervangt, in artikel 31 van de wet van 25 december 2016, de woorden « in artikel 9, § 2 » door de woorden « in artikel 9, § 1, 18° ».

Die wijzigingen vormen slechts technische correcties van de artikelen 15, § 2, en 31 van de wet van 25 december 2016, zonder dat zij die bepalingen vervangen, zodat zij niet kunnen worden geacht een weerslag te hebben op het voorwerp van het voorliggende beroep.

B.11.4. Voor het overige houdt het Hof rekening met de voormelde wijzigingen teneinde meer bepaald de draagwijdte van de bestreden bepalingen vast te stellen.

B.12.1. De artikelen 2 tot 11 van de wet van 2 mei 2019, bekendgemaakt in het *Belgisch Staatsblad* van 24 mei 2019, hebben eveneens de wet van 25 december 2016 gewijzigd.

De artikelen 2 en 4 tot 7 van de wet van 2 mei 2019 wijzigen verscheidene bestreden artikelen van de wet van 25 december 2016 als volgt :

« Art. 2. In de artikelen 3, § 2, 14, § 2, 15, § 4, 23, § 2, tweede lid, 29, § 4, 30, § 1, 44, § 2, 7° en 9° en § 4, van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, worden de woorden ' de Commissie voor de bescherming van de persoonlijke levenssfeer ' telkens vervangen door de woorden ' de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens ' ».

« Art. 4. In artikel 15 van dezelfde wet, gewijzigd bij de wetten van 15 juli 2018 en 30 juli 2018, worden de volgende wijzigingen aangebracht :

1° In paragrafen 2 en 4, worden de woorden ' wet tot bescherming van de persoonlijke levenssfeer ' telkens vervangen door de woorden ' wet gegevensbescherming '.

2° In paragraaf 2, worden de woorden ' artikel 1, § 4 ' vervangen door de woorden ' artikel 26, 8°. '

Art. 5. Artikel 24, § 2, van dezelfde wet, gewijzigd bij de wet van 15 juli 2018 wordt aangevuld met een lid, luidende :

' In het kader van het in het eerste lid beoogde doel waarvoor de positieve overeenstemming werd verkregen, berust het gebruik van passagiersgegevens in het kader van de voorafgaande beoordeling gedurende een periode van vierentwintig uur vanaf de validatie bedoeld in paragraaf 4 op :

1° de relevante passagiersgegevens van hetzelfde vervoer als dit waaruit de positieve overeenstemming voortvloeit voor zover deze gegevens verband houden met de gegevens opgenomen in de positieve overeenstemming.

2° de andere in de passagiersgegevensbank geregistreerde passagiersgegevens van de persoon die het voorwerp heeft uitgemaakt van de positieve overeenstemming, onverminderd de toepassing van artikelen 19 en 20 '.

Art. 6. Artikel 27 van dezelfde wet wordt vervangen door :

' Art. 27. De passagiersgegevens worden gebruikt om gerichte opzoekingen te verrichten voor de doelen beoogd in artikel 8, § 1, 1°, 2°, 4° en 5°, en onder de voorwaarden bepaald in artikel 46*septies* van het Wetboek van strafvordering, in artikel 16/3 van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst of in artikel 281, § 4 van de algemene wet inzake douane en accijnzen gecoördineerd op 18 juli 1977 '.

Art. 7. In artikel 29 van dezelfde wet, worden de volgende wijzigingen aangebracht :

1° in paragraaf 1, worden de woorden ' belast met de grenscontroles ' vervangen door de woorden ' bedoeld in artikel 14, § 1, 2°, *a)* ';

2° in paragraaf 36, worden de woorden ' die belast zijn met de controle aan de buitengrenzen van België ' vervangen door de woorden ' zoals bedoeld in artikel 14, § 1, 2°, *a)* ' ».

Die wijzigingen zijn in werking getreden op 3 juni 2019.

B.12.2. De artikelen 2, 4 en 7 van de wet van 2 mei 2019 vormen enkel technische correcties van de artikelen 3, § 2, 14, § 2, 15, § 4, 29 en 30, § 1, van de wet van 25 december 2016, zodat die wijzigingen geen weerslag hebben op het voorwerp van het onderhavige beroep.

Overigens, ook al vervangt artikel 6 van de wet van 2 mei 2019 het bestreden artikel 27 van de wet van 25 december 2016, het beroep tot vernietiging behoudt, in zoverre het is gericht tegen die bepaling, een voorwerp voor zover de inhoud van artikel 6 van de wet van 2 mei 2019 identiek is aan de oorspronkelijke versie van dat artikel 27.

Voor het overige houdt het Hof rekening met de wijziging die bij artikel 5 van de wet van 2 mei 2019 is aangebracht in artikel 24, § 2, van de wet van 25 december 2016 teneinde inzonderheid de draagwijdte van de bestreden bepaling vast te stellen.

Ten aanzien van de prejudiciële verwijzing naar het Hof van Justitie

B.13.1. Bij zijn tussenarrest nr. 135/2019 van 17 oktober 2019 heeft het Hof aan het Hof van Justitie vragen gesteld over de uitlegging van de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG » (algemene verordening gegevensbescherming) (hierna : de AVG), alsook over de uitlegging en de geldigheid van de PNR–richtlijn en van de API–richtlijn. Het Hof heeft het Hof van Justitie eveneens gevraagd of het, in geval van vernietiging van de bestreden wet wegens schending van het Europees recht, de gevolgen van die wet voorlopig zou kunnen handhaven.

B.13.2. Het Hof heeft derhalve aan het Hof van Justitie van de Europese Unie de volgende tien prejudiciële vragen gesteld :

« 1. Dient artikel 23 van de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 ' betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG ' (Algemene verordening gegevens — AVG) », in samenhang gelezen met artikel 2, lid 2, *d)*, van die verordening, in die zin te worden geïnterpreteerd dat het van toepassing is op een nationale wetgeving zoals de wet van 25 december 2016 ' betreffende de verwerking van passagiersgegevens ', die niet enkel de richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 ' over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit ' omzet, alsook de richtlijn 2004/82/EG van de Raad van 29 april 2004 ' betreffende de verplichting voor vervoerders om passagiersgegevens door te geven ' en de richtlijn 2010/65/EU van het Europees Parlement en de Raad van 20 oktober 2010 ' betreffende meldingsformaliteiten voor schepen die aankomen in en/of vertrekken uit havens van de lidstaten en tot intrekking van Richtlijn 2002/6/EG ' ?

2. Is bijlage I van de richtlijn (EU) 2016/681 bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin dat de erin opgesomde gegevens zeer ruim zijn – onder meer de gegevens die worden beoogd in punt 18 van bijlage I van de richtlijn (EU) 2016/681, die verder gaan dan de gegevens beoogd in artikel 3, lid 2, van de richtlijn 2004/82/EG – en doordat die gegevens, in hun geheel beschouwd, gevoelige gegevens zouden kunnen onthullen, en aldus de grenzen van het « strikt noodzakelijke » zou kunnen overschrijden ?

3. Zijn de punten 12 en 18 van bijlage I bij de richtlijn (EU) 2016/681 bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in zoverre, rekening houdend met de bewoordingen ' onder meer ' en ' met inbegrip van ', de erin beoogde gegevens bij wijze van voorbeeld en niet exhaustief worden vermeld, zodat de vereiste van nauwkeurigheid en duidelijkheid van de regels die leiden tot een inmenging in het recht op eerbiediging van het privéleven en in het recht op bescherming van de persoonsgegevens niet in acht zou zijn genomen ?

4. Zijn artikel 3, punt 4, van de richtlijn 2016/681/EU en bijlage I bij dezelfde richtlijn bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in zoverre het systeem van het algemeen verzamelen, doorgeven en verwerken van passagiersgegevens dat die bepalingen instellen, iedere persoon beoogt die het desbetreffende vervoersmiddel gebruikt, los van elk objectief element dat het mogelijk maakt ervan uit te gaan dat die persoon een risico voor de openbare veiligheid kan vormen ?

5. Dient artikel 6 van de richtlijn (EU) 2016/681, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus te worden uitgelegd dat het zich verzet tegen een nationale wetgeving zoals de bestreden wet, die, als doel van de ' PNR-gegevensverwerking ', het toezien op door de inlichtingen– en veiligheidsdiensten beoogde activiteiten aanvaardt, waarbij het dat doel aldus opneemt in het voorkomen, het opsporen, het onderzoeken en het vervolgen van terroristische misdrijven en ernstige criminaliteit ?

6. Is artikel 6 van de richtlijn (EU) 2016/681 bestaanbaar met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in zoverre de voorafgaande beoordeling die daarin wordt geregeld, door een correlatie met de gegevensbanken en de vooraf bepaalde criteria, stelselmatig en op algemene wijze van toepassing is op de passagiersgegevens, los van elk objectief element dat toelaat ervan uit te gaan dat die passagiers een risico kunnen vormen voor de openbare veiligheid ?

7. Kan het begrip ' andere bevoegde nationale instantie ' bepaald in artikel 12, lid 3, van de richtlijn (EU) 2016/681 zo worden geïnterpreteerd dat het de PIE beoogt die bij de wet van 25 december 2016 is opgericht en die derhalve de toegang tot de ' PNR-gegevens ', na een termijn van zes maanden, in het kader van de gerichte opzoekingen zou kunnen toestaan ?

8. Dient artikel 12 van de richtlijn (EU) 2016/681, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zo te worden geïnterpreteerd dat het zich verzet tegen een nationale wetgeving zoals de bestreden wet die voorziet in een algemene bewaartermijn van de gegevens van vijf jaar, zonder onderscheid of de betrokken passagiers, in het kader van de voorafgaande beoordeling, al dan niet een risico kunnen vormen voor de openbare veiligheid ?

9. *a)* Is de richtlijn 2004/82/EG bestaanbaar met artikel 3, lid 2, van het Verdrag betreffende de Europese Unie en met artikel 45 van het Handvest van de grondrechten van de Europese Unie, in zoverre de daarbij ingevoerde verplichtingen van toepassing zijn op de vluchten binnen de Europese Unie ?

b) Dient de richtlijn 2004/82/EG, in samenhang gelezen met artikel 3, lid 2, van het Verdrag betreffende de Europese Unie en met artikel 45 van het Verdrag betreffende de grondrechten van de Europese Unie, zo te worden geïnterpreteerd dat zij zich verzet tegen een nationale wetgeving zoals de bestreden wet die, met het oog op de strijd tegen illegale immigratie en het verbeteren van de grenscontroles, een systeem toestaat voor de verzameling en verwerking van de passagiersgegevens ' van, naar en op doorreis over het nationaal grondgebied ', hetgeen indirect een herinvoering van de controles aan de binnengrenzen zou kunnen impliceren ?

10. Zou het Grondwettelijk Hof, indien het op grond van de antwoorden op de hiervoor weergegeven prejudiciële vragen, tot de conclusie zou komen dat de bestreden wet, die met name de richtlijn (EU) 2016/681 omzet, één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van de wet van 25 december 2016 ' betreffende de verwerking van passagiersgegevens ' tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen worden gebruikt voor de door de wet beoogde doelstellingen ? ».

B.14. Bij zijn arrest van 21 juni 2022 in zake *Ligue des droits humains t. Ministerraad*, (C—817/19, ECLI:EU:C:2022:491), heeft het Hof van Justitie van de Europese Unie, in grote kamer, op de voormelde prejudiciële vragen geantwoord.

In het voormelde arrest onderzoekt het Hof van Justitie opeenvolgend :

- de eerste prejudiciële vraag betreffende de samenhang van de AVG met de PNR–richtlijn (punten 63 tot 84);

- de tweede tot de vierde en de zesde prejudiciële vraag met betrekking tot de geldigheid van de PNR–richtlijn en/of van de bijlagen ervan wat betreft het systeem voor de verzameling van gegevens en de beoogde gegevens (punten 85 tot 228);

- de vijfde prejudiciële vraag met betrekking tot de uitlegging van de PNR–richtlijn wat betreft de doeleinden op het vlak van inlichting en veiligheid (punten 229 tot 237);

- de zevende prejudiciële vraag met betrekking tot de uitlegging van het begrip « onafhankelijke nationale autoriteit » bedoeld in de PNR–richtlijn (punten 238 tot 247);

- de achtste prejudiciële vraag met betrekking tot de uitlegging van de bewaartermijn van de gegevens zoals bedoeld in de PNR–richtlijn (punten 248 tot 262);

- de negende prejudiciële vraag, punt a, met betrekking tot de geldigheid van de API–richtlijn, indien die richtlijn van toepassing is op de vluchten binnen de EU (punten 263 tot 269);

- de negende prejudiciële vraag, punt b, met betrekking tot de uitlegging van de API–richtlijn in zoverre zij zou toelaten illegale immigratie te bestrijden en opnieuw een vorm van controle aan de grenzen in te voeren (punten 270 tot 291);

- de tiende prejudiciële vraag met betrekking tot een eventuele handhaving van de gevolgen van de wet die mogelijk onverenigbaar zou zijn met het Unierecht (punten 292 tot 298).

Ten aanzien van het eerste middel

B.15. Het eerste middel, dat in hoofdorde wordt geformuleerd, is afgeleid uit de schending van artikel 22 van de Grondwet, al dan niet in samenhang gelezen met artikel 23 van de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016, met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie en met artikel 8 van het Europees Verdrag voor de rechten van de mens.

Volgens de verzoekende partij zou de wet van 25 december 2016 afbreuk doen aan het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens, die door die bepalingen worden gewaarborgd. De wet van 25 december 2016 zou het wettigheidsbeginsel niet in acht nemen. Het systematisch en ongedifferentieerd verzamelen, doorgeven en verwerken van PNR-gegevens volgens een methode van « *pre-screening* » zou niet noodzakelijk zijn, noch verantwoord door een doel van algemeen belang en verscheidene doorgevoerde maatregelen zouden onevenredig zijn.

Wat de referentienormen betreft

B.16.1. Artikel 22 van de Grondwet bepaalt :

« Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht ».

B.16.2. Artikel 8 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op eerbiediging van zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling.

2. Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen ».

B.16.3. De Grondwetgever heeft gestreefd naar een zo groot mogelijke concordantie tussen artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens (*Parl. St.*, Kamer, 1992-1993, nr. 997/5, p. 2).

De draagwijdte van dat artikel 8 is analoog aan die van de voormelde grondwetsbepaling, zodat de waarborgen die beide bepalingen bieden, een onlosmakelijk geheel vormen.

B.17.1. Het recht op eerbiediging van het privéleven, zoals gewaarborgd in de voormelde grondwets- en verdragsbepalingen, heeft als essentieel doel de personen te beschermen tegen inmengingen in hun privéleven.

Dat recht heeft een ruime draagwijdte en omvat, onder meer, de eerbiediging van de fysieke integriteit van de persoon (EHRM, grote kamer, 8 april 2021, *Vavřička e.a. t. Tsjechië*, ECLI:CE:ECHR:2021:0408JUD004762113, § 261) en de bescherming van persoonsgegevens en van persoonlijke informatie met betrekking tot de gezondheid (EHRM, 25 februari 1997, *Z. t. Finland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; 10 oktober 2006, *L.L. t. Frankrijk*, ECLI:CE:ECHR:2006:1010JUD000750802, § 32; 27 februari 2018, *Mockuté t. Litouwen*, ECLI:CE:ECHR:2018:0227JUD006649009, § 93). Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens blijkt dat, onder meer, de volgende gegevens en informatie betreffende personen vallen onder de bescherming van dat recht : de naam, het adres, de professionele activiteiten, de persoonlijke relaties, digitale vingerafdrukken, camerabeelden, foto's, communicatiegegevens, DNA–gegevens, gerechtelijke gegevens (veroordeling of inverdenkingstelling), financiële gegevens, informatie over bezittingen en medische gegevens (zie onder meer EHRM, 26 maart 1987, *Leander t. Zweden*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47–48; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66–68; 17 december 2009, *B.B. t. Frankrijk*, ECLI:CE:ECHR:2009:1217JUD000533506, § 57; 10 februari 2011, *Dimitrov–Kazakov t. Bulgarije*, ECLI:CE:ECHR:2011:0210JUD001137903, §§ 29–31; 18 oktober 2011, *Khelili t. Zwitserland*, ECLI:CE:ECHR:2011:1018JUD001618807, §§ 55–57; 9 oktober 2012, *Alkaya t. Turkije*, ECLI:CE:ECHR:2012:1009JUD004281106, § 29; 18 april 2013, *M.K. t. Frankrijk*, ECLI:CE:ECHR:2013:0418JUD001952209, § 26; 18 september 2014, *Brunet t. Frankrijk*, ECLI:CE:ECHR:2014:0918JUD002101010, § 31; 13 oktober 2020, *Frâncu t. Roemenië*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

B.17.2. De rechten die bij artikel 22 van de Grondwet en bij artikel 8 van het Europees Verdrag voor de rechten van de mens worden gewaarborgd, zijn evenwel niet absoluut.

Zij sluiten een overheidsinmenging in het recht op eerbiediging van het privéleven niet uit, maar vereisen dat zij wordt toegestaan door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en dat zij evenredig is met de daarmee nagestreefde wettige doelstelling. Die bepalingen houden voor de overheid bovendien de positieve verplichting in om maatregelen te nemen die een daadwerkelijke eerbiediging van het privéleven verzekeren, ook in de sfeer van de onderlinge verhoudingen tussen individuen (EHRM, 27 oktober 1994, *Kroon e.a. t. Nederland*, ECLI:CE:ECHR:1994:1027JUD001853591, § 31; grote kamer, 12 november 2013, *Söderman t. Zweden*, ECLI:CE:ECHR:2013:1112JUD000578608, § 78).

Wanneer zij de afweging maken tussen het belang van de Staat bij de verwerking van persoonsgegevens en het individueel belang bij de bescherming van de vertrouwelijkheid van die gegevens, beschikken de nationale autoriteiten over een zekere beoordelingsmarge (*ibid.*, § 99). In het licht van het fundamentele belang van de bescherming van persoonsgegevens is die marge evenwel vrij beperkt (EHRM, 26 januari 2017, *Surikov t. Oekraïne*, ECLI:CE:ECHR:2017:0126JUD004278806, § 73). Opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat een billijk evenwicht wordt bereikt tussen alle rechten en belangen die in het geding zijn. Bij de beoordeling van dat evenwicht dient rekening te worden gehouden met de bepalingen van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (hierna : het Verdrag nr. 108) (EHRM, 25 februari 1997, *Z t. Finland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204, § 103; 26 januari 2017, *Surikov t. Oekraïne*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

Het Verdrag nr. 108 bevat onder meer de beginselen inzake de verwerking van persoonsgegevens : rechtmatigheid, behoorlijkheid, transparantie, doelbinding, evenredigheid, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, en verantwoordingsplicht.

Datzelfde Verdrag is geactualiseerd bij een protocol tot amendering dat op 10 oktober 2018 voor ondertekening is opengesteld.

Uit Verdrag nr. 108 vloeit voort dat het nationale recht in het bijzonder moet garanderen dat persoonsgegevens relevant en niet excessief zijn in het licht van de doeleinden waarvoor ze worden verzameld of bijgehouden, dat de gegevens worden bewaard in een vorm die de identificatie van de betrokkenen niet langer dan vereist mogelijk maakt, en dat de bijgehouden data op efficiënte wijze worden beschermd tegen verkeerdelijk gebruik en misbruik. Het heeft ook erop gewezen dat het van essentieel belang is dat het nationale recht duidelijke en gedetailleerde regels bevat inzake de reikwijdte en toepassing van de betrokken maatregelen, en ook minimumwaarborgen bevat inzake, onder andere, de duurtijd, de bewaring, het gebruik, de toegang van derden, procedures voor het behoud van de integriteit en vertrouwelijkheid van gegevens en procedures voor de vernietiging ervan, zodat in elke fase van de gegevensverwerking er voldoende waarborgen zijn tegen het risico van misbruik en willekeur (EHRM, 26 januari 2017, *Surikov t. Oekraïne*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

B.18.1. Artikel 7 van het Handvest van de grondrechten van de Europese Unie bepaalt :

« Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie– en gezinsleven, zijn woning en zijn communicatie ».

B.18.2. Artikel 8 van hetzelfde Handvest bepaalt :

« 1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd ».

B.18.3. Binnen de werkingssfeer van het Europees Unierecht waarborgen artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 7 van het Handvest analoge grondrechten (HvJ, grote kamer, 9 november 2010, C—92/09 en C—93/09, *Volker und Markus Schecke GbR en anderen*, ECLI:EU:C:2010:662), terwijl artikel 8 van dat Handvest een specifieke rechtsbescherming van persoonsgegevens beoogt (HvJ, grote kamer, 21 december 2016, C—203/15 en C—698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, punt 129; HvJ, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, punt 114).

Het Hof van Justitie herinnert in dat verband eraan dat « artikel 7 van het Handvest, inzake de eerbiediging van het privéleven en van het familie– en gezinsleven, rechten bevat die corresponderen met rechten welke zijn gegarandeerd door artikel 8, lid 1, van het Europees Verdrag voor de rechten van de mens, ondertekend te Rome op 4 november 1950 (hierna : het EVRM), en dat, overeenkomstig artikel 52, lid 3, van het Handvest, aan dat artikel 7 dus dezelfde inhoud en reikwijdte moeten worden toegekend als die welke aan artikel 8, lid 1, van het EVRM worden toegekend, zoals uitgelegd in de rechtspraak van het Europees Hof voor de Rechten van de Mens » (HvJ, 17 december 2015, C—419/14, *WebMindLicenses Kft.*, ECLI:EU:C:2015:832, punt 70; 14 februari 2019, C—345/17, *Buivids*, ECLI:EU:C:2019:122, punt 65).

B.18.4. Het Hof van Justitie van de Europese Unie is van mening dat de eerbiediging van het recht op persoonlijke levenssfeer bij de verwerking van persoonsgegevens gelijk welke informatie betreft aangaande een geïdentificeerde of identificeerbare natuurlijke persoon (HvJ, grote kamer, 9 november 2010, C—92/09 en C—93/09, *Volker und Markus Schecke GbR e.a.*, ECLI:EU:C:2010:662, punt 52; 16 januari 2019, C—496/17, *Deutsche Post AG*, ECLI:EU:C:2019:26, punt 54).

B.18.5. De in de artikelen 7 en 8 van het Handvest verankerde grondrechten hebben evenmin een absolute gelding (HvJ, grote kamer, 16 juli 2020, C—311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, punt 172).

Overeenkomstig artikel 52, lid 1, eerste volzin, van het Handvest moeten beperkingen op de uitoefening van de daarin erkende rechten en vrijheden, waaronder met name het door artikel 7 gewaarborgde recht op eerbiediging van het privéleven en het in artikel 8 ervan neergelegde recht op bescherming van persoonsgegevens, bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen (HvJ, grote kamer, 6 oktober 2020, C—623/17, *Privacy International*, ECLI:EU:C:2020:790, punt 64).

B.18.6. In zijn advies 1/15 van 26 juli 2017 « betreffende het ontwerp van overeenkomst tussen Canada en de Europese Unie over de doorgifte en verwerking van persoonsgegevens van luchtreizigers », stelt het Hof van Justitie vast dat PNR-gegevens informatie bevatten over geïdentificeerde of identificeerbare personen, waardoor het verzamelen en verwerken ervan alsook de toegang tot die gegevens kunnen raken aan het door artikel 7 van het Handvest gewaarborgde recht op eerbiediging van het privéleven, en aan het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens (HvJ, grote kamer, 26 juli 2017, advies 1/15, *Overeenkomst PNR EU-Canada,* ECLI:EU:C:2017:592, punten 122-126).

Met betrekking tot de beperkingen die kunnen worden gesteld aan de artikelen 7 en 8 van het Handvest, oordeelt het Hof van Justitie dat « de in de artikelen 7 en 8 van het Handvest verankerde rechten [...] geen absolute gelding [hebben], maar [...] in relatie tot hun sociale functie [moeten] worden beschouwd » (*ibid.*, punt 136) :

« 137. In dit verband moet tevens worden opgemerkt dat persoonsgegevens luidens artikel 8, lid 2, van het Handvest met name moeten worden verwerkt ' voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet '.

138. Overeenkomstig artikel 52, lid 1, eerste volzin, van het Handvest moeten beperkingen op de uitoefening van de daarin erkende rechten en vrijheden bij wet worden gesteld en moeten zij de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Volgens artikel 52, lid 1, tweede volzin, van het Handvest kunnen, met inachtneming van het evenredigheidsbeginsel, slechts beperkingen aan deze rechten en vrijheden worden gesteld indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen » (*ibid.*).

B.19.1. Bij artikel 22 van de Grondwet wordt aan de bevoegde wetgever de bevoegdheid voorbehouden om te bepalen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven. Het waarborgt aldus aan elke burger dat geen inmenging in de uitoefening van dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

Een delegatie aan een andere macht is evenwel niet in strijd met het wettigheidsbeginsel, voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld.

B.19.2. Naast het formele wettigheidsvereiste legt artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8 en 52 van het Handvest van de grondrechten van de Europese Unie, de verplichting op dat de inmenging in de uitoefening van het recht op eerbiediging van het privéleven en van het recht op bescherming van persoonsgegevens in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging toestaat.

Inzake de bescherming van de persoonsgegevens impliceert dat vereiste van voorzienbaarheid dat voldoende precies moet worden bepaald in welke omstandigheden de verwerkingen van persoonsgegevens zijn toegelaten (EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). Het vereiste dat de beperking bij wet dient te worden ingesteld, houdt met name in dat de wettelijke grondslag die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (HvJ, 6 oktober 2020, C—623/17, *Privacy International*, ECLI:EU:C:2020:790, punt 65).

Derhalve moet eenieder een voldoende duidelijk beeld kunnen hebben van de verwerkte gegevens, de bij een bepaalde gegevensverwerking betrokken personen en de voorwaarden voor en de doeleinden van de verwerking.

B.20.1. Artikel 23 van de AVG bepaalt :

« 1. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van :

a) de nationale veiligheid;

b) landsverdediging;

c) de openbare veiligheid;

d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;

e) andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

f) de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;

g) de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;

h) een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten *a)*, tot en met *e)* en punt *g)* bedoelde gevallen;

i) de bescherming van de betrokkene of van de rechten en vrijheden van anderen;

j) de inning van civielrechtelijke vorderingen.

2. De in lid 1 bedoelde wettelijke maatregelen bevatten met name specifieke bepalingen met betrekking tot, in voorkomend geval, ten minste :

a) de doeleinden van de verwerking of van de categorieën van verwerking,

b) de categorieën van persoonsgegevens,

c) het toepassingsgebied van de ingevoerde beperkingen,

d) de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,

e) de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken,

f) de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking,

g) de risico's voor de rechten en vrijheden van de betrokkenen, en

h) het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking ».

Overeenkomstig die bepaling moeten beperkingen van bepaalde verplichtingen van de verwerkingsverantwoordelijken — waarin het Handvest voorziet — en van de rechten van de betrokkenen worden ingesteld bij wet, moeten zij de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laten en moeten zij een in een democratische samenleving noodzakelijke en evenredige maatregel zijn ter verwezenlijking van het nagestreefde doel en de in het tweede lid geformuleerde specifieke vereisten naleven (HvJ, grote kamer, 6 oktober 2020, C—511/18, C—512/18 en C—520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, punten 209—210; 10 december 2020, C—620/19, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, punt 46).

B.20.2. Artikel 2 van de AVG bepaalt :

« 1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

[...]

d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

[...] ».

B.20.3. Overweging 19 van de AVG bepaalt :

« De bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, en het vrije verkeer van die gegevens wordt geregeld in een specifieke rechtshandeling van de Unie. Deze verordening mag derhalve niet van toepassing zijn op de met die doeleinden verrichte verwerkingsactiviteiten. Overeenkomstig deze verordening door overheidsinstanties verwerkte persoonsgegevens die voor die doeleinden worden gebruikt, moeten vallen onder een meer specifieke rechtshandeling van de Unie, namelijk Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad. De lidstaten kunnen bevoegde autoriteiten in de zin van Richtlijn (EU) 2016/680 taken opdragen die niet noodzakelijk worden verricht met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, zodat de verwerking van persoonsgegevens voor die andere doeleinden binnen het toepassingsgebied van deze verordening valt, voor zover zij binnen het toepassingsgebied van de Uniewetgeving valt.

Aangaande de verwerking van persoonsgegevens door die bevoegde instanties voor doeleinden die binnen het toepassingsgebied van deze verordening vallen, moeten de lidstaten meer specifieke bepalingen kunnen handhaven of invoeren om de toepassing van de regels van deze verordening aan te passen. In die bepalingen kunnen meer bepaald specifieke voorschriften voor de verwerking van persoonsgegevens door die bevoegde instanties voor de genoemde andere doeleinden worden vastgesteld, rekening houdend met de grondwettelijke, organisatorische en bestuurlijke structuur van de lidstaat in kwestie. Wanneer de verwerking van persoonsgegevens door privaatrechtelijke organen onder de onderhavige verordening valt, moet deze verordening voorzien in de mogelijkheid dat de lidstaten onder specifieke voorwaarden bij wet vastgestelde verplichtingen en rechten beperken, indien een dergelijke beperking in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter bescherming van specifieke belangen van betekenis, waaronder de openbare veiligheid en de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Dit is bijvoorbeeld van belang in het kader van de bestrijding van witwassen of de werkzaamheden van forensische laboratoria ».

Zoals uit die overweging blijkt, valt de verwerking van persoonsgegevens door bevoegde instanties met het oog op de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen in principe niet onder de AVG, maar onder de richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad » (hierna : de Politierichtlijn).

B.20.4. De Politierichtlijn stelt, op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking, specifieke regels vast betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, met inachtneming van de specifieke aard van die activiteiten.

Artikel 1, lid 1, van de Politierichtlijn bepaalt :

« Bij deze richtlijn worden de regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid ».

Artikel 9, leden 1 en 2, van dezelfde richtlijn bepaalt :

« 1. Persoonsgegevens die door bevoegde autoriteiten voor de in artikel 1, lid 1 omschreven doeleinden worden verzameld, worden niet verwerkt voor andere doeleinden, tenzij die verwerking krachtens het Unierecht of het lidstatelijke recht is toegestaan. Wanneer persoonsgegevens voor zulke andere doeleinden worden verwerkt, is Verordening (EU) 2016/679 van toepassing, tenzij de verwerking geschiedt in het kader van een activiteit die buiten de werkingssfeer van het Unierecht valt.

2. Wanneer aan bevoegde autoriteiten krachtens het lidstatelijke recht andere taken dan die ter verwezenlijking van de in artikel 1, lid 1, omschreven doeleinden worden toevertrouwd, is Verordening (EU) 2016/679 van toepassing op verwerking voor die doeleinden, waaronder archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, tenzij de verwerking geschiedt in het kader van een activiteit die buiten de werkingssfeer van het Unierecht valt ».

Overweging 11 van de Politierichtlijn preciseert in dat verband :

« [...] Die bevoegde autoriteiten kunnen niet alleen overheidsinstanties zoals de rechterlijke autoriteiten, de politie of andere rechtshandhavingsautoriteiten omvatten, maar ook ieder ander orgaan dat of iedere andere entiteit die krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen voor de doeleinden van deze richtlijn. Wanneer dat orgaan of die entiteit persoonsgegevens verwerkt voor andere doeleinden dan die van deze richtlijn, is Verordening (EU) 2016/679 van toepassing. Verordening (EU) 2016/679 is dan ook van toepassing in gevallen waarin een orgaan of entiteit persoonsgegevens verzamelt voor andere doeleinden en die persoonsgegevens verder verwerkt met het oog op nakoming van een wettelijke verplichting waaraan het orgaan of de entiteit is onderworpen. Zo bewaren financiële instellingen met het oog op onderzoek, opsporing of vervolging van strafbare feiten bepaalde persoonsgegevens die door hen worden verwerkt, en verstrekken zij die persoonsgegevens uitsluitend in specifieke gevallen en overeenkomstig het lidstatelijke recht aan de bevoegde nationale autoriteiten. Een orgaan dat of entiteit die namens die autoriteiten persoonsgegevens verwerkt binnen het toepassingsgebied van deze richtlijn, dient gebonden te zijn door een overeenkomst of een andere rechtshandeling en door de ingevolge deze richtlijn op verwerkers toepasselijke bepalingen, terwijl Verordening (EU) 2016/679 onverminderd van toepassing blijft op de verwerking van persoonsgegevens door de verwerker die buiten het toepassingsgebied van deze richtlijn valt ».

Overweging 34 van de Politierichtlijn preciseert ook :

« [...] Wanneer de persoonsgegevens in eerste instantie zijn verzameld door een bevoegde autoriteit voor een van de doeleinden van deze richtlijn, moet Verordening (EU) 2016/679 van toepassing zijn op de doorzending van die gegevens voor andere doeleinden dan die van deze richtlijn, indien deze verwerking is toegestaan bij het Unierecht of het lidstatelijke recht. Meer bepaald dienen de bepalingen van Verordening (EU) 2016/679 van toepassing te zijn op de doorgifte van persoonsgegevens voor doeleinden die niet onder deze richtlijn vallen. Verordening (EU) 2016/679 dient van toepassing te zijn op de verwerking van persoonsgegevens door een ontvanger die niet de bevoegde autoriteit is of die niet optreedt als bevoegde autoriteit in de zin van deze richtlijn en aan wie de persoonsgegevens rechtmatig zijn bekendgemaakt door een bevoegde autoriteit [...] ».

B.21.1. De Ministerraad werpt in hoofdorde een exceptie van niet-ontvankelijkheid van het eerste middel op, in zoverre het is afgeleid uit de schending van artikel 23 van de AVG, dat niet van toepassing zou zijn op de wet van 25 december 2016.

B.21.2. De wet van 25 december 2016 organiseert de verzameling en de doorgifte van PNR-gegevens, de oprichting van een passagiersgegevensbank, die wordt beheerd door de PIE, de doelstellingen van de verwerking van die gegevensbank en de toegang tot die laatste.

De wet van 25 december 2016 zet hoofdzakelijk de PNR-richtlijn om, maar heeft ook, zoals aangegeven in artikel 2 ervan, en zoals vermeld in B.2, een inhoud die verder gaat dan de omzetting van die richtlijn.

B.21.3. Op de vraag van het Hof of artikel 23, in samenhang gelezen met artikel 2, lid 2, *d)*, van de AVG zo moet worden geïnterpreteerd dat het van toepassing is op een nationale wetgeving zoals de wet van 25 december 2016, die tegelijk de PNR–richtlijn, de API–richtlijn en de richtlijn 2010/65/EU omzet, heeft het Hof van Justitie, in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geantwoord dat uit de bewoordingen van artikel 2, lid 2, *d)*, van de AVG « duidelijk [...] blijkt [...] dat aan twee voorwaarden moet zijn voldaan opdat gegevensverwerking onder de daarin genoemde uitzondering valt » en dat « de eerste voorwaarde [...] de doeleinden [betreft] van de verwerking, die moet plaatsvinden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. De tweede voorwaarde betreft de auteur van deze verwerking, waarbij het moet gaan om een ' bevoegde autoriteit ' in de zin van die bepaling » (punt 67), maar dat de in artikel 2, lid 2, onder *d)*, van de AVG bedoelde uitzondering « net als de andere in artikel 2, lid 2, AVG genoemde uitzonderingen op de werkingssfeer van deze verordening, strikt [dient] te worden uitgelegd » (punt 70) :

« 71. Blijkens overweging 19 van deze verordening is deze uitzondering ingegeven door de omstandigheid dat de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op onder meer de voorkoming en de opsporing van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, onder een specifiekere handeling van de Unie valt, te weten richtlijn 2016/680, die is vastgesteld op dezelfde dag als de AVG [arrest van 22 juni 2021, *Latvijas Republikas Saeima (Strafpunten)*, C—439/19, EU:C:2021:504, punt 69].

72. Zoals de overwegingen 9 tot en met 11 van richtlijn 2016/680 trouwens verduidelijken, zijn in deze richtlijn specifieke regels voor de bescherming van natuurlijke personen in verband met die verwerkingen vastgesteld, daarbij rekening houdend met de specifieke aard van deze activiteiten die onder de justitiële samenwerking in strafzaken en de politiële samenwerking vallen, terwijl in de AVG algemene regels voor de bescherming van die personen zijn vastgesteld die voor die verwerkingen gelden wanneer de specifiekere handeling – richtlijn 2016/680 – niet van toepassing is. Zo staat in overweging 11 van deze richtlijn dat de AVG van toepassing is op de verwerking van persoonsgegevens die door een ' bevoegde autoriteit ' in de zin van artikel 3, punt 7, van deze richtlijn wordt verricht voor andere doeleinden dan die welke worden genoemd in deze richtlijn [zie in die zin arrest van 22 juni 2021, *Latvijas Republikas Saeima (Strafpunten)*, C—439/19, EU:C:2021:504, punt 70].

73. Wat de eerste van de in punt 67 van het onderhavige arrest genoemde voorwaarden betreft, namelijk de doeleinden van de verwerking van persoonsgegevens in de zin van de PNR–richtlijn, zij eraan herinnerd dat PNR–gegevens volgens artikel 1, lid 2, van deze richtlijn uitsluitend mogen worden verwerkt om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen. Deze doelstellingen vallen onder die welke in artikel 2, lid 2, onder *d)*, AVG en artikel 1, lid 1, van richtlijn 2016/680 worden genoemd, zodat die verwerking onder de uitzondering van artikel 2, lid 2, onder *d)*, van deze verordening en dus binnen de werkingssfeer van deze richtlijn kan vallen.

74. Dit is daarentegen niet het geval voor de verwerking waarin de API–richtlijn en richtlijn 2010/65 voorzien, die andere doeleinden hebben dan die welke in artikel 2, lid 2, onder *d)*, AVG en artikel 1, lid 1, van richtlijn 2016/680 worden genoemd.

75. Zoals uit de overwegingen 1, 7 en 9 en artikel 1 van de API–richtlijn blijkt, beoogt deze immers grenscontroles te verbeteren en illegale immigratie te bestrijden, door te verlangen dat vervoerders vooraf passagiersgegevens verstrekken aan de bevoegde nationale autoriteiten. Verschillende overwegingen en bepalingen van de API–richtlijn maken trouwens duidelijk dat de hierin voorgeschreven gegevensverwerking binnen de werkingssfeer van de AVG valt. Zo luidt het in overweging 12 van deze richtlijn dat ' richtlijn [95/46] van toepassing [is] op de verwerking van persoonsgegevens door de autoriteiten van de lidstaten ', en wordt in artikel 6, lid 1, vijfde alinea, ervan verduidelijkt dat de lidstaten de API–gegevens ook kunnen gebruiken voor wetshandhavingsdoeleinden ' overeenkomstig [...] de in [richtlijn 95/46] vervatte bepalingen inzake gegevensbescherming ', een uitdrukking die ook voorkomt in de derde alinea van deze bepaling. Evenzo staat onder meer in overweging 9 ' zonder afbreuk te doen aan [richtlijn 95/46] '. Tot slot heet het in artikel 6, lid 2, van de API–richtlijn dat de vervoerders informatie moeten verstrekken aan de passagiers ' overeenkomstig [richtlijn 95/46] '.

76. Richtlijn 2010/65 heeft dan weer tot doel, zoals uit overweging 2 en artikel 1, lid 1, ervan blijkt, de administratieve procedures die van toepassing zijn op het zeevervoer te vereenvoudigen en te harmoniseren door een algemene invoering van de elektronische overdracht van gegevens en door rationalisering van de meldingsformaliteiten. Artikel 8, lid 2, van deze richtlijn bevestigt dat de hierin geregelde gegevensverwerking binnen de werkingssfeer van de AVG valt, aangezien deze bepaling de lidstaten verplicht om er wat persoonsgegevens betreft op toe te zien dat wordt voldaan aan richtlijn 95/46.

77. Bijgevolg valt gegevensverwerking die wordt voorgeschreven in nationale wetgeving die de API–richtlijn en richtlijn 2010/65 in nationaal recht omzet, binnen de werkingssfeer van de AVG. Gegevensverwerking die wordt voorgeschreven in nationale wetgeving die de PNR–richtlijn omzet, valt daarentegen op grond van de uitzondering in artikel 2, lid 2, onder *d)*, AVG buiten de werkingssfeer van deze verordening, mits de tweede in punt 67 van dit arrest aangehaalde voorwaarde is vervuld, namelijk dat de verwerking gebeurt door een bevoegde autoriteit in de zin van laatstgenoemde bepaling.

78. In verband met deze tweede voorwaarde heeft het Hof geoordeeld dat de in artikel 3, punt 7, van richtlijn 2016/680 gegeven definitie van ' bevoegde autoriteit ' naar analogie behoort te gelden voor artikel 2, lid 2, onder *d)*, AVG [zie in die zin arrest van 22 juni 2021, *Latvijas Republikas Saeima (Strafpunten)*, C—439/19, EU:C:2021:504, punt 69].

79. Volgens de artikelen 4 en 7 van de PNR–richtlijn moet elke lidstaat een instantie aanwijzen die als PIE bevoegd is om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen, alsook een lijst opstellen van de instanties die de PIE om PNR–gegevens of het verwerkingsresultaat van deze gegevens mogen verzoeken of dergelijke gegevens of het verwerkingsresultaat ervan van de PIE mogen ontvangen. Artikel 7, lid 2, van deze richtlijn verduidelijkt dat ook deze instanties bevoegd moeten zijn om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen.

80. Bijgevolg voldoet de door de PIE en de door deze bevoegde instanties voor deze doeleinden verrichte PNR–gegevensverwerking aan de twee voorwaarden van punt 67 van dit arrest en valt deze verwerking dus niet alleen onder de PNR–richtlijn zelf maar ook onder richtlijn 2016/680, en niet onder de AVG, wat overweging 27 van de PNR–richtlijn overigens bevestigt.

81. Marktdeelnemers, zoals luchtvaartmaatschappijen, worden daarentegen niet door deze richtlijn gemachtigd om openbaar gezag of openbare bevoegdheden uit te oefenen en kunnen dus, ondanks hun juridische verplichting om PNR–gegevens door te geven, niet beschouwd worden als bevoegde autoriteiten in de zin van artikel 3, lid 7, van richtlijn 2016/680 en artikel 2, lid 2, onder *d)*, AVG, zodat het verzamelen van deze gegevens door luchtvaartmaatschappijen en het doorgeven ervan aan de PIE onder deze verordening vallen. Hetzelfde geldt in een situatie als die waarin de wet van 25 december 2016 voorziet, waarin het verzamelen en doorgeven gebeurt door andere vervoerders of door reisoperatoren.

82. Tot slot vraagt de verwijzende rechter zich af wat de mogelijke gevolgen zijn van het feit dat nationale wetgeving tegelijkertijd de PNR–richtlijn, de API–richtlijn en richtlijn 2010/65 beoogt om te zetten, zoals het geval is bij de wet van 25 december 2016. In dit verband zij eraan herinnerd dat, zoals uit de punten 72 en 75 tot en met 77 van dit arrest blijkt, de gegevensverwerking die bij deze twee laatste richtlijnen wordt voorgeschreven, binnen de werkingssfeer van de AVG valt, die algemene regels bepaalt voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

83. Gegevensverwerking die op basis van die wetgeving gebeurt en die onder de API–richtlijn en/of richtlijn 2010/65 valt, is dus onderworpen aan de AVG. Hetzelfde geldt voor gegevensverwerking die op diezelfde basis gebeurt en die, wegens de doelstelling ervan, niet alleen onder de PNR–richtlijn maar ook onder de API–richtlijn en/of richtlijn 2010/65 valt. Wanneer gegevensverwerking die op die basis gebeurt tot slot wegens de doelstelling ervan enkel onder de PNR–richtlijn valt, is de AVG van toepassing voor zover het de verzameling en doorgifte van PNR–gegevens aan de PIE door de luchtvaartmaatschappijen betreft. Gebeurt deze verwerking daarentegen door de PIE of door de bevoegde autoriteiten voor de in artikel 1, lid 2, van de PNR–richtlijn genoemde doeleinden, dan valt die onder het nationale recht en onder richtlijn 2016/680.

84. Gelet op de voorgaande overwegingen dient op de eerste vraag te worden geantwoord dat artikel 2, lid 2, onder *d)*, en artikel 23 AVG aldus moeten worden uitgelegd dat de AVG van toepassing is op de verwerking van persoonsgegevens die wordt voorgeschreven in nationale wetgeving die tegelijkertijd de API-richtlijn, richtlijn 2010/65 en de PNR–richtlijn in nationaal recht beoogt om te zetten, wanneer de verwerking door particuliere marktdeelnemers gebeurt of wanneer zij door overheidsinstanties wordt verricht en enkel of ook onder de API–richtlijn of richtlijn 2010/65 valt. Die verordening is daarentegen niet van toepassing op door dergelijke wetgeving voorgeschreven gegevensverwerking die enkel onder de PNR–richtlijn valt, die de PIE of de bevoegde autoriteiten verrichten voor de doeleinden die worden genoemd in artikel 1, lid 2, van deze richtlijn ».

B.21.4. Uit hetgeen voorafgaat, vloeit voort dat de AVG van toepassing is op de verwerking van persoonsgegevens waarin een nationale wetgeving voorziet, zoals de wet van 25 december 2016, die ertoe strekt tegelijk de bepalingen van de PNR–richtlijn, van de API–richtlijn en van de richtlijn 2010/65/EU om te zetten, ofwel (1) wanneer een gegevensverwerking die op basis van die wetgeving gebeurt, onder de API–richtlijn en/of de richtlijn 2010/65/EU valt, ofwel (2) wanneer een gegevensverwerking die op diezelfde basis gebeurt, wegens de doelstelling ervan niet alleen onder de PNR–richtlijn maar ook onder de API–richtlijn en/of de richtlijn 2010/65/EU valt, ofwel (3) wanneer een gegevensverwerking die op basis van die wetgeving gebeurt, wegens de doelstelling ervan enkel onder de PNR–richtlijn valt, maar het gaat om de verzameling en doorgifte van PNR-gegevens aan de PIE door de luchtvaartmaatschappijen of andere vervoerders, of reisoperatoren betreft.

Daarentegen, wanneer een gegevensverwerking die op basis van dezelfde wetgeving gebeurt, wegens de doelstelling ervan alleen valt onder de PNR–richtlijn en gebeurt door de PIE of door de bevoegde autoriteiten voor de in artikel 1, lid 2, van de PNR–richtlijn genoemde doeleinden, dan is de AVG niet van toepassing, maar valt die verwerking onder het nationaal recht en onder de Politierichtlijn.

B.21.5. Het Hof houdt derhalve, in het onderzoek van het middel, rekening met artikel 23 van de AVG, behalve wanneer de gegevensverwerking die gebeurt op basis van de wet van 25 december 2016, wegens de doelstelling ervan, alleen valt onder de PNR–richtlijn, en wanneer die gebeurt door de PIE of de bevoegde autoriteiten voor de in artikel 1, lid 2, van de PNR–richtlijn genoemde doeleinden.

B.21.6. Voor het overige stelt het Hof vast dat de verzoekende partijen uit die bepaling geen andere argumenten afleiden dan die welke zijn afgeleid uit de schending van de artikelen 7 en 8 van het Handvest.

B.21.7. De exceptie van de Ministerraad wordt in die mate verworpen.

Wat betreft de geldigheid van de PNR–richtlijn

B.22.1. Op vragen van het Hof over de geldigheid van de PNR–richtlijn heeft het Hof van Justitie, in het voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geantwoord dat « een uitlegging van de PNR–richtlijn in het licht van de artikelen 7, 8 en 21 en artikel 52, lid 1, van het Handvest [garandeert] dat deze richtlijn in overeenstemming is met deze artikelen van het Handvest, en [...] het onderzoek van de tweede tot en met de vierde vraag en de zesde vraag dus niet gebleken [is] van feiten of omstandigheden die de geldigheid van deze richtlijn kunnen aantasten » (punt 228).

B.22.2. Inleidend herinnert het Hof van Justitie eraan dat, « een Uniehandeling volgens een algemeen uitleggingsbeginsel zoveel mogelijk aldus moet worden uitgelegd dat geen afbreuk wordt gedaan aan de geldigheid ervan en dat het gehele primaire recht, waaronder met name de bepalingen van het Handvest, in acht wordt genomen » (punt 86), en dat de lidstaten « bij de tenuitvoerlegging van die maatregelen niet alleen hun nationale recht conform deze richtlijn moeten uitleggen, maar er ook op moeten toezien dat zij zich niet baseren op een uitlegging van deze richtlijn die in conflict zou komen met de door de rechtsorde van de Unie beschermde grondrechten of de andere algemene beginselen die in deze rechtsorde worden erkend » (punt 87).

Wat betreft de PNR–richtlijn merkt het Hof van Justitie op dat « in de overwegingen 15, 20, 22, 25, 36 en 37 met de verwijzing naar een hoog niveau van gegevensbescherming wordt benadrukt hoeveel belang de Uniewetgever hecht aan de volledige eerbiediging van de in de artikelen 7, 8 en 21 van het Handvest neergelegde grondrechten en van het evenredigheidsbeginsel » (punt 88), alsook dat « artikel 19, lid 2, van de PNR–richtlijn de Commissie de verplichting [oplegt] om bij de evaluatie van deze richtlijn bijzondere aandacht te besteden aan ‘ de naleving van de geldende normen voor de bescherming van persoonsgegevens ’, ‘ de noodzakelijkheid en evenredigheid van het verzamelen en het verwerken van PNR-gegevens voor elk van de in deze richtlijn genoemde doelen ’ en ‘ de lengte van de bewaartermijn ’ » (punt 90).

B.22.3. Ten aanzien van de inmengingen die voortvloeien uit de PNR–richtlijn in de grondrechten die zijn gewaarborgd bij de artikelen 7 en 8 van het Handvest, stelt het Hof van Justitie vast dat de PNR–richtlijn « inmengingen van een zekere ernst in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten met zich brengt, met name voor zover deze richtlijn een systeem van permanente, niet-gerichte en systematische controle beoogt in te voeren waarbij de persoonsgegevens van iedereen die luchtvervoerdiensten gebruikt automatisch worden beoordeeld » (punt 111) :

« 97. Aldus vormt zowel de doorgifte van de PNR-gegevens door de luchtvaartmaatschappijen aan de PIE van de betrokken lidstaat [artikel 1, lid 1, onder *a)*, *juncto* artikel 8 van de PNR–richtlijn] als de afbakening van de voorwaarden inzake de bewaring en het gebruik van deze gegevens en de eventuele latere doorgifte ervan aan de bevoegde autoriteiten van deze lidstaat, de PIE’s en de bevoegde autoriteiten van andere lidstaten, Europol of autoriteiten van derde landen – zoals toegestaan door met name de artikelen 6, 7, 9 en 10 tot en met 12 van deze richtlijn – een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten.

98. Wat de ernst van deze inmenging betreft, zij er ten eerste op gewezen dat de PNR–richtlijn volgens artikel 1, lid 1, onder *a)*, *juncto* artikel 8 ervan voorziet in een stelselmatige, continue doorgifte aan de PIE’s van de PNR–gegevens van iedereen die een vlucht naar of vanuit een derde land in de zin van artikel 3, punt 2, ervan neemt, dat wil zeggen tussen een derde land en de Unie. Zoals de advocaat–generaal in punt 73 van zijn conclusie heeft opgemerkt, betekent dit dat de PIE’s algemene toegang hebben tot alle meegedeelde PNR–gegevens van alle personen die een vlucht nemen, ongeacht welk gebruik daar later van wordt gemaakt.

99. Ten tweede bepaalt artikel 2 van de PNR–richtlijn in lid 1 dat de lidstaten kunnen beslissen om deze richtlijn toe te passen op vluchten binnen de EU in de zin van artikel 3, punt 3, ervan, en in lid 2 dat in dit geval alle bepalingen van deze richtlijn ‘ van toepassing [zijn] op vluchten binnen de EU alsof het om vluchten naar of vanuit derde landen gaat, en op de PNR–gegevens van vluchten binnen de EU alsof het om PNR–gegevens gaat van vluchten naar of vanuit derde landen ’.

100. Ten derde lijken bepaalde van de in bijlage I bij de PNR–richtlijn opgesomde PNR–gegevens – die worden samengevat in punt 93 van dit arrest – op zichzelf beschouwd weliswaar geen nauwkeurige informatie te kunnen verschaffen over het privéleven van de betrokkenen, maar kunnen zij samen beschouwd onder meer een volledige reisroute blootleggen, inzicht geven in reisgewoontes en relaties tussen twee of meer personen, inlichtingen verschaffen over de financiële situatie van luchtreizigers, hun voedingsgewoonten of hun gezondheidstoestand, en zelfs gevoelige gegevens over deze passagiers onthullen [zie in die zin advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 128].

101. Ten vierde is het volgens artikel 6, lid 2, onder *a)* en *b)*, van de PNR–richtlijn de bedoeling dat de door de luchtvaartmaatschappijen doorgegeven gegevens niet alleen op voorhand worden beoordeeld, vóór de geplande aankomst of het geplande vertrek van de passagiers, maar ook achteraf.

102. Uit artikel 6, lid 2, onder *a)*, en lid 3, van de PNR–richtlijn blijkt dat de PIE’s van de lidstaten de voorafgaande beoordeling systematisch en met geautomatiseerde middelen verrichten, dat wil zeggen continu en ongeacht of er aanwijzingen zijn dat de personen in kwestie mogelijkerwijs betrokken zijn bij terrorisme of ernstige criminaliteit, en dat de PNR–gegevens daarbij kunnen worden vergeleken met ‘ databanken die relevant zijn ’ en kunnen worden verwerkt aan de hand van ‘ vooraf bepaalde criteria ’.

103. In dit verband zij eraan herinnerd dat het Hof reeds heeft geoordeeld dat de mate waarin de geautomatiseerde verwerking van de PNR–gegevens een inmenging oplevert in de rechten die in de artikelen 7 en 8 zijn verankerd, hoofdzakelijk afhangt van de vooraf vastgestelde modellen en criteria en de databanken waarop dit type van gegevensverwerking is gebaseerd [advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 172].

104. Zoals de advocaat–generaal in punt 78 van zijn conclusie heeft opgemerkt, kunnen met de verwerking die in artikel 6, lid 3, onder *a)*, van de PNR–richtlijn wordt voorgeschreven – het vergelijken van de PNR–gegevens met ‘ databanken die relevant zijn ’ – aanvullende gegevens over het privéleven van de luchtreizigers worden verkregen en daar zeer precieze conclusies over worden getrokken.

105. Wat de verwerking van PNR–gegevens aan de hand van ‘ vooraf bepaalde criteria ’ betreft [artikel 6, lid 3, onder *b)*, van de PNR–richtlijn], vereist artikel 6, lid 4, van deze richtlijn dat de beoordeling van passagiers op basis van dergelijke criteria op niet–discriminerende wijze gebeurt en met name zonder dat wordt gekeken naar een reeks in de laatste volzin van dit lid 4 genoemde kenmerken. De gekozen criteria moeten bovendien doelgericht, evenredig en specifiek zijn.

106. Het Hof heeft evenwel reeds geoordeeld dat geautomatiseerde analyses van PNR–gegevens, aangezien zij worden uitgevoerd op basis van niet–geverifieerde persoonsgegevens en gebaseerd zijn op vooraf vastgestelde modellen en criteria, noodzakelijkerwijs een zekere foutenmarge vertonen [zie naar analogie advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 169]. Zoals de advocaat–generaal in punt 78 van zijn conclusie in wezen heeft aangegeven, blijkt met name uit het werkdocument van de Commissie [SWD(2020) 128 final] dat als bijlage bij haar verslag van 24 juli 2020 over de evaluatie van de PNR–richtlijn is gevoegd, dat het aantal positieve overeenkomsten dat geautomatiseerde verwerking als bedoeld in artikel 6, lid 3, onder *a)* en *b)*, van deze richtlijn oplevert en dat na een afzonderlijke niet-geautomatiseerde controle onjuist blijkt te zijn, vrij aanzienlijk is en in 2018 en 2019 minstens vijf op de zes geïdentificeerde personen bedroeg. Die verwerking draait dus uit op een uitgebreide analyse van de PNR–gegevens van deze personen.

107. Wat betreft de beoordeling achteraf van PNR–gegevens als bedoeld in artikel 6, lid 2, onder *b)*, van de PNR–richtlijn, blijkt uit deze bepaling dat de PIE gedurende de in artikel 12, lid 2, van deze richtlijn genoemde termijn van zes maanden na de doorgifte van die gegevens verplicht is om deze in bepaalde gevallen op verzoek van de bevoegde instanties te verstrekken en te verwerken voor het bestrijden van terroristische misdrijven of ernstige criminaliteit.

108. Zelfs nadat de PNR–gegevens na het verstrijken van die termijn van zes maanden zijn gedepersonaliseerd – door bepaalde elementen ervan af te schermen – kan de PIE overeenkomstig artikel 12, lid 3, van de PNR–richtlijn gehouden zijn de bevoegde instanties op verzoek de volledige PNR–gegevens mee te delen in een vorm die het mogelijk maakt de betrokkene te identificeren, mits er redelijkerwijs kan worden aangenomen dat dit noodzakelijk is voor de in artikel 6, lid 2, onder *b)*, van deze richtlijn genoemde doelstellingen en hiervoor goedkeuring is gegeven door een gerechtelijke instantie of een ‘ andere nationale instantie die [...] bevoegd is ’.

109. Ten vijfde bepaalt artikel 12, lid 1, van de PNR–richtlijn zonder verdere precisering dat PNR–gegevens in een databank worden bewaard gedurende een termijn van vijf jaar nadat zij zijn doorgegeven aan de PIE van de lidstaat waar de vlucht aankomt of vertrekt. Aangezien de gegevens – ondanks de depersonalisering ervan na de initiële termijn van zes maanden, door afscherming van bepaalde elementen – nog integraal kunnen worden meegedeeld in het in het vorige punt genoemde geval, is het dus mogelijk om gedurende een periode die het Hof in zijn advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017 (EU:C:2017:592, punt 132) erg lang heeft genoemd, te beschikken over informatie over het privéleven van de luchtreizigers.

110. Aangezien er regelmatig vliegtuigreizen worden gemaakt, impliceert een dergelijke bewaartermijn dat voor een zeer groot deel van de Uniebevolking herhaaldelijk PNR–gegevens worden bewaard in het kader van het door de PNR–richtlijn ingestelde systeem, en dus gedurende lange tijd – en zelfs onbepaalde tijd bij personen die meer dan eens in de vijf jaar het vliegtuig nemen – beschikbaar zijn om door de PIE en de bevoegde autoriteiten te worden geanalyseerd bij de beoordelingen vooraf en achteraf ».

B.22.4.1. Ten aanzien van de rechtvaardiging van de inmengingen die voortvloeien uit de PNR–richtlijn herinnert het Hof van Justitie inzonderheid eraan dat « bij de beoordeling of de lidstaten een beperking van de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten kunnen rechtvaardigen, [moet] worden bepaald wat de ernst is van de inmenging die een dergelijke beperking meebrengt, en worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst » (punt 116) :

« 117. De betrokken regeling die de inmenging bevat, voldoet slechts aan het evenredigheidsvereiste indien zij duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de daarin bepaalde maatregelen bevat die minimale eisen opleggen, zodat degenen van wie de gegevens zijn doorgegeven over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. Zij moet in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens geautomatiseerd worden verwerkt. Deze overwegingen gelden inzonderheid wanneer de PNR–gegevens gevoelige informatie over de passagiers kunnen onthullen [advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 141, en arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C—511/18, C—512/18 en C—520/18, EU:C:2020:791, punt 132 en aldaar aangehaalde rechtspraak].

118. Een regeling die voorziet in de bewaring van persoonsgegevens moet derhalve steeds beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel [zie in die zin advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 191 en aldaar aangehaalde rechtspraak, en arresten van 3 oktober 2019, A e.a., C—70/18, EU:C:2019:823, punt 63, en 6 oktober 2020, *La Quadrature du Net e.a.*, C—511/18, C—512/18 en C—520/18, EU:C:2020:791, punt 133].

a) Eerbiediging van het wettigheidsbeginsel en van de wezenlijke inhoud van de betrokken grondrechten

119. De beperking op de uitoefening van de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten die voortvloeit uit het systeem van de PNR–richtlijn, is ingevoerd bij een wetgevingshandeling van de Unie. Wat betreft de vraag of deze richtlijn, als Uniehandeling die de inmenging in deze rechten toestaat, in overeenstemming met de in punt 114 van dit arrest aangehaalde rechtspraak zelf de reikwijdte van de beperking op de uitoefening van deze rechten bepaalt, moet worden vastgesteld dat deze richtlijn en de bijlagen I en II daarbij een opsomming van de PNR–gegevens bevatten alsook een kader voor de verwerking ervan met onder meer de doelstellingen van en de nadere regels voor die verwerking. Deze vraag valt voor de rest grotendeels samen met de vraag of is voldaan aan het in punt 117 van het onderhavige arrest aangehaalde evenredigheidsvereiste (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C—311/18, EU:C:2020:559, punt 180), en zal hierna worden onderzocht in de punten 125 e.v.

120. Wat de eerbiediging van de wezenlijke inhoud van de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten betreft, moet worden erkend dat PNR–gegevens in voorkomend geval zeer precieze informatie over het privéleven van een persoon kunnen onthullen. Toch kan niet met de in deze richtlijn bedoelde gegevens alleen een compleet beeld van iemands privéleven worden gegeven, ten eerste omdat deze gegevens slechts bepaalde aspecten van het privéleven betreffen, die met name met vliegtuigreizen te maken hebben, en ten tweede omdat artikel 13, lid 4, van de PNR–richtlijn de verwerking van gevoelige gegevens in de zin van artikel 9, lid 1, AVG uitdrukkelijk verbiedt. Bovendien worden in artikel 1, lid 2, juncto artikel 3, punten 8 en 9, van deze richtlijn en bijlage II daarbij de doeleinden van de verwerking van deze gegevens afgebakend. Ten slotte bevatten de artikelen 4 tot en met 15 van deze richtlijn regels voor de doorgifte, de verwerking en de bewaring van deze gegevens en regels om met name de beveiliging, de vertrouwelijkheid en de integriteit van deze gegevens te verzekeren en om ze te beschermen tegen illegale toegang en verwerking. Bijgevolg doen de inmengingen die de PNR–richtlijn met zich brengt, geen afbreuk aan de wezenlijke inhoud van de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten.

b) Doelstelling van algemeen belang en geschiktheid van de « PNR-gegevensverwerking » daarvoor

121. Wat betreft de vraag of het bij de PNR–richtlijn ingestelde systeem een doelstelling van algemeen belang nastreeft, blijkt uit de overwegingen 5, 6 en 15 ervan dat deze richtlijn tot doel heeft de interne veiligheid van de EU te garanderen en zodoende het leven en de veiligheid van personen te beschermen, en een juridisch kader te creëren dat garandeert dat wanneer PNR–gegevens door de bevoegde autoriteiten worden verwerkt, de grondrechten van de passagiers – en met name het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens – in hoge mate worden beschermd.

122. Hiertoe bepaalt artikel 1, lid 2, van de PNR–richtlijn dat overeenkomstig deze richtlijn verzamelde PNR–gegevens uitsluitend mogen worden verwerkt als bedoeld in artikel 6, lid 2, onder *a)* tot en met *c)*, ervan om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen. Deze doelstellingen vormen duidelijk doelstellingen van algemeen belang van de Unie die – zelfs zware – inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten kunnen rechtvaardigen [zie in die zin arrest van 8 april 2014, *Digital Rights Ireland e.a.*, C—293/12 en C—594/12, EU:C:2014:238, punt 42, en advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punten 148 en 149].

123. Wat betreft de geschiktheid van het door de PNR–richtlijn ingestelde systeem om de beoogde doelstellingen te bereiken, moet worden geconstateerd dat de kans op ' vals negatieve ' resultaten en het feit dat de bij deze richtlijn voorgeschreven geautomatiseerde verwerking, zoals in punt 106 van het onderhavige arrest is aangegeven, in 2018 en 2019 een vrij groot aantal ' vals–positieve ' resultaten heeft opgeleverd, dit systeem minder geschikt kunnen maken. Toch is dit systeem daarom nog niet ongeschikt om de doelstelling van bestrijding van terroristische misdrijven en ernstige criminaliteit te helpen bereiken. Zoals uit het in punt 106 van dit arrest vermelde werkdocument van de Commissie blijkt, zijn dankzij de geautomatiseerde verwerking die op grond van deze richtlijn wordt uitgevoerd, immers al daadwerkelijk vliegtuigpassagiers geïdentificeerd die een risico vormden in termen van terroristische misdrijven en ernstige criminaliteit.

124. Gelet op de foutenmarge die inherent is aan de geautomatiseerde verwerking van PNR–gegevens en met name op het vrij groot aantal ' vals-positieve ' resultaten, hangt de geschiktheid van het bij de PNR–richtlijn ingestelde systeem bovendien voornamelijk af van de goede werking van de daaropvolgende controle – met niet–geautomatiseerde middelen – van de verwerkingsresultaten, wat volgens deze richtlijn een taak van de PIE is. De bepalingen die met het oog daarop in deze richtlijn zijn opgenomen, dragen dus bij aan de verwezenlijking van die doelstellingen ».

B.22.4.2. In verband met de noodzakelijkheid van de door de PNR–richtlijn veroorzaakte inmengingen herinnert het Hof van Justitie eraan dat « moet worden nagegaan of de uit de PNR–richtlijn resulterende inmenging tot het strikt noodzakelijke beperkt is en, in het bijzonder, of deze richtlijn duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de daarin bepaalde maatregelen bevat en of het systeem van deze richtlijn steeds beantwoordt aan objectieve criteria die een verband leggen tussen de PNR-gegevens, die nauw samenhangen met het reserveren en maken van vliegreizen, en de doelstellingen van deze richtlijn, namelijk het bestrijden van terroristische misdrijven en ernstige criminaliteit » (punt 125).

Het Hof van Justitie besluit dat het geen enkel element heeft opgemerkt dat de geldigheid van de PNR–richtlijn kan aantasten daar « een uitlegging van de PNR–richtlijn in het licht van de artikelen 7, 8 en 21 en artikel 52, lid 1, van het Handvest [garandeert] dat deze richtlijn in overeenstemming is met deze artikelen van het Handvest » (punt 228), waardoor de grenzen van het strikt noodzakelijke in acht zijn genomen, waarbij verschillende verduidelijkingen worden geformuleerd in verband met (1) de gegevens van de luchtreizigers bedoeld in de PNR–richtlijn (punten 126–140), (2) de doeleinden van de PNR-gegevensverwerking (punten 141–152), (3) het verband tussen de PNR-gegevens en de doeleinden van de verwerking van die gegevens (punten 153–157), (4) de betrokken luchtreizigers en vluchten (punten 158–175), (5) de voorafgaande beoordeling van PNR-gegevens via geautomatiseerde verwerking (punten 176–213) en (6) het achteraf verstrekken en beoordelen van PNR-gegevens (punten 214–227).

B.22.5. Bij het onderzoek van het middel houdt het Hof rekening met die verduidelijkingen die het Hof van Justitie formuleert in verband met de uitlegging van de PNR–richtlijn.

Wat betreft de volgorde van het onderzoek van de grieven

B.23.1. Uit het onderzoek van het eerste middel en van de bestreden bepalingen blijkt dat de verzoekende partij meerdere aspecten van de wet van 25 december 2016 bekritiseert.

B.23.2. Bij zijn arrest nr. 135/2019 van 17 oktober 2019 heeft het Hof geoordeeld dat het middel niet gegrond is in zoverre het is gericht tegen de uitvoeringsmodaliteiten van de wet van 25 december 2016 (artikelen 3, § 2, en 7, § 3 – B.21 tot B.29) en tegen de begrippen « identiteitsdocumenten » en « reisdocumenten » (artikel 7, §§ 1 en 2 – B.30 tot B.33).

B.23.3. De grieven die nog moeten worden onderzocht, rekening houdend met het antwoord van het Hof van Justitie in zijn arrest van 21 juni 2022, zijn gericht tegen de volgende aspecten :

1. de beoogde gegevens (artikelen 4, 9°, en 9) (B.24-B.34);

2. het begrip « passagier » (artikel 4, 10°) (B.35-B.41);

3. de doeleinden van de PNR–gegevensverwerking (artikel 8) (B.42-B.56);

4. het beheer van de passagiersgegevensbank en de gegevensverwerking in het kader van de voorafgaande beoordeling van de passagiers en de gerichte opzoekingen (artikelen 12 tot 16 en 24 tot 27 en artikelen 50 en 51) (B.57-B.70);

5. de bewaartermijn van de PNR-gegevens (artikel 18) (B.71–B.75).

1. *De beoogde gegevens (artikelen* 4, 9°, *en* 9*)*

B.24. De verzoekende partij voert in de eerste plaats aan dat het zeer ruime toepassingsgebied met betrekking tot de passagiersgegevens die worden beoogd in de artikelen 4, 9°, en 9, van de wet van 25 december 2016 kennelijk onevenredig is ten aanzien van het nagestreefde doel. De verzoekende partij is van mening dat op zijn minst de categorie van gegevens die worden beoogd in artikel 9, § 1, 12°, van de bestreden wet, zou moeten worden begrensd.

Bovendien zouden de beoogde gegevens, volgens de verzoekende partij, gevoelige gegevens, zoals het lidmaatschap van een vakorganisatie, de persoonlijke affiniteit en de persoonlijke of professionele relaties, kunnen onthullen.

B.25.1. Overeenkomstig de beginselen waaraan wordt herinnerd in B.17 en B.18, moet een inmenging in het recht op eerbiediging van het privéleven door middel van een verwerking van persoonsgegevens, te dezen door een toegang van overheidsdiensten tot en het gebruik van bepaalde persoonsgegevens via bijzondere technieken (EHRM, 26 maart 1987, *Leander t. Zweden*, ECLI:CE:ECHR:1987:0326JUD000924881, § 48; grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, ECLI:CE:ECHR:2000:0504JUD002834195, § 46; HvJ, grote kamer, 8 april 2014, C—293/12, *Digital Rights Ireland Ltd*, en C—594/12, *Kärntner Landesregierung e.a.*, ECLI:EU:C:2014:238) berusten op een redelijke verantwoording en dient zij evenredig te zijn met de door de wetgever nagestreefde doelstellingen.

B.25.2. Wat de evenredigheid betreft, houden het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie rekening met het al dan niet aanwezig zijn van de in B.19 vermelde materiële en procedurele waarborgen in de betrokken regeling.

Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens, dient aldus rekening te worden gehouden met, onder meer, het geautomatiseerde karakter ervan, de gebruikte technieken, de accuraatheid, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van afdoende controlerechten en rechtsmiddelen voor de betrokkenen, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt, het onderscheidend karakter van de regeling en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik en misbruik van de verwerkte persoonsgegevens door de overheidsdiensten (EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, ECLI:CE:ECHR:2000:0504JUD002834195, § 59; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 101–103, 119, 122 en 124; 18 april 2013, *M.K. t. Frankrijk*, ECLI:CE:ECHR:2013:0418JUD001952209, §§ 37 en 42–44; 18 september 2014, *Brunet t. Frankrijk*, ECLI:CE:ECHR:2014:0918JUD002101010, §§ 35–37; 12 januari 2016, *Szabó en Vissy t. Hongarije*, ECLI:CE:ECHR:2016:0112JUD003713814, § 68; HvJ, grote kamer, 8 april 2014, C—293/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238, punten 56—66).

B.25.3. In zijn advies 1/15 van 26 juli 2017 heeft het Hof van Justitie eveneens eraan herinnerd dat een inmenging in het recht op bescherming van de persoonsgegevens tot het « strikt noodzakelijke » moet worden beperkt :

« 140. Wat de inachtneming van het evenredigheidsbeginsel betreft, vereist de bescherming van het grondrecht op eerbiediging van het privéleven op het niveau van de Unie — volgens vaste rechtspraak van het Hof — dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (arresten van 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07, EU:C:2008:727, punt 56; 8 april 2014, *Digital Rights Ireland e.a.*, C—293/12 en C-594/12, EU:C:2014:238, punten 51 en 52; 6 oktober 2015, *Schrems*, C—362/14, EU:C:2015:650, punt 92, en 21 december 2016, *Tele*2 *Sverige en Watson e.a.*, C-203/15 en C—698/15, EU:C:2016:970, punten 96 en 103).

141. De betrokken regeling die de inmenging bevat, voldoet slechts aan dit vereiste indien zij duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel bevat die minimale eisen opleggen, zodat degenen van wie de gegevens zijn doorgegeven over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. Zij moet in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens geautomatiseerd worden verwerkt. Deze overwegingen gelden inzonderheid wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, *Tele*2 *Sverige en Watson e.a.*, C—203/15 en C-698/15, EU:C:2016:970, punten 109 en 117; zie in die zin eveneens arrest EHRM, 4 december 2008, *S. en Marper tegen Verenigd Koninkrijk*, CE:ECHR:2008:1204JUD003056204, punt 103) ».

B.26.1. Artikel 4, 9°, van de wet van 25 december 2016 definieert de « PNR » als zijnde « het bestand met de reisgegevens van iedere passagier, dat de in artikel 9 bedoelde informatie bevat ». Zoals is vermeld in B.4.1, maakt artikel 9 van de wet van 25 december 2016 een onderscheid tussen, enerzijds, de voorafgaande gegevens van de check-in-status en het instappen (API-gegevens) zoals bedoeld in artikel 9, § 1, 18°, die exhaustief zijn opgesomd in artikel 9, § 2, van de wet van 25 december 2016, en, anderzijds, de reservatiegegevens (PNR-gegevens), die maximaal de 19 elementen bevatten die exhaustief zijn opgesomd in artikel 9, § 1, van de wet van 25 december 2016, waaronder de API-gegevens zoals bedoeld in artikel 9, § 1, 18°.

Het onderscheid tussen API-gegevens en PNR-gegevens wordt geëxpliciteerd in de in B.3 geciteerde parlementaire voorbereiding.

B.26.2.1. De parlementaire voorbereiding betreffende artikel 9 van de wet van 25 december 2016 zet uiteen :

« Artikel 9 bepaalt welke passagiersgegevens moeten worden doorgestuurd. Deze gegevens worden doorgestuurd via een opgelegd en eenvormig dataformaat per vervoersector en reisoperator, waarvoor gebruik wordt gemaakt van een internationaal aanvaarde norm (voor luchtvaartmaatschappijen is dit bijvoorbeeld het formaat PNRGOV, ontwikkeld door IATA/ICAO/WCO).

Artikel 9 maakt een onderscheid tussen, enerzijds, de in § 1 bedoelde reservatiegegevens en, anderzijds, de in § 2 vermelde check-in– en instapgegevens » (*Parl. St.*, Kamer, 2015-2016, DOC 54–2069/001, pp. 20-21).

Dat onderscheid komt overeen met het onderscheid tussen de gegevens die worden beoogd door de API-richtlijn en die welke worden beoogd door de PNR-richtlijn.

B.26.2.2. De door de wet van 25 december 2016 georganiseerde doorgifte van passagiersgegevens houdt voor de vervoerders en reisoperatoren evenwel geen verplichting in om meer gegevens te verzamelen dan die waarover zij reeds beschikken :

« De vervoerders en reisoperatoren verzamelen en verwerken de gegevens van hun passagiers reeds voor commerciële doeleinden. De luchtvaartmaatschappijen bijvoorbeeld bewaren zowel op voorhand af te geven passagiersgegevens (API-gegevens) als PNR–gegevens, maar dit is niet algemeen. De API-gegevens zijn onder meer de gegevens die worden afgelezen van de ' *machine readable zone* ' van het identiteitsdocument. Conform de EU-PNR-Richtlijn dienen de vervoerders en reisoperatoren enkel de data door te geven waarover ze reeds beschikken en dienen ze geen aanvullende gegevens te verzamelen of te bewaren van passagiers. Ze dienen evenmin passagiers te verplichten om nog meer gegevens aan hen te verstrekken dan thans het geval is » (*ibid.*, pp. 15-16).

De overwegingen 8 en 9 van de PNR-richtlijn geven in dat verband eveneens aan :

« (8) Luchtvaartmaatschappijen verzamelen en verwerken PNR-gegevens van hun passagiers reeds voor hun eigen commerciële doeleinden. Deze richtlijn mag niet voorschrijven dat de luchtvaartmaatschappijen ertoe worden verplicht aanvullende gegevens bij passagiers te verzamelen of deze te bewaren, en evenmin dat passagiers ertoe worden verplicht nog meer gegevens aan de luchtvaartmaatschappijen te verstrekken dan thans het geval is.

(9) Sommige luchtvaartmaatschappijen bewaren de API-gegevens die zij verzamelen als onderdeel van de PNR-gegevens, andere niet. Het gecombineerde gebruik van PNR– en API–gegevens biedt meerwaarde doordat het de lidstaten helpt bij de identiteitscontrole van personen, waardoor uit het oogpunt van rechtshandhaving dat resultaat aan waarde wint, en het risico wordt beperkt dat onschuldige personen het voorwerp uitmaken van controle en onderzoek. Daarom moet er beslist voor worden gezorgd dat luchtvaartmaatschappijen die API–gegevens verzamelen, deze doorgeven, ongeacht of zij API-gegevens bewaren door middel van andere technische middelen dan voor PNR-gegevens ».

B.27.1. Wat de API-gegevens betreft, bepaalt artikel 3, lid 2, van de API-richtlijn dat de informatie over de passagiers die de luchtvervoerders zullen vervoeren naar een aangewezen grensdoorlaatpost via welke die personen het grondgebied van een lidstaat binnenkomen, onder meer de volgende inlichtingen bevat :

« - het nummer en de aard van het gebruikte reisdocument,

- de nationaliteit,

- de volledige naam,

- de geboortedatum,

- de grensdoorlaatpost van binnenkomst op het grondgebied van de lidstaten,

- het vervoermiddel,

- het tijdstip van vertrek en van aankomst van het vervoermiddel,

- het totale aantal met dat vervoermiddel vervoerde passagiers,

- het eerste instappunt ».

B.27.2.1. Voorheen waren de luchtvervoerders reeds verplicht om de API-gegevens door te geven, overeenkomstig het koninklijk besluit van 11 december 2006, dat werd opgeheven bij artikel 10 van het koninklijk besluit van 18 juli 2017.

De parlementaire voorbereiding van de wet van 25 december 2016 bevestigt immers :

« Het [voorontwerp] van wet herneemt in hoofdzaak het regime dat voorzien wordt door het hierboven genoemd koninklijk besluit van 11 december 2006 betreffende de verplichting voor luchtvervoerders om passagiersgegevens door te geven. De door dit voorontwerp van wet voorziene lijst van de ' API '-gegevens komt in hoofdzaak dus overeen met de lijst die door dit besluit is opgesteld.

Het toepassingsgebied van het voorontwerp van wet is echter groter dan het toepassingsgebied van de richtlijn 2004/82/EG, omdat de aan de vervoerders opgelegde verplichting tot alle transportsectoren wordt uitgebreid » (*ibid.*, p. 11).

B.27.2.2. Vóór de opheffing ervan bij het koninklijk besluit van 18 juli 2017, beoogde artikel 3, § 2, van het koninklijk besluit van 11 december 2006, als inlichtingen die door de luchtvaartmaatschappijen moesten worden doorgegeven :

« 1° het nummer en de aard van het gebruikte reisdocument;

2° de nationaliteit;

3° de volledige naam;

4° de geboortedatum;

5° de grensdoorlaatpost van binnenkomst op het Belgisch grondgebied;

6° het vluchtnummer;

7° het tijdstip van vertrek en van aankomst van de vlucht;

8° het totale aantal vervoerde passagiers;

9° het eerste instappunt ».

Die lijst van inlichtingen was dus een overname van de minimale lijst waarin artikel 3, lid 2, van de API-richtlijn voorziet.

B.28.1. Wat de PNR-gegevens betreft, geeft overweging 15 van de PNR-richtlijn aan :

« Een lijst van de PNR-gegevens die door een PIE worden verkregen, dient zo te worden opgesteld dat wordt tegemoetgekomen aan de legitieme behoeften van de overheid in verband met het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, en dat aldus de interne veiligheid van de EU wordt bevorderd, en dient anderzijds de bescherming van de grondrechten, en met name het recht op eerbiediging van de persoonlijke levenssfeer en op bescherming van persoonsgegevens, te waarborgen. Daartoe moeten hoge normen worden toegepast in overeenstemming met het Handvest van de grondrechten van de Europese Unie (het ' Handvest '), het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (' Verdrag nr. 108 ') en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (' EVRM '). Dergelijke lijst mag niet uitgaan van ras of etnische oorsprong, godsdienstige of levensbeschouwelijke overtuiging, politieke of andere opvattingen, vakbondslidmaatschap, gezondheid, seksleven of seksuele geaardheid. De PNR-gegevens dienen uitsluitend details over de reserveringen en de reisroutes van de passagier te bevatten die de bevoegde instanties in staat stellen te bepalen welke vliegtuigpassagiers een risico voor de interne veiligheid vormen ».

B.28.2. Overeenkomstig artikel 3, punt 5, van de PNR-richtlijn wordt onder de « *Passenger Name Record* » of « PNR » verstaan « een bestand met de reisgegevens van iedere passagier, dat informatie bevat die de boekende en de deelnemende luchtvaartmaatschappijen nodig hebben om reserveringen te kunnen verwerken en controleren bij elke reis die door of namens iemand wordt geboekt; dit bestand kan zich bevinden in een reserveringssysteem, een vertrekcontrolesysteem dat wordt gebruikt bij het inchecken van passagiers op vluchten, of een soortgelijk systeem dat dezelfde functies vervult ».

Artikel 4, 9°, van de wet van 25 december 2016 neemt in vrijwel identieke bewoordingen die definitie van het « PNR-bestand » over.

B.28.3.1. Bijlage I van de PNR-richtlijn, met als opschrift « PNR-gegevens verzameld door luchtvaartmaatschappijen », bepaalt :

« 1. PNR-bestandslocatie

2. Datum van reservering/afgifte van het biljet

3. Geplande reisdatum (-data)

4. Naam/namen

5. Adres en contactgegevens (telefoonnummer, e-mailadres)

6. Alle betalingsinformatie, met inbegrip van het factuuradres

7. Volledige reisroute voor dit specifieke PNR

8. Informatie betreffende reizigers die gebruikmaken van een loyaliteitsprogramma voor frequent reizen

9. Reisbureau/reisagent

10. Reisstatus van de passagier, met inbegrip van bevestigingen, check-in-status en ' *no-show* ' of ' *go-show* '-informatie

11. Opgesplitste/opgedeelde PNR-informatie

12. Algemene opmerkingen (met inbegrip van alle beschikbare informatie over niet-begeleide minderjarigen jonger dan 18 jaar, zoals naam en geslacht van de minderjarige, leeftijd, talen die de minderjarige spreekt, naam en contactgegevens van de persoon die de minderjarige begeleidt naar het vertrek en de aard van de relatie van deze persoon met de minderjarige, naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van deze persoon met de minderjarige, functionaris voor vertrek en aankomst)

13. Informatie uit de biljetuitgifte (' *ticketing field* '-informatie), waaronder het biljetnummer, de uitgiftedatum van het reisbiljet, biljetten voor enkele reizen en geautomatiseerde prijsnotering van reisbiljetten

14. Zitplaatsinformatie, waaronder het zitplaatsnummer

15. Informatie over gemeenschappelijke vluchtnummers

16. Alle bagage-informatie

17. Aantal en namen van de andere reizigers in het PNR

18. Alle verzamelde API-gegevens (*Advance Passenger Information*) (onder meer soort, nummer, land van afgifte en geldigheidsdatum van een identiteitsdocument, nationaliteit, familienaam, voornaam, geslacht, geboortedatum, luchtvaartmaatschappij, vluchtnummer, datum van vertrek, datum van aankomst, luchthaven van vertrek, luchthaven van aankomst, tijdstip van vertrek, tijdstip van aankomst)

19. Alle vroegere wijzigingen in de onder de punten 1 tot en met 18 genoemde PNR-gegevens ».

B.28.3.2. Rubriek 18 van bijlage I van de PNR-richtlijn breidt dus het begrip API-gegevens, zoals bedoeld in artikel 3, lid 2, van de API-richtlijn, uit.

B.29.1.1. Wat de reservatiegegevens betreft, beoogt artikel 9, § 1, van de wet van 25 december 2016 maximaal als PNR-gegevens :

« Wat de reservatiegegevens betreft, bevatten de passagiersgegevens maximaal :

1° de PNR-bestandslocatiecode;

2° de datum van reservering en afgifte van het biljet;

3° de geplande reisdata;

4° de namen, voornamen en geboortedatum;

5° het adres en de contactgegevens (telefoonnummer, e-mailadres);

6° de betalingsinformatie, met inbegrip van het factureringsadres;

7° de volledige reisroute voor de betrokken passagier;

8° de informatie over de ' geregistreerde reizigers ', met name de reizigers die gebruikmaken van een loyauteitsprogramma voor frequent reizen;

9° het reisbureau of de reisagent;

10° de status van de reiziger, met inbegrip van de bevestigingen, *check-in*-status, *no-show*– *of go-show*-informatie;

11° de aanwijzingen over de opgesplitste of opgedeelde PNR-informatie;

12° de algemene opmerkingen, met inbegrip van alle beschikbare informatie over de niet-begeleide minderjarigen onder 18 jaar, zoals de naam en het geslacht van de minderjarige, zijn leeftijd, de taal/talen die hij spreekt, de naam en de contactgegevens van de voogd die de minderjarige begeleidt bij het vertrek en de aard van zijn relatie met de minderjarige, de naam en de contactgegevens van de voogd aanwezig bij de aankomst en de aard van zijn relatie met de minderjarige, de ambtenaar die bij het vertrek en de aankomst aanwezig is;

13° de informatie betreffende de biljetuitgifte, waaronder het biljetnummer, de uitgiftedatum, de biljetten voor enkele reizen en de geautomatiseerde prijsnotering van de biljetten;

14° het zitplaatsnummer en andere informatie over de zitplaats;

15° de informatie over gezamenlijke vluchtnummers;

16° alle bagage-informatie;

17° het aantal en de namen van de andere reizigers in het PNR;

18° alle voorafgaande passagiersgegevens (API-gegevens) die werden verzameld en worden opgesomd in § 2;

19. Alle vroegere wijzigingen in de onder de punten 1 tot en met 18 opgesomde gegevens ».

B.29.1.2. De PNR-gegevens bedoeld in artikel 9, § 1, van de wet van 25 december 2016 zijn dus een overname van de gegevens bedoeld in bijlage I van de PNR-richtlijn.

B.29.2.1. Wat de voorafgaande gegevens van de *check-in*-status en het instappen betreft, beoogt artikel 9, § 2, van de wet van 25 december 2016 als zijnde de API-gegevens :

« Wat de gegevens van de check-in-status en het instappen betreft, zijn de voorafgaande gegevens bedoeld in § 1, 18°, de volgende :

1° soort reisdocument;

2° nummer van het document;

3° nationaliteit;

4° land van afgifte van het document;

5° vervaldatum van het document;

6° familienaam, voornaam, geslacht, geboortedatum;

7° vervoerder/reisoperator;

8° nummer van het vervoer;

9° datum van vertrek, datum van aankomst;

10° plaats van vertrek, plaats van aankomst;

11° tijdstip van vertrek, tijdstip van aankomst;

12° totaal aantal vervoerde personen;

13° zitplaatsnummer;

14° PNR-bestandslocatiecode;

15° aantal, gewicht en identificatie van de bagagestukken;

16° grensdoorlaatpost van binnenkomst op het nationaal grondgebied ».

B.29.2.2. De API-gegevens bedoeld in artikel 9, § 2, van de wet van 25 december 2016 nemen hoofdzakelijk de gegevens bedoeld in punt 18 van bijlage I van de PNR-richtlijn over, en zijn dus ruimer dan de gegevens die werden beoogd door artikel 3, lid 2, van de API-richtlijn.

B.30.1. Bij zijn voormelde arrest van 21 juni 2022 in zake *Ligue des droits humains t. Ministerraad* heeft het Hof van Justitie, in antwoord op de prejudiciële vragen van het Hof over de geldigheid van de PNR–richtlijn, in verband met de gegevens van de luchtreizigers bedoeld in de PNR–richtlijn (punten 126–140), inleidend, herinnerd aan overweging 15 van de PNR–richtlijn en aan het feit dat artikel 13, lid 4, eerste zin, van de PNR–richtlijn verbiedt « dat uit de verwerking van PNR-gegevens ras of etnische afkomst, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuiging, vakbondslidmaatschap, gezondheid of seksuele geaardheid van de betrokkene blijkt », om aan te nemen dat « de in bijlage I bij de PNR–richtlijn genoemde gegevens die worden verzameld en meegedeeld, [...] dus rechtstreeks verband [moeten] houden met de betrokken vlucht en passagier en [...] zodanig [moeten] worden beperkt dat uitsluitend wordt tegemoetgekomen aan legitieme behoeften van de overheid op het gebied van het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, en dat gevoelige gegevens worden uitgesloten » (punt 128).

Het Hof van Justitie is van oordeel dat de rubrieken 1 tot 4, 7, 9, 11, 15, 17 en 19 van bijlage I van de PNR–richtlijn voldoen aan die vereisten, alsook aan die van duidelijkheid en nauwkeurigheid, aangezien het gemakkelijk te identificeren en duidelijk afgebakende informatie betreft die rechtstreeks verband houdt met de betrokken vlucht en passagier, en dat hetzelfde geldt, ondanks de open formulering ervan, voor de rubrieken 10, 13, 14 en 16 (punt 129).

B.30.2. Het Hof van Justitie acht het daarentegen nodig om de volgende verduidelijkingen te geven wat de uitlegging van de rubrieken 5, 6, 8, 12 en 18 betreft :

« 131. Rubriek 5, ' Adres en contactgegevens (telefoonnummer, e-mailadres) ', geeft niet uitdrukkelijk aan of enkel het adres en de contactgegevens van de vliegtuigpassagier worden bedoeld of ook het adres en de contactgegevens van derden die de vlucht voor hem hebben gereserveerd, derden bij wie hij kan worden bereikt of derden die moeten worden ingelicht in geval van nood. Gelet op de vereisten van duidelijkheid en nauwkeurigheid kan deze rubriek echter, zoals de advocaat-generaal in punt 162 van zijn conclusie in wezen heeft aangegeven, niet aldus worden uitgelegd dat het impliciet is toegestaan om ook persoonsgegevens van deze derden te verzamelen en door te geven. Zij moet dus in die zin worden uitgelegd dat het enkel gaat om het postadres en de contactgegevens (telefoonnummer en e–mailadres) van de passagier op naam van wie de vlucht is gereserveerd.

132. Rubriek 6, ' Alle betalingsinformatie, met inbegrip van het factuuradres ', moet ten behoeve van de vereisten van duidelijkheid en nauwkeurigheid aldus worden uitgelegd dat het enkel gaat om informatie over de betalingswijzen en de facturatie van het vliegticket, niet om andere informatie die geen rechtstreeks verband houdt met de vlucht [zie naar analogie advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 159].

133. Rubriek 8, ' Informatie betreffende reizigers die gebruikmaken van een loyaliteitsprogramma voor frequent reizen ', moet, zoals de advocaat–generaal in punt 164 van zijn conclusie heeft aangegeven, aldus worden uitgelegd dat het enkel gaat om de status die een passagier heeft in een frequent-flyerprogramma van een bepaalde (groep) luchtvaartmaatschappij(en) en om het nummer waarmee hij als ' frequent flyer ' wordt geïdentificeerd. Met rubriek 8 kan dus geen informatie worden verzameld over de transacties waardoor die status is verkregen.

134. Rubriek 12 betreft algemene opmerkingen (met inbegrip van alle beschikbare informatie over niet-begeleide minderjarigen jonger dan 18 jaar, zoals naam en geslacht van de minderjarige, leeftijd, talen die de minderjarige spreekt, naam en contactgegevens van de persoon die de minderjarige begeleidt naar het vertrek en de aard van de relatie van deze persoon met de minderjarige, naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van deze persoon met de minderjarige, functionaris voor vertrek en aankomst).

135. Hierbij zij er meteen op gewezen dat de woorden ' algemene opmerkingen ' niet voldoen aan de vereisten van duidelijkheid en nauwkeurigheid, omdat zij op zichzelf genomen geenszins de aard en omvang beperken van de informatie die krachtens rubriek 12 kan worden verzameld en meegedeeld aan een PIE [zie in die zin advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 160]. De opsomming tussen haakjes voldoet daarentegen wel aan deze vereisten.

136. Teneinde rubriek 12 overeenkomstig de in punt 86 van het onderhavige arrest aangehaalde rechtspraak de uitlegging te geven die ervoor zorgt dat zij in overeenstemming is met de vereisten van duidelijkheid en nauwkeurigheid en meer algemeen met de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, moet bijgevolg worden geoordeeld dat enkel de gegevens die in deze rubriek uitdrukkelijk worden genoemd, mogen worden verzameld en verstrekt, te weten de naam en het geslacht van de minderjarige vliegtuigpassagier, zijn leeftijd, de taal of talen die hij spreekt, de naam en contactgegevens van de persoon die hem begeleidt naar het vertrek en de aard van de relatie van deze persoon met de minderjarige, de naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van deze persoon met de minderjarige, en de functionaris voor vertrek en aankomst.

137. Tot slot is er rubriek 18, ' Alle verzamelde API–gegevens (Advance Passenger Information) (onder meer soort, nummer, land van afgifte en geldigheidsdatum van een identiteitsdocument, nationaliteit, familienaam, voornaam, geslacht, geboortedatum, luchtvaartmaatschappij, vluchtnummer, datum van vertrek, datum van aankomst, luchthaven van vertrek, luchthaven van aankomst, tijdstip van vertrek, tijdstip van aankomst) '.

138. Zoals de advocaat–generaal in de punten 156 tot en met 160 van zijn conclusie in wezen heeft aangegeven, blijkt uit rubriek 18, gelezen in samenhang met de overwegingen 4 en 9 van de PNR–richtlijn, dat de daarin bedoelde inlichtingen uitsluitend de API–gegevens zijn die in die rubriek en in artikel 3, lid 2, van de API–richtlijn worden genoemd.

139. Rubriek 18 kan dan ook, voor zover zij aldus begrepen wordt dat zij uitsluitend de daarin en de in artikel 3, lid 2, van de API–richtlijn uitdrukkelijk bedoelde inlichtingen omvat, geacht worden aan de vereisten van duidelijkheid en nauwkeurigheid te voldoen [zie naar analogie advies 1/15 (PNR–Overeenkomst EU–Canada) van 26 juli 2017, EU:C:2017:592, punt 161].

140. Bijgevolg moet worden geconstateerd dat bijlage I bij de PNR–richtlijn, indien die wordt uitgelegd in overeenstemming met hetgeen met name in de punten 130 tot en met 139 van het onderhavige arrest is overwogen, in haar geheel voldoende duidelijk en nauwkeurig is en dus de omvang afbakent van de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten ».

B.31.1. Zoals is vermeld in B.3, heeft de wet van 25 december 2016 tot doel de openbare veiligheid te verzekeren door een doorgifte van passagiersgegevens en het gebruik van die gegevens in te voeren in het kader van de strijd tegen terroristische misdrijven en zware grensoverschrijdende criminaliteit.

Die doelstellingen vormen doelstellingen van algemeen belang die inmengingen kunnen verantwoorden in het recht op eerbiediging van het privéleven en in het recht op bescherming van persoonsgegevens (HvJ, grote kamer, 8 april 2014, C—293/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238, punt 42). Het Hof van Justitie heeft overigens bevestigd dat die doelstellingen van algemeen belang de doorgifte en verwerking van persoonsgegevens van passagiers konden rechtvaardigen (HvJ, grote kamer, 26 juli 2017, advies 1/15, ECLI:EU:C:2017:592, punten 148 en 149; HvJ, grote kamer, 21 juni 2022, C—817/19, *Ligue des droits humains t. Ministerraad*, ECLI:EU:C:2022:491, punt 122).

B.31.2. Het verzamelen van de door de wet van 25 december 2016 beoogde passagiersgegevens gaat gepaard met waarborgen wat de inhoud van die gegevens betreft.

B.31.3. In de eerste plaats zijn die gegevens, zoals is vermeld in B.4.1, exhaustief vastgelegd bij artikel 9 van de wet van 25 december 2016.

Die gegevens zijn inlichtingen die rechtstreeks verband houden met de reis die aanleiding geeft tot het vervoer dat binnen het toepassingsgebied van de wet van 25 december 2016 valt. Zoals is vermeld in B.26.2.2, gaat het om gegevens waarover de vervoerders en reisoperatoren in principe reeds beschikken. Overigens stemmen die gegevens overeen met bijlage I van de richtsnoeren van de Internationale Burgerluchtvaartorganisatie (ICAO) (HvJ, grote kamer, 26 juli 2017, advies 1/15, ECLI:EU:2017:592, punt 156). Die gegevens zijn bijgevolg pertinent gezien de doelstellingen die door de wet van 25 december 2016 worden nagestreefd.

B.31.4.1. Overigens bepalen de artikelen 10 en 11 van de wet van 25 december 2016, die niet worden bestreden :

« Art. 10. De passagiersgegevens mogen geen betrekking hebben op de raciale of etnische oorsprong van een persoon, zijn religieuze of levensbeschouwelijke overtuigingen, zijn politieke opvattingen, zijn vakbondslidmaatschap, zijn gezondheidstoestand of zijn seksleven of seksuele geaardheid.

Art. 11. Wanneer de door de vervoerders en de reisoperatoren doorgegeven passagiersgegevens andere gegevens bevatten dan de in artikel 9 opgesomde gegevens of gegevens bevatten die in artikel 10 zijn opgesomd, verwijdert de PIE deze aanvullende gegevens definitief bij hun ontvangst ».

B.31.4.2. De parlementaire voorbereiding van de wet van 25 december 2016 bevestigt in dat verband :

« De passagiersgegevens mogen bovendien in geen geval betrekking hebben op de raciale of etnische afkomst, de godsdienstige of levensbeschouwelijke overtuiging, de politieke opvattingen, het lidmaatschap van een vakvereniging, de gezondheid, het seksuele leven of de seksuele geaardheid van de betrokkene. De gegevens moeten daarentegen gedetailleerde informatie over de reservering en de reisroute van de passagier bevatten, die de bevoegde instanties in staat stellen te bepalen welke passagiers een risico kunnen vormen voor de veiligheid.

[...]

De lijsten van passagiersgegevens zijn beperkt tot wat strikt noodzakelijk is om tegemoet te komen aan de legitieme behoeften van de bevoegde diensten in kader van de in de wet bepaalde doelen. Andere gegevens dan die omschreven in artikel 9 of 10 van deze wet, worden niet verzameld en onmiddellijk verwijderd » (*Parl. St.*, Kamer, 2015-2016, DOC 54–2069/001, p. 21).

B.31.5. Die bepalingen waarborgen aldus dat gevoelige gegevens niet kunnen worden verzameld of bewaard als « passagiersgegevens » bedoeld in de wet van 25 december 2016 (artikel 10). De gegevens die verder zouden gaan dan die welke exhaustief zijn opgesomd in artikel 9 of die welke gevoelige gegevens zouden bevatten, worden door de PIE verwijderd (artikel 11).

Die waarborg, wat de gevoelige gegevens betreft, sluit aldus aan op die welke het Hof van Justitie heeft onderstreept in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022 in verband met overweging 15 en artikel 13, lid 4, eerste zin, van de PNR–richtlijn (punt 128), zoals het dat reeds had onderstreept in zijn voormelde advies nr. 1/15 van 26 juli 2017 (punt 167).

De omstandigheid dat dergelijke gegevens, wanneer zij worden gecombineerd, gevoelige informatie zouden kunnen onthullen, leidt niet tot een andere conclusie, daar een dergelijke operatie een verwerking achteraf zou veronderstellen van de gegevens die zijn opgesomd in artikel 9 van de wet van 25 december 2016, die niet zou overeenstemmen met de doelstellingen en doeleinden van de wet van 25 december 2016.

B.32.1. Zoals is vermeld in B.29, stemmen de PNR-gegevens bedoeld in artikel 9, § 1, van de wet van 25 december 2016 overeen met de gegevens bedoeld in bijlage I van de PNR–richtlijn, en de API–gegevens bedoeld in artikel 9, § 2, van de wet van 25 december 2016 nemen, in hoofdzaak, de gegevens over die worden bedoeld in rubriek 18 van bijlage I van de PNR–richtlijn.

B.32.2. Thans moet worden nagegaan of die inmengingen voldoende nauwkeurig, evenredig en tot het « strikt noodzakelijke » beperkt zijn om de doelstellingen te bereiken die worden nagestreefd met de wet van 25 december 2016, rekening houdend met het voormelde arrest van het Hof van Justitie in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, waaraan wordt herinnerd in B.30.

B.33.1. Uit het voormelde arrest van het Hof van Justitie blijkt dat de PNR-gegevens « rechtstreeks verband [moeten] houden met de betrokken vlucht en passagier en [...] zodanig [moeten] worden beperkt dat uitsluitend wordt tegemoetgekomen aan legitieme behoeften van de overheid op het gebied van het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, en dat gevoelige gegevens worden uitgesloten » (punt 128). Die overwegingen kunnen worden toegepast op de andere vervoermiddelen die worden beoogd door het PNR–systeem.

Analoog met wat het Hof van Justitie heeft geoordeeld in verband met de PNR–richtlijn (punt 129), stelt het Hof vast dat de gegevens bedoeld in artikel 9, § 1, 1° tot 4°, 7°, 9°, 11°, 15°, 17° en 19°, van de wet van 25 december 2016 voldoen aan die vereisten, alsook aan die van duidelijkheid en nauwkeurigheid, aangezien het gemakkelijk te identificeren en duidelijk afgebakende informatie betreft die rechtstreeks verband houdt met de uitgevoerde vlucht en betrokken passagier, en hetzelfde geldt, ondanks de open formulering ervan, voor de gegevens bedoeld in artikel 9, § 1, 10°, 13°, 14° en 16°, van dezelfde wet.

B.33.2. Wat betreft artikel 9, § 1, 5°, van de wet van 25 december 2016, dat « het adres en de contactgegevens (telefoonnummer, e-mailadres) » beoogt, dienen die termen, analoog met wat het Hof van Justitie heeft geoordeeld in verband met rubriek 5 van de PNR-richtlijn (punt 131), zo te worden uitgelegd dat zij alleen het adres en de contactgegevens, namelijk het telefoonnummer en het e-mailadres, van de passagier op naam van wie de reservatie is gebeurd, beogen. Aldus kunnen die termen niet zo worden geïnterpreteerd dat zij, impliciet, ook het verzamelen en doorgeven van persoonsgegevens van derden toelaten.

B.33.3. Wat betreft artikel 9, § 1, 6°, van de wet van 25 december 2016, dat « de betalingsinformatie, met inbegrip van het factureringsadres » beoogt, dienen, teneinde tegemoet te komen aan de vereisten van duidelijkheid en nauwkeurigheid, die termen, analoog met wat het Hof van Justitie heeft geoordeeld in verband met rubriek 6 van de PNR-richtlijn (punt 132), zo te worden uitgelegd dat zij alleen de informatie beogen over de betalingswijzen en de facturatie van het vliegticket of van het vervoerbewijs, met uitsluiting van alle andere informatie die geen rechtstreeks verband houdt met de vlucht of het traject.

B.33.4. Wat betreft artikel 9, § 1, 8°, van de wet van 25 december 2016, dat « de informatie over de ' geregistreerde reizigers ', met name de reizigers die gebruikmaken van een loyauteitsprogramma voor frequent reizen » beoogt, dienen die termen, analoog met wat het Hof heeft geoordeeld in verband met rubriek 8 van de PNR-richtlijn (punt 133), zo te worden uitgelegd dat zij uitsluitend de gegevens beogen met betrekking tot de status die een passagier heeft in een *frequent flyer*–programma van een bepaalde (groep) luchtvaartmaatschappij(en), of in een ander getrouwheidssysteem voor frequente reizigers, alsook het nummer waarmee hij als « *frequent flyer* » of begunstigde van een ander getrouwheidssysteem wordt geïdentificeerd. Zo geïnterpreteerd laten die termen dus niet toe dat informatie wordt verzameld met betrekking tot de transacties waardoor die status is verkregen.

B.33.5. Wat betreft artikel 9, § 1, 12°, van de wet van 25 december 2016, dat « de algemene opmerkingen, met inbegrip van alle beschikbare informatie over de niet-begeleide minderjarigen onder 18 jaar, zoals de naam en het geslacht van de minderjarige, zijn leeftijd, de taal/talen die hij spreekt, de naam en de contactgegevens van de voogd die de minderjarige begeleidt bij het vertrek en de aard van zijn relatie met de minderjarige, de naam en de contactgegevens van de voogd aanwezig bij de aankomst en de aard van zijn relatie met de minderjarige, de ambtenaar die bij het vertrek en de aankomst aanwezig is » beoogt, dienen die termen, analoog met wat het Hof heeft geoordeeld in verband met rubriek 12 van de PNR-richtlijn (punten 134-136), zo te worden geïnterpreteerd dat het enkel is toegestaan die gegevens te verzamelen en mede te delen die uitdrukkelijk in die bepaling worden opgesomd, namelijk de naam en het geslacht van de minderjarige vliegtuigpassagier of reiziger, zijn leeftijd, de gesproken taal of talen, de naam en de contactgegevens van de persoon die de minderjarige begeleidt naar het vertrek en de aard van de relatie van die persoon met de minderjarige, de naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van die persoon met de minderjarige, en de ambtenaar die bij het vertrek en de aankomst aanwezig is.

Zo uitgelegd dat het op exhaustieve wijze een lijst van gegevens vaststelt, voldoet artikel 9, § 1, 12°, van de wet van 25 december 2016 aan de vereisten van duidelijkheid en nauwkeurigheid.

B.33.6.1. Artikel 9, § 1, 18°, van de wet van 25 december 2016 beoogt « alle voorafgaande passagiersgegevens (API–gegevens) die werden verzameld en worden opgesomd in § 2 », namelijk : soort reisdocument (1°), nummer van het document (2°), nationaliteit (3°), land van afgifte van het document (4°), vervaldatum van het document (5°), familienaam, voornaam, geslacht, geboortedatum (6°), vervoerder/reisoperator (7°), nummer van het vervoer (8°), datum van vertrek, datum van aankomst (9°), plaats van vertrek, plaats van aankomst (10°), tijdstip van vertrek, tijdstip van aankomst (11°), totaal aantal vervoerde personen (12°), zitplaatsnummer (13°), PNR-bestandslocatiecode (14°), aantal, gewicht en identificatie van de bagagestukken (15°) en grensdoorlaatpost van binnenkomst op het nationaal grondgebied (16°).

Wat betreft rubriek 18 van de PNR-richtlijn heeft het Hof van Justitie geoordeeld dat, op voorwaarde dat zij aldus wordt begrepen dat zij uitsluitend de daarin en de in artikel 3, lid 2, van de API–richtlijn uitdrukkelijk bedoelde inlichtingen omvat, die rubriek kan worden geacht aan de vereisten van duidelijkheid en nauwkeurigheid te voldoen (punten 137—139).

B.33.6.2. In dat verband stelt het Hof vast dat, in tegenstelling tot rubriek 18 van de PNR-richtlijn, artikel 9, § 1, 18°, van de wet van 25 december 2016 verwijst naar een lijst van gegevens die exhaustief worden opgesomd in artikel 9, § 2, van dezelfde wet, zodat die bepalingen voldoen aan de vereisten van duidelijkheid en nauwkeurigheid.

B.33.6.3. Ten aanzien van de omvang van de API-gegevens bedoeld in artikel 9, § 2, van de wet van 25 december 2016 nemen die gegevens, in hoofdzaak, zoals in B.29 is vermeld, de gegevens over die worden bedoeld in rubriek 18 van bijlage I van de PNR-richtlijn.

Aldus stemmen de in artikel 9, § 2, 1° tot 11°, van de wet van 25 december 2016 beoogde gegevens volkomen overeen met de gegevens die uitdrukkelijk worden opgesomd in de voormelde rubriek 18.

De gegevens bedoeld in artikel 9, § 2, 12°, 14° en 16°, van de wet van 25 december 2016 stemmen bovendien volkomen overeen met de gegevens die uitdrukkelijk worden opgesomd in artikel 3, lid 2, van de API–richtlijn.

B.33.6.4. Hieruit vloeit voort dat alleen de API–gegevens bedoeld in artikel 9, § 2, 13° en 15°, van de wet van 25 december 2016, namelijk het zitplaatsnummer (13°) en het aantal, het gewicht en de identificatie van de bagagestukken (15°) niet uitdrukkelijk overeenstemmen met de inlichtingen die worden beoogd in rubriek 18 van bijlage I van de PNR-richtlijn, alsook in artikel 3, lid 2, van de API–richtlijn.

Op grond van de voorgaande vaststelling kan evenwel niet ervan worden uitgegaan dat die gegevens onvoldoende duidelijk en nauwkeurig zouden zijn, noch dat zij de grens van het « strikt noodzakelijke » zouden overschrijden om de doelstellingen te bereiken die worden nagestreefd met de wet van 25 december 2016.

Immers, zoals is aangegeven in B.3.2, zijn de API-gegevens de gegevens die worden doorgegeven in het kader van de check-in en het instappen, en die minder snel beschikbaar zijn dan de PNR-gegevens. Dergelijke gegevens zijn, zoals advocaat–generaal Pitruzzella onderstreept in zijn conclusies voorgelegd op 27 januari 2022 in de zaak C-817/19, « door de luchtvaartmaatschappijen [...] verzameld in het kader van hun normale bedrijfsvoering » (ECLI:EU:C:2022:65, punt 160), en zulks geldt in voorkomend geval ook voor de andere vervoerders. Alleen indien de gegevens worden verzameld door de vervoerders in het kader van hun normale bedrijfsvoering vallen zij onder de API-gegevens bedoeld in artikel 9, § 1, 18°, van de wet van 25 december 2016, daar, zoals is vermeld in B.26.2.2, de voormelde wet geen extra verplichting tot het verzamelen van de gegevens invoert.

De PNR-gegevens die zijn vermeld in artikel 9, § 1, 14° en 16°, beogen reeds, respectievelijk, – zoals de rubrieken 14 en 16 van de PNR-richtlijn – « het zitplaatsnummer en andere informatie over de zitplaats » en « alle bagage-informatie », en dergelijke gegevens worden, zoals is vermeld in B.33.1, geacht te voldoen aan de vereisten van duidelijkheid en nauwkeurigheid en vertonen een rechtstreeks verband met de uitgevoerde vlucht of het gevolgde traject, en met de te dezen nagestreefde doelstellingen. Artikel 9, § 1, 19°, beoogt eveneens, onder de PNR-gegevens, « alle vroegere wijzigingen van de onder 1° tot 18° opgesomde gegevens », met inbegrip van de eventuele wijzigingen betreffende de zitplaats of de bagage. De gegevens betreffende de zitplaats en de bagage, bedoeld in artikel 9, § 2, 13° en 15°, zijn bijgevolg reeds opgenomen in de gegevens bedoeld in artikel 9, § 1, 14° en 16°.

Doordat artikel 9, § 2, 13° en 15°, van de wet van 25 december 2016, onder de API-gegevens, namelijk de gegevens die worden verzameld in het stadium van de check-in en het instappen, uitdrukkelijk de inlichtingen betreffende de zitplaatsen en de bagage beoogt, creëert het derhalve geen extra gegevens ten opzichte van de lijst van de gegevens die moeten worden verzameld krachtens artikel 9, § 1, 14° en 16°, en beantwoordt het aldus aan de vereisten van duidelijkheid, nauwkeurigheid en evenredigheid.

B.34. Onder voorbehoud van de interpretaties vermeld in B.33.2 tot B.33.5, is het middel, in zoverre het is gericht tegen de artikelen 4, 9°, en 9, van de wet van 25 december 2016, niet gegrond.

2. *Het begrip « passagier » (artikel* 4, 10°*)*

B.35. De verzoekende partij bekritiseert het ruime karakter van het begrip « passagier », dat leidt tot een systematische, niet-doelgerichte, geautomatiseerde verwerking van de gegevens van alle passagiers.

B.36.1. Artikel 4, 10°, van de bestreden wet definieert de « passagier » als « iedere persoon, met inbegrip van de transferpassagiers en transitpassagiers en met uitsluiting van de bemanningsleden, die wordt vervoerd of moet worden vervoerd door een vervoerder, met de toestemming van deze laatste, wat zich vertaalt door de inschrijving van deze persoon op de passagierslijst ».

Dat artikel neemt de inhoud over van artikel 3, punt 4, van de PNR-richtlijn, dat de « passagier » ook definieert als « iedere persoon, met inbegrip van de transferpassagiers en transitpassagiers en met uitsluiting van de bemanningsleden, die met toestemming van de luchtvaartmaatschappij in een luchtvaartuig wordt vervoerd of zal worden vervoerd, en waarbij die toestemming blijkt uit de vermelding van die persoon op de passagierslijst ».

B.36.2. De definitie van « passagier » heeft tot gevolg dat het verzamelen, het doorgeven en het verwerken van de PNR-gegevens van die « passagiers » algemene en ongedifferentieerde verplichtingen vormen, die van toepassing zijn op elke persoon die wordt vervoerd of moet worden vervoerd en die op de passagierslijst is ingeschreven.

De verplichtingen die de wet van 25 december 2016 oplegt, zijn aldus van toepassing los van het bestaan van ernstige redenen om te geloven dat de betrokken personen een misdrijf hebben gepleegd of op het punt staan een misdrijf te plegen, of aan een misdrijf schuldig zijn bevonden.

De wet van 25 december 2016 voert het algemeen en ongedifferentieerd verzamelen, doorgeven en gebruiken in van de PNR-gegevens voor alle passagiers die reizen met een luchtvaartuig, los van het overschrijden van de buitengrenzen van de Unie, en die gegevensverzameling is uitgebreid tot het vervoer per trein of per bus bij de koninklijke besluiten van 3 februari 2019, aangehaald in B.8.

B.36.3. In haar advies van 19 augustus 2016 « over de implicaties inzake gegevensbescherming van de verwerking van passagiersgegevens » heeft de Adviescommissie inzake het Verdrag van de Raad van Europa nr. 108 « tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens » dienaangaande opgemerkt :

« De verwerking van de PNR-gegevens — die het unieke voordeel heeft de identificatie van personen die van belang zijn mogelijk te maken — is een algemene en niet-selectieve filtering van alle passagiers, met inbegrip van diegenen die niet ervan worden verdacht enig strafrechtelijk misdrijf te hebben gepleegd, door verschillende bevoegde instanties, en zij betreft gegevens die aanvankelijk voor commerciële doeleinden door private entiteiten verzameld zijn. Gelet op de omvang van de aantasting van de rechten op privéleven en op gegevensbescherming die uit de verwerking van de PNR-gegevens zou voortvloeien, dient duidelijk te worden aangetoond dat de genoemde verwerking een noodzakelijke maatregel met een wettig doel in een democratische samenleving is; bovendien is vereist dat passende waarborgen worden ingevoerd. Het is onontbeerlijk de noodzaak van het verzamelen en het later gebruiken van de PNR-gegevens uitdrukkelijk aan te tonen » (advies van 19 augustus 2016, T—PD(2016)18rev, p. 5).

De Commissie heeft ook de noodzaak onderstreept van een periodieke evaluatie van een dergelijk PNR-systeem, teneinde te bepalen of het nog steeds verantwoord is :

« In het geval van de bestaande systemen voor de verwerking van de PNR-gegevens door de bevoegde instanties dient een grotere transparantie met betrekking tot de evaluatie van de doeltreffendheid van die systemen te worden nagestreefd teneinde een gegronde en onafhankelijke evaluatie van de noodzaak van het systeem mogelijk te maken. Hoewel die transparantie gedetailleerd moet zijn, mag zij evenwel niet ingaan tegen de wettige doelstelling. Bijvoorbeeld, objectieve en kwantificeerbare informatie met betrekking tot de bereikte resultaten, zoals het aantal aangehouden personen, de terroristische bedreigingen die zouden kunnen zijn vermeden, de andere ontradende effecten, de wijziging van de gedragingen van de delinquenten (bijvoorbeeld, het afzien van overwogen criminele handelingen), de waarschijnlijkheid van een aanzienlijke verhoging van de kosten en van de moeilijkheid om misdrijven (zoals terroristische aanslagen) te plegen, zouden het mogelijk maken de evaluatie van de noodzaak van een systeem voor de verwerking van de PNR-gegevens te belichten.

Er dient met geregelde tussenpozen te worden overgegaan tot een onderzoek van de noodzaak van het systeem van de PNR teneinde te bepalen of het nog steeds verantwoord is » (*ibid.*, p. 6).

B.36.4.1. Artikel 19 van de PNR-richtlijn, met als opschrift « Evaluatie », bepaalt dat de Commissie, op basis van de door de lidstaten verstrekte informatie, waaronder statistische gegevens, uiterlijk op 25 mei 2020 alle elementen van de richtlijn evalueert en bij het Europees Parlement en bij de Raad een verslag indient en dat toelicht.

Artikel 19, lid 3, van de PNR-richtlijn bepaalt dat « de Commissie [...] rekening [houdt] met de ervaring die in de lidstaten is opgedaan, en met name in de lidstaten die deze richtlijn toepassen op vluchten binnen de EU overeenkomstig artikel 2 » en dat « ook aandacht [wordt] besteed aan de noodzaak om marktdeelnemers die geen luchtvaartmaatschappij zijn, zoals reisbureaus en touroperators die diensten in verband met reizen aanbieden, met inbegrip van het boeken van vluchten, in het toepassingsgebied van deze richtlijn op te nemen ».

Overeenkomstig die bepaling heeft de Commissie aan het Europees Parlement en de Raad op 24 juli 2020 haar verslag bezorgd « over de evaluatie van Richtlijn (EU) 2016/681 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit » (COM(2020) 305 final).

Dat verslag besluit :

« In algemene zin oordeelt de Commissie positief over de eerste twee toepassingsjaren van de richtlijn. De belangrijkste conclusies van de evaluatie is dat de richtlijn een positieve bijdrage levert aan haar voornaamste doelstelling, namelijk het invoeren van doeltreffende PNR-systemen in de lidstaten als instrument voor de bestrijding van terrorisme en ernstige criminaliteit » (p. 13).

Wat betreft het toepassingsgebied van de verzameling van de PNR-gegevens heeft de Commissie onderstreept :

« Op één na alle lidstaten hebben de verzameling van PNR-gegevens uitgebreid naar vluchten binnen de EU. Nationale instanties beschouwen de verzameling van PNR-gegevens over vluchten binnen de EU (en in het bijzonder binnen de Schengenlanden) als een belangrijk rechtshandhavingsmiddel om de bewegingen van bekende verdachten te volgen en verdachte reispatronen te ontdekken van onbekende personen die binnen het Schengengebied reizen en mogelijk betrokken zijn bij criminele of terroristische activiteiten. Aangezien lidstaten al op doeltreffende wijze PNR-gegevens over vluchten binnen de EU verzamelen, acht de Commissie het op dit moment niet noodzakelijk de verzameling van PNR-gegevens voor dit soort vluchten te verplichten » (p. 11).

B.36.4.2. Artikel 52, § 1, van de wet van 25 december 2016 bepaalt dat « deze wet [...] aan een evaluatie [wordt] onderworpen drie jaar na de inwerkingtreding ervan ».

B.37. Op een vraag van het Hof over een systeem voor het algemeen en ongedifferentieerd verzamelen, doorgeven en gebruiken van de PNR-gegevens voor alle « passagiers », los van een overschrijding van de buitengrenzen van de Unie, heeft het Hof van Justitie, in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geantwoord :

« 158. Het bij de PNR-richtlijn ingevoerde systeem bestrijkt de PNR-gegevens van eenieder die ‘ passagier ’ is in de zin van artikel 3, punt 4, van deze richtlijn en die een vlucht neemt die binnen de werkingssfeer van deze richtlijn valt.

159. Volgens artikel 8, lid 1, van de PNR-richtlijn moeten deze gegevens worden doorgegeven aan de PIE van de lidstaat waar de vlucht moet aankomen of vertrekken, ongeacht of er een objectieve reden is om aan te nemen dat de passagier mogelijk betrokken is bij terroristische misdrijven of ernstige criminaliteit. Na deze doorgifte worden de gegevens echter onder meer automatisch verwerkt tijdens de voorafgaande beoordeling die wordt verricht op grond van artikel 6, lid 2, onder *a)*, en lid 3, van deze richtlijn. Zoals uit overweging 7 blijkt, heeft deze beoordeling tot doel personen te identificeren die vooralsnog niet van terroristische misdrijven of ernstige criminaliteit werden verdacht maar naar wie de bevoegde instanties nader onderzoek moeten verrichten.

160. Blijkens artikel 1, lid 1, onder *a)*, en artikel 2 van de PNR-richtlijn wordt in het bijzonder een onderscheid gemaakt tussen passagiers van vluchten naar of vanuit derde landen en passagiers van vluchten binnen de EU.

161. Wat passagiers van vluchten naar of vanuit derde landen betreft, zij eraan herinnerd dat het Hof in verband met passagiers van vluchten tussen de Unie en Canada reeds heeft geoordeeld dat de geautomatiseerde verwerking van hun PNR-gegevens vóór hun aankomst in Canada ervoor zorgt dat de veiligheidscontroles, met name aan de grens, veel soepeler en sneller verlopen. Bovendien zou de uitsluiting van bepaalde categorieën personen of bepaalde gebieden van herkomst in de weg staan aan de verwezenlijking van de doelstelling van de geautomatiseerde verwerking van de PNR-gegevens – te weten door middel van een verificatie van deze gegevens die luchtreizigers identificeren die een risico zouden kunnen opleveren voor de openbare veiligheid – en het mogelijk maken om aan deze verificatie te ontsnappen [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 187].

162. Deze overwegingen gelden mutatis mutandis voor passagiers van vluchten tussen de Unie en om het even welk derde land, waarvoor de lidstaten volgens artikel 1, lid 1, onder *a)*, *juncto* artikel 3, punten 2 en 4, van de PNR-richtlijn verplicht zijn het systeem van deze richtlijn toe te passen. Het doorgeven en vooraf beoordelen van PNR-gegevens van luchtreizigers die de Unie binnenkomen en verlaten kan immers niet enkel voor een welbepaalde kring van luchtreizigers gebeuren, gelet op de aard zelf van de dreiging voor de openbare veiligheid die kan worden veroorzaakt door terroristische misdrijven en ernstige vormen van criminaliteit die, op zijn minst indirect, een objectief verband vertonen met het luchtvervoer van passagiers tussen de Unie en derde landen. Aldus moet worden geoordeeld dat er een noodzakelijk verband bestaat tussen deze gegevens en de doelstelling dergelijke strafbare feiten te bestrijden, en dat de PNR-richtlijn dus niet verder dan het strikt noodzakelijke gaat enkel omdat zij de lidstaten verplicht de PNR-gegevens van al die passagiers systematisch op voorhand door te geven en te beoordelen.

163. Wat passagiers van vluchten tussen lidstaten van de Unie betreft, biedt artikel 2, lid 1, *juncto* overweging 10 van de PNR-richtlijn de lidstaten louter de mogelijkheid om het systeem van de PNR-richtlijn uit te breiden naar vluchten binnen de EU.

164. De Uniewetgever heeft de lidstaten dus niet willen verplichten dit systeem ook op vluchten binnen de EU toe te passen, maar heeft, zoals uit artikel 19, lid 3, van deze richtlijn blijkt, het recht voorbehouden om over een dergelijke uitbreiding te beslissen na een grondige evaluatie van de juridische gevolgen daarvan met name voor de grondrechten van de betrokkenen.

165. In dit verband zij opgemerkt dat artikel 19, lid 3, van de PNR-richtlijn bepaalt dat het in lid 1 van dit artikel bedoelde evaluatieverslag van de Commissie ' ook een evaluatie [bevat] van de noodzakelijkheid, evenredigheid en doeltreffendheid van het in het toepassingsgebied van deze richtlijn opnemen van het verplicht verzamelen en doorgeven van PNR-gegevens inzake alle of een aantal uitgekozen vluchten binnen de EU ' en dat zij daarbij rekening moet houden met ' de ervaring die in de lidstaten is opgedaan, en met name in de lidstaten die deze richtlijn toepassen op vluchten binnen de EU overeenkomstig artikel 2 '. De Uniewetgever acht het dus duidelijk niet noodzakelijk het systeem van de PNR-richtlijn uit te breiden naar alle vluchten binnen de EU.

166. In diezelfde lijn bepaalt artikel 2, lid 3, van de PNR-richtlijn dat de lidstaten kunnen besluiten de bepalingen van deze richtlijn uitsluitend op geselecteerde vluchten binnen de EU toe te passen indien zij dat ter bereiking van de doelstellingen van deze richtlijn noodzakelijk achten, in welk geval zij te allen tijde kunnen besluiten de geselecteerde vluchten te wijzigen.

167. Hoe dan ook moet de keuzemogelijkheid van de lidstaten om het systeem van de PNR-richtlijn uit te breiden naar vluchten binnen de EU worden uitgeoefend met volledige eerbiediging van de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zoals uit overweging 22 van deze richtlijn blijkt. Het staat volgens overweging 19 weliswaar aan de lidstaten zelf om dreigingen op het gebied van terroristische misdrijven en ernstige criminaliteit te beoordelen, maar dit neemt niet weg dat zij, om de voormelde keuze te kunnen maken, bij die beoordeling het bestaan van een dergelijke dreiging moeten vaststellen die kan rechtvaardigen dat deze richtlijn ook op vluchten binnen de EU wordt toegepast.

168. Derhalve moet een lidstaat die gebruik wenst te maken van de in artikel 2 van de PNR-richtlijn geboden mogelijkheid – of dit nu is voor alle vluchten binnen de EU (artikel 2, lid 2) dan wel enkel voor bepaalde vluchten binnen de EU (artikel 2, lid 3) – steeds nagaan of die uitbreiding naar alle of een deel van de vluchten binnen de EU werkelijk noodzakelijk is voor en evenredig is aan de doelstelling van artikel 1, lid 2, ervan.

169. Zo moet een dergelijke lidstaat, gelet op de overwegingen 5 tot en met 7, 10 en 22 van de PNR-richtlijn, nagaan of de in deze richtlijn bedoelde verwerking van PNR-gegevens van passagiers die (bepaalde) vluchten binnen de EU nemen, gezien de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, wel strikt noodzakelijk is om de interne veiligheid van de Unie of minstens die lidstaat te verzekeren en het leven en de veiligheid van personen te beschermen.

170. Wat terroristische dreigingen in het bijzonder betreft, blijkt uit de rechtspraak van het Hof dat terroristische activiteiten behoren tot de activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, en dat elke lidstaat er groot belang bij heeft deze activiteiten te voorkomen en te bestrijden teneinde de essentiële staatsfuncties en de fundamentele belangen van de samenleving te beschermen en dus de nationale veiligheid te waarborgen. Dergelijke bedreigingen verschillen door hun aard, hun bijzondere ernst en het bijzondere karakter van de omstandigheden waarin zij zich voordoen, van het algemene, permanente risico op ernstige strafbare feiten (zie in die zin arresten van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 135 en 136, en 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punten 61 en 62).

171. In de situatie waarin een lidstaat bij de door hem gemaakte beoordeling voldoende concrete redenen vaststelt om aan te nemen dat hij te maken heeft met een terroristische dreiging die reëel en actueel of voorzienbaar is, lijkt het feit dat deze lidstaat de PNR-richtlijn krachtens artikel 2, lid 1, ervan voor een beperkte duur wil toepassen op alle vluchten binnen de EU van of naar deze lidstaat, dus niet verder te gaan dan strikt noodzakelijk is. Het bestaan van een dergelijke bedreiging toont immers op zichzelf een verband aan tussen de doorgifte en verwerking van de betrokken gegevens enerzijds en de bestrijding van terrorisme anderzijds (zie naar analogie arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 137).

172. De beslissing om tot die toepassing over te gaan, moet effectief kunnen worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of de voormelde situatie zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien. De duur van de toepassing moet ook worden beperkt tot het strikt noodzakelijke, maar kan worden verlengd indien de dreiging voortduurt (zie naar analogie arresten van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 168, en 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 58).

173. Wordt de betrokken lidstaat niet met een werkelijke en actuele of voorzienbare terroristische dreiging geconfronteerd, dan kan daarentegen niet worden geoordeeld dat het ongedifferentieerd toepassen van het systeem van de PNR-richtlijn – én op vluchten naar of vanuit derde landen én op vluchten binnen de EU – beperkt is tot het strikt noodzakelijke.

174. In een dergelijke situatie moet het bij de PNR-richtlijn ingevoerde systeem worden beperkt tot bepaalde vluchten binnen de EU en meer bepaald tot de doorgifte en verwerking van PNR-gegevens voor vluchten die met name verband houden met bepaalde verbindingen, reisroutes of luchthavens waarvoor er aanwijzingen bestaan dat deze toepassing gerechtvaardigd is. De betrokken lidstaat dient dan de vluchten binnen de EU te selecteren op basis van de resultaten van de beoordeling die hij in overeenstemming met de in de punten 163 tot en met 169 van het onderhavige arrest uiteengezette vereisten moet verrichten, en die regelmatig te herzien in het licht van wijzigingen in de omstandigheden die de selectie rechtvaardigden, om te verzekeren dat het bij deze richtlijn ingevoerde systeem steeds in de mate van het strikte noodzakelijke wordt toegepast op vluchten binnen de EU.

175. Uit het voorgaande volgt dat de uitlegging die aldus in het licht van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest is gegeven aan artikel 2 en artikel 3, punt 4, van de PNR-richtlijn, kan verzekeren dat deze bepalingen de grenzen van het strikt noodzakelijke respecteren ».

B.38.1. Wat betreft het begrip « passagier » bedoeld in de PNR-richtlijn heeft het Hof van Justitie geoordeeld dat, wanneer de gegevens van de « passagiers » worden doorgegeven aan de PIE van de lidstaat, ongeacht of er een objectieve reden is om aan te nemen dat de passagier mogelijk betrokken is bij terroristische misdrijven of ernstige criminaliteit, die gegevens worden onderworpen aan een geautomatiseerde verwerking die, zoals blijkt uit overweging 7 van die richtlijn, tot doel heeft personen te identificeren die niet ervan verdacht werden deel te nemen aan terroristische misdrijven of aan ernstige vormen van criminaliteit vóór die beoordeling en die zouden moeten worden onderworpen aan een grondiger onderzoek door de bevoegde autoriteiten (punt 161).

Gelet op de aard zelf van de dreiging voor de openbare veiligheid die kan worden veroorzaakt door terroristische misdrijven en ernstige vormen van criminaliteit die, op zijn minst indirect, een objectief verband vertonen met het luchtvervoer van passagiers, is het Hof van Justitie van oordeel dat « het doorgeven en vooraf beoordelen van PNR-gegevens van luchtreizigers die de Unie binnenkomen en verlaten [...] niet enkel voor een welbepaalde kring van luchtreizigers [kan] gebeuren » : er « moet worden geoordeeld dat er een noodzakelijk verband bestaat tussen deze gegevens en de doelstelling dergelijke strafbare feiten te bestrijden, en dat de PNR-richtlijn dus niet verder dan het strikt noodzakelijke gaat enkel omdat zij de lidstaten verplicht de PNR-gegevens van al die passagiers systematisch op voorhand door te geven en te beoordelen » (punt 162).

B.38.2. Zoals het Hof van Justitie in het voormelde arrest onderstreept, is de verzameling van de gegevens van alle passagiers bedoeld in artikel 4, 10°, van de wet van 25 december 2016 onderworpen aan een geautomatiseerde verwerking achteraf die ertoe strekt, onder die passagiers, diegenen te identificeren die zouden moeten worden onderworpen aan een grondiger onderzoek door de bevoegde autoriteiten, in het kader van de beoogde bestrijding van terroristische misdrijven en ernstige vormen van criminaliteit.

Een dergelijk systeem onderscheidt zich aldus van een systeem van algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronische-communicatiemiddelen, alsook van de verplichting voor de aanbieders van elektronische-communicatiediensten om die gegevens stelselmatig en voortdurend te bewaren zonder enige uitzondering (vergelijk met HvJ, grote kamer, 21 december 2016, C-203/15 en C-698/15, *Tele*2 *Sverige AB t. Post-och telestyrelsen e.a.*, ECLI:EU:C:2016:970, punten 103-112).

B.39.1. Wat betreft de betrokken vluchten heeft het Hof van Justitie geoordeeld dat de lidstaten die beslissen de toepassing van het door die richtlijn vastgestelde systeem uit te breiden tot de vluchten binnen de Europese Unie, niet meer dan een mogelijkheid aanwenden waarin wordt voorzien in artikel 2, lid 1, van de PNR-richtlijn.

Het verslag van de Commissie « over de evaluatie van Richtlijn (EU) 2016/681 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit », aangehaald in B.36.4.1, bepaalt overigens dat alle lidstaten, op één na, het systeem van de verzameling van de PNR-gegevens hebben uitgebreid tot de vluchten binnen de EU.

B.39.2. Uit het arrest van het Hof van Justitie, aangehaald in B.37, blijkt overigens dat de eventuele uitbreiding van het systeem van de verzameling van de PNR-gegevens tot alle vluchten binnen de EU waartoe een lidstaat kan beslissen door gebruik te maken van de mogelijkheid waarin die richtlijn voorziet, onderworpen is aan de voorwaarde dat, op basis van de door de lidstaat uitgevoerde beoordeling, wordt vastgesteld dat voldoende concrete redenen bestaan om aan te nemen dat de betrokken lidstaat te maken heeft met een terroristische dreiging die reëel en actueel of voorzienbaar is, waarbij het bestaan van een dergelijke dreiging op zich een verband kan aantonen tussen, enerzijds, de doorgifte en de verwerking van de betrokken gegevens en, anderzijds, de bestrijding van terrorisme (punt 171).

De beslissing om tot die toepassing over te gaan, moet overigens effectief kunnen worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, en de duur van de toepassing moet ook tijdelijk worden beperkt tot het strikt noodzakelijke, maar kan worden verlengd indien de dreiging voortduurt (punt 172).

Ten slotte, wanneer het bestaan van die dreiging niet is aangetoond, dan dient het systeem van de verzameling van de PNR-gegevens te worden beperkt tot de vluchten die met name verband houden met bepaalde verbindingen, reisroutes of luchthavens waarvoor er, volgens de beoordeling van de betrokken lidstaat, aanwijzingen bestaan die die toepassing kunnen rechtvaardigen, en dient het strikt noodzakelijke karakter van die toepassing op de vluchten binnen de EU die aldus zijn geselecteerd, regelmatig te worden herzien in het licht van wijzigingen in de omstandigheden die de selectie hebben gerechtvaardigd (punt 174).

B.40.1. Zoals wordt aangegeven in de parlementaire voorbereiding ervan, strekt de wet van 25 december 2016, met de omzetting van de PNR-richtlijn, ertoe de terroristische dreiging te bestrijden :

« De aanslagen van 22 maart 2016 in de vertrekhal van de nationale luchthaven en in het metrostation Maalbeek, de aanslagen van 13 november 2015 in Parijs en de andere dramatische gebeurtenissen in Brussel (Joods Museum, mei 2014), in Parijs (Charlie Hebdo, januari 2015), in Kopenhagen (februari 2015), de dreiging die in eigen land heerst en rechtstreeks verband houdt met de problematiek van de ' *foreign fighters* ' en de ' *returnees* ' herinneren er ons meer dan ooit aan dat het van essentieel belang is voor de overheden die de bescherming en de veiligheid van de burgers willen verzekeren, niet enkel een reactieve houding aan te nemen, maar ook te anticiperen op de risico's die gekoppeld zijn aan de verplaatsingen van criminelen.

Deze anticipatie is met name mogelijk dankzij de analyse van de bestanden met reisgegevens in het kader van het voorkomen en het opsporen van terroristische misdrijven, van vormen van ernstige criminaliteit, van inbreuken op de openbare orde in het kader van gewelddadige radicalisering en van activiteiten die de fundamentele belangen van de Staat kunnen bedreigen » (*Parl. St.*, Kamer, 2015-2016, DOC 54-2069/001, p. 5).

B.40.2.1. Aangezien in België de twee terroristische aanslagen hebben plaatsgehad waarnaar in de voormelde parlementaire voorbereiding wordt verwezen (Joods Museum in mei 2014 en metrostation Maalbeek en luchthaven van Zaventem in maart 2016), vermocht de wetgever ervan uit te gaan, wanneer hij de wet van 25 december 2016 heeft aangenomen, dat de terroristische dreiging reëel en actueel was.

Bovendien blijkt dat die terroristische dreiging nog steeds reëel en actueel is. Aldus maakte het Coördinatieorgaan voor de Dreigingsanalyse (OCAD), opgericht bij artikel 5 van de wet van 10 juli 2006 « betreffende de analyse van de dreiging » (hierna : de wet van 10 juli 2006), in 2022 gewag van 215 seiningen in verband met terrorisme en extremisme, en het algemene dreigingsniveau in België is thans 2 op 4, namelijk een gemiddelde dreiging.

B.40.2.2. Daarnaast dient, om de realiteit van die dreiging te beoordelen, rekening te worden gehouden met de geografische situering van het land, met een beperkt grondgebied en met gemakkelijk te overschrijden grenzen, in het centrum van Europa, en waar talrijke Europese en internationale instellingen zijn gevestigd. Die kenmerkende geografische realiteit van het land verhoogt aanzienlijk het risico dat wordt gebruikgemaakt van alle vervoersmiddelen via België voor het plegen van terroristische misdrijven of ernstige vormen van criminaliteit. Het land is aldus geografisch gesitueerd op de kruising van talrijke vervoersassen, in de lucht, via het spoor of op de weg, die kunnen worden gebruikt door terroristische en criminele organisaties voor het plegen van terroristische misdrijven of ernstige vormen van criminaliteit.

B.40.2.3. Uit hetgeen voorafgaat, vloeit voort dat de beoordeling van de dreiging die de uitbreiding van het PNR–systeem tot alle vluchten binnen de EU rechtvaardigt, het voorwerp heeft uitgemaakt van een toetsing, te dezen een jurisdictionele, door het Hof en dat de realiteit en actualiteit ervan werden vastgesteld.

B.40.3.1. Zoals het Hof van Justitie onderstreept, moet de duur van de toepassing van de maatregelen die zijn gerechtvaardigd door de beoordeling van de dreiging, worden beperkt tot het « strikt noodzakelijke ».

In dat verband zij eraan herinnerd dat het OCAD onder meer de opdracht heeft « op periodieke basis een gemeenschappelijke strategische evaluatie uit te voeren die moet toelaten te oordelen of dreigingen, bedoeld in artikel 3, zich kunnen voordoen of, indien ze al vastgesteld werden, hoe deze evolueren en welke maatregelen in voorkomend geval noodzakelijk zijn » (artikel 8, 1°, van de voormelde wet van 10 juli 2006), waarbij de in artikel 3 beoogde dreigingen zijn « opgesomd in artikel 8, 1°, *b)* en *c)*, van de wet inzake de inlichtingen– en veiligheidsdienst, die de inwendige en uitwendige veiligheid van de Staat, de Belgische belangen en de veiligheid van de Belgische onderdanen in het buitenland of elk ander fundamenteel belang van het land zoals bepaald door de Koning op voorstel van de Nationale Veiligheidsraad, zouden kunnen aantasten ». Uit hetgeen voorafgaat, vloeit voort dat een periodieke beoordeling van de dreiging is georganiseerd en toevertrouwd aan het OCAD.

B.40.3.2. Voor het overige voorziet artikel 52, § 1, van de wet van 25 december 2016 in een evaluatie van de wet drie jaar na de inwerkintreding ervan.

Gelet op hetgeen is vermeld in B.40.2.3 betreffende de realiteit en de actualiteit van de dreiging, staat het aan de wetgever, op basis van de evaluatie van de dreiging door het OCAD, een periodieke evaluatie van de wet van 25 december 2016 uit te voeren, waarbij een eerste evaluatie moet plaatshebben uiterlijk drie jaar na de datum van de uitspraak van het onderhavige arrest.

B.40.3.3. In de veronderstelling dat de realiteit en actualiteit of de voorzienbaarheid van de dreiging niet langer aangetoond zijn, staat het aan de wetgever de mogelijkheid te onderzoeken, in het licht van de nagestreefde doelstellingen, om het systeem van de verzameling van de PNR-gegevens te beperken, op de wijze zoals aangegeven door het Hof van Justitie in punt 174 van zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022.

B.41. Gelet op hetgeen is vermeld in B.40.3.2 en B.40.3.3, is het middel, in zoverre het is gericht tegen artikel 4, 10°, van de wet van 25 december 2016, niet gegrond.

3. *De doeleinden van de PNR-gegevensverwerking (artikel 8)*

B.42. De verzoekende partij bekritiseert de in artikel 8 van de wet van 25 december 2016 vervatte definitie van de doeleinden van de PNR-gegevensverwerking, die veel ruimer zou zijn dan de enkel tot terroristische misdrijven en ernstige criminaliteit beperkte « specifieke doeleinden » van de PNR-richtlijn. Zij is van mening dat die eerste doeleinden de grenzen van het « strikt noodzakelijke » overschrijden.

B.43.1. Artikel 1, lid 2, van de PNR-richtlijn bepaalt :

« Overeenkomstig deze richtlijn verzamelde PNR-gegevens mogen uitsluitend worden verwerkt om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen overeenkomstig artikel 6, lid 2, onder *a)*, *b)* en *c)* ».

Artikel 6, lid 2, van de PNR-richtlijn bepaalt :

« De PIE verwerkt de PNR-gegevens uitsluitend voor de volgende doeleinden :

a) het beoordelen van de passagiers vóór hun geplande aankomst in of gepland vertrek uit de lidstaat, om te bepalen welke personen moeten worden onderworpen aan een nader onderzoek door de in artikel 7 bedoelde bevoegde instanties, en, in voorkomend geval, door Europol overeenkomstig artikel 10, omdat zij betrokken zouden kunnen zijn bij een terroristisch misdrijf of bij ernstige criminaliteit;

b) het per geval inwilligen van een op afdoende gronden gebaseerd, gemotiveerd verzoek van de bevoegde instanties om in bepaalde gevallen PNR-gegevens te verstrekken en te verwerken voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven of ernstige criminaliteit, en de resultaten van deze verwerking aan die instanties of, in voorkomend geval, aan Europol mee te delen; en

c) het analyseren van PNR-gegevens voor het bijstellen van bestaande of het formuleren van nieuwe criteria die moeten worden gebruikt bij de beoordelingen die worden verricht op grond van lid 3, onder *b)*, om te bepalen welke personen betrokken zouden kunnen zijn bij een terroristisch misdrijf of bij ernstige criminaliteit ».

In overweging nr. 7 van de PNR-richtlijn wordt ook gepreciseerd :

« Door PNR-gegevens te gebruiken kan het gevaar van terroristische misdrijven en ernstige criminaliteit vanuit een andere invalshoek worden aangepakt dan bij de verwerking van andere categorieën persoonsgegevens het geval is. Om echter ervoor te zorgen dat de verwerking van PNR-gegevens beperkt blijft tot het noodzakelijke, dient de vaststelling en toepassing van beoordelingscriteria te worden beperkt tot terroristische misdrijven en ernstige criminaliteit waarvoor het gebruik van dergelijke criteria relevant is ».

B.43.2. De doeleinden van de verwerking van de PNR-gegevens zoals bepaald in de PNR-richtlijn vormen dus enkel doelstellingen inzake het voorkomen, opsporen, onderzoeken en vervolgen van de terroristische misdrijven en ernstige criminaliteit.

B.43.3. In artikel 3, punt 8, van de PNR-richtlijn worden « terroristische misdrijven » gedefinieerd als « de in de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ bedoelde, volgens nationaal recht strafbare feiten ».

In artikel 3, punt 9, van de PNR-richtlijn wordt « ernstige criminaliteit » gedefinieerd als « de in bijlage II bedoelde strafbare feiten, waarop in het nationale recht van een lidstaat een vrijheidsbenemende straf of een tot detentie strekkende maatregel met een maximumduur van ten minste drie jaar staat ».

Bijlage II, met als opschrift « Lijst van de in artikel 3, punt 9, bedoelde strafbare feiten », van de PNR-richtlijn bepaalt :

« 1. deelneming aan een criminele organisatie,

2. mensenhandel,

3. seksuele uitbuiting van kinderen en kinderpornografie,

4. illegale handel in verdovende middelen en psychotrope stoffen,

5. illegale handel in wapens, munitie en explosieven,

6. corruptie,

7. fraude, met inbegrip van fraude ten nadele van de financiële belangen van de Unie,

8. witwassen van opbrengsten van criminaliteit en valsemunterij, met inbegrip van namaak van de euro,

9. computercriminaliteit/cybercriminaliteit,

10. milieumisdrijven, met inbegrip van de illegale handel in bedreigde diersoorten en de illegale handel in bedreigde planten- en boomsoorten,

11. hulp bij illegale binnenkomst en illegaal verblijf,

12. moord, zware mishandeling,

13. illegale handel in menselijke organen en weefsels,

14. ontvoering, wederrechtelijke vrijheidsberoving en gijzeling,

15. georganiseerde en gewapende diefstal,

16. illegale handel in cultuurgoederen, waaronder antiquiteiten en kunstvoorwerpen,

17. namaak van producten en productpiraterij,

18. vervalsing van administratieve documenten en handel in valse documenten,

19. illegale handel in hormonale stoffen en andere groeibevorderaars,

20. illegale handel in nucleaire of radioactieve stoffen,

21. verkrachting,

22. misdrijven die onder de rechtsmacht van het Internationaal Strafhof vallen,

23. kaping van vliegtuigen/schepen,

24. sabotage,

25. handel in gestolen voertuigen,

26. industriële spionage ».

B.44.1. In zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022 heeft het Hof van Justitie, in verband met de doeleinden van de PNR-gegevensverwerking, gepreciseerd :

« 2*) Doeleinden van « PNR-gegevensverwerking »*

141. Blijkens artikel 1, lid 2, van de PNR-richtlijn heeft het verwerken van de overeenkomstig deze richtlijn verzamelde PNR-gegevens tot doel ‘ terroristische misdrijven ’ en ‘ ernstige criminaliteit ’ te bestrijden.

142. Wat betreft de vraag of de PNR-richtlijn ter zake duidelijke en nauwkeurige regels bevat die de toepassing van het systeem van deze richtlijn beperken tot het strikt noodzakelijke, moet ten eerste worden opgemerkt dat ‘ terroristische misdrijven ’ in artikel 3, punt 8, van deze richtlijn worden gedefinieerd als ‘ de in de artikelen 1 tot en met 4 van [kaderbesluit 2002/475] bedoelde, volgens nationaal recht strafbare feiten ’.

143. Dit kaderbesluit definieerde in de artikelen 1 tot en met 3 duidelijk en nauwkeurig ‘ terroristische misdrijven ’, ‘ strafbare feiten met betrekking tot een terroristische groep ’ en ‘ strafbare feiten in verband met terroristische activiteiten ’, die de lidstaten ingevolge dit kaderbesluit strafbaar moesten stellen. Ook richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van kaderbesluit 2002/475 en tot wijziging van besluit 2005/671/JBZ van de Raad (PB 2017, L 88, blz. 6) definieert diezelfde strafbare feiten in de artikelen 3 tot en met 14 op duidelijke en nauwkeurige wijze.

144. Ten tweede wordt ‘ ernstige criminaliteit ’ in artikel 3, punt 9, van de PNR-richtlijn gedefinieerd als ‘ de in bijlage II [bij deze richtlijn] bedoelde strafbare feiten, waarop in het nationale recht van een lidstaat een vrijheidsbenemende straf of een tot detentie strekkende maatregel met een maximumduur van ten minste drie jaar staat ’.

145. Om te beginnen somt deze bijlage de verschillende categorieën strafbare feiten die ‘ ernstige criminaliteit ’ in de zin van artikel 3, punt 9, van de PNR-richtlijn kunnen uitmaken uitputtend op.

146. Voorts hadden de strafrechtsystemen van de lidstaten ten tijde van de vaststelling van deze richtlijn, bij gebreke van harmonisatie van de daarin bedoelde strafbare feiten, hun eigen kenmerken, en mocht de Uniewetgever dus gewoon categorieën strafbare feiten bepalen zonder de bestanddelen daarvan te specificeren, te meer daar deze bestanddelen in theorie noodzakelijkerwijs zijn vastgesteld in het nationale recht, waarnaar artikel 3, punt 9, van de PNR-richtlijn verwijst, aangezien de lidstaten het legaliteitsbeginsel inzake delicten en straffen dienen na te leven, dat een onderdeel is van de met de Unie gedeelde gemeenschappelijke waarde van de rechtsstaat, neergelegd in artikel 2 VEU (zie naar analogie arrest van 16 februari 2022, Hongarije/Parlement en Raad, C-156/21, EU:C:2022:97, punten 136, 160 en 234). Het legaliteitsbeginsel inzake delicten en straffen is overigens neergelegd in artikel 49, lid 1, van het Handvest, dat de lidstaten moeten naleven bij de tenuitvoerlegging van een Uniehandeling als de PNR-richtlijn (zie in die zin arrest van 10 november 2011, QB, C-405/10, EU:C:2011:722, punt 48 en aldaar aangehaalde rechtspraak). Bijgevolg moet, mede gelet op de gebruikelijke betekenis van de in bijlage II gebruikte bewoordingen, worden geoordeeld dat daarin voldoende duidelijk en nauwkeurig wordt aangegeven welke strafbare feiten ernstige criminaliteit kunnen vormen.

147. De punten 7, 8, 10 en 16 van bijlage II betreffen weliswaar zeer algemene categorieën van strafbare feiten (fraude, witwassen van opbrengsten van criminaliteit en valsemunterij, milieumisdrijven en illegale handel in cultuurgoederen), maar er wordt niettemin ook in verwezen naar specifieke strafbare feiten die onder deze algemene categorieën vallen. Om voldoende nauwkeurigheid te kunnen garanderen, wat ook artikel 49 van het Handvest vereist, moeten die punten zo worden uitgelegd dat zij verwijzen naar deze strafbare feiten, zoals gespecificeerd in het nationale recht en/of het Unierecht ter zake. Aldus uitgelegd kunnen die punten worden geacht te voldoen aan de vereisten van duidelijkheid en nauwkeurigheid.

148. Tot slot zij er nog aan herinnerd dat de bestrijding van zware criminaliteit volgens het evenredigheidsbeginsel weliswaar een rechtvaardiging kan vormen voor de ernstige inmenging die de PNR-richtlijn in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten veroorzaakt, maar dat dit niet het geval is voor de bestrijding van criminaliteit in het algemeen. Deze laatste doelstelling kan enkel niet-ernstige inmengingen rechtvaardigen (zie naar analogie arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 59 en aldaar aangehaalde rechtspraak). Deze richtlijn moet dan ook middels duidelijke en nauwkeurige regels verzekeren dat het daarbij ingevoerde systeem enkel geldt voor strafbare feiten die zware criminaliteit uitmaken en dus niet voor die welke gewone criminaliteit vormen.

149. Zoals de advocaat-generaal in punt 121 van zijn conclusie heeft opgemerkt, zijn een groot aantal van de in bijlage II bij de PNR-richtlijn genoemde strafbare feiten – zoals mensenhandel, seksuele uitbuiting van kinderen en kinderpornografie, illegale handel in wapens, munitie en explosieven, witwassen, computercriminaliteit/cybercriminaliteit, illegale handel in menselijke organen en weefsels, illegale handel in verdovende middelen en psychotrope stoffen, illegale handel in nucleaire of radioactieve stoffen, kaping van vliegtuigen of schepen, misdrijven die onder de rechtsmacht van het Internationaal Strafhof vallen, moord, verkrachting, ontvoering, wederrechtelijke vrijheidsberoving en gijzeling – naar hun aard ontegensprekelijk zeer ernstig.

150. Andere in die bijlage genoemde strafbare feiten worden weliswaar op het eerste gezicht minder snel met ernstige criminaliteit geassocieerd, maar uit de bewoordingen van artikel 3, punt 9, van de PNR-richtlijn blijkt dat deze strafbare feiten slechts als ernstige criminaliteit kunnen worden beschouwd indien er in het nationale recht van de betrokken lidstaat een vrijheidsbenemende straf of een tot detentie strekkende maatregel met een maximumduur van minstens drie jaar op staat. Met deze vereisten, die betrekking hebben op de aard en de ernst van de toepasselijke straf, kan de toepassing van het systeem van deze richtlijn in principe worden beperkt tot strafbare feiten die voldoende ernstig zijn om de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten die dit systeem creëert, te rechtvaardigen.

151. Aangezien artikel 3, punt 9, van de PNR-richtlijn het niet over de toepasselijke minimumstraf maar over de toepasselijke maximumstraf heeft, valt evenwel niet uit te sluiten dat er PNR-gegevens worden verwerkt om strafbare feiten te bestrijden die weliswaar aan het ernstcriterium in deze bepaling voldoen maar die, gelet op de bijzonderheden van het nationale strafrechtsysteem, geen ernstige criminaliteit maar gewone criminaliteit uitmaken.

152. Het staat dus aan de lidstaten om ervoor te zorgen dat het bij de PNR-richtlijn ingevoerde systeem daadwerkelijk enkel wordt toegepast in de strijd tegen ernstige criminaliteit en niet wordt uitgebreid naar strafbare feiten die gewone criminaliteit vormen.

3*) Verband tussen PNR-gegevens en de doeleinden van de verwerking ervan*

153. Zoals de advocaat-generaal in wezen heeft opgemerkt in punt 119 van zijn conclusie, bevat artikel 3, punten 8 en 9, van de PNR-richtlijn, gelezen in samenhang met bijlage II daarbij, geen uitdrukkelijk criterium dat de werkingssfeer van deze richtlijn beperkt tot strafbare feiten die naar hun aard op zijn minst indirect een objectief verband kunnen vertonen met vliegreizen en dus met de categorieën gegevens die ter uitvoering van deze richtlijn worden doorgegeven, verwerkt en bewaard.

154. Toch kunnen bepaalde van de in bijlage II bij de PNR-richtlijn genoemde strafbare feiten, zoals mensenhandel, illegale handel in verdovende middelen of in wapens, hulp bij illegale binnenkomst en illegaal verblijf en vliegtuigkaping, zoals de advocaat-generaal in punt 121 van zijn conclusie heeft aangegeven, reeds naar hun aard rechtstreeks verband houden met het luchtvervoer van passagiers. Hetzelfde geldt voor bepaalde terroristische misdrijven, zoals het veroorzaken van grootschalige vernieling van vervoersystemen of infrastructurele voorzieningen of het kapen van een luchtvaartuig, die vermeld stonden in artikel 1, lid 1, onder *d)* en *e)*, van kaderbesluit 2002/475, waarnaar artikel 3, punt 8, van de PNR-richtlijn verwijst, en voor reizen met een terroristisch oogmerk en het organiseren of faciliteren van dergelijke reizen, die in de artikelen 9 en 10 van richtlijn 2017/541 worden vermeld.

155. In deze context zij er ook aan herinnerd dat de Commissie haar voorstel voor een richtlijn van het Europees Parlement en de Raad over het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit van 2 februari 2011 [COM(2011) 32 final], dat aan de PNR–richtlijn ten grondslag ligt, heeft gemotiveerd door het feit dat ‘ de terroristische aanslagen in de Verenigde Staten in 2001, de mislukte terroristische aanslag in 2006, waarbij een aantal vliegtuigen onderweg van het Verenigd Koninkrijk en de Verenigde Staten had moeten worden opgeblazen, en de verijdelde terreuraanslag op een vlucht van Amsterdam naar Detroit in december 2009 [duidelijk hebben gemaakt] dat terroristen in welk land dan ook kunnen toeslaan op internationale vluchten ’ en dat ‘ de meeste terroristische activiteiten [...] transnationaal van aard [zijn] en [...] gepaard [gaan] met internationaal verkeer, onder meer naar trainingskampen buiten de EU ’. Ook heeft de Commissie, ter rechtvaardiging van de noodzaak om in de strijd tegen ernstige criminaliteit PNR-gegevens te analyseren, het voorbeeld aangehaald van een groep mensensmokkelaars die valse documenten hadden gebruikt om in te checken voor een vlucht, en van een netwerk van mensen– en drugshandelaars dat, om drugs in te voeren in verschillende delen van Europa, gebruikmaakte van personen die zelf het slachtoffer waren van mensenhandel, en de vliegtuigtickets van deze personen aankocht met gestolen kredietkaarten. In al deze gevallen hielden de strafbare feiten rechtstreeks verband met het luchtvervoer van passagiers : het luchtvervoer was het doelwit of het strafbare feit werd tijdens of door middel van een vliegreis gepleegd.

156. Bovendien moet worden geconstateerd dat ook strafbare feiten die niet rechtstreeks verband houden met het luchtvervoer van passagiers, daar afhankelijk van de omstandigheden een indirect verband mee kunnen vertonen. Dit is met name het geval wanneer luchtvervoer het middel is om dergelijke strafbare feiten voor te bereiden of om strafvervolging te ontlopen nadat ze zijn gepleegd. Strafbare feiten die geen enkel – ook maar indirect – objectief verband vertonen met het luchtvervoer van passagiers, kunnen daarentegen geen rechtvaardiging zijn om het systeem van de PNR-richtlijn toe te passen.

157. In die omstandigheden verlangt artikel 3, punten 8 en 9, van deze richtlijn, gelezen in samenhang met bijlage II daarbij en in het licht van de vereisten die voortvloeien uit de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, dat de lidstaten er met name tijdens de afzonderlijke niet–geautomatiseerde controle als bedoeld in artikel 6, lid 5, van deze richtlijn op toezien dat het systeem van deze richtlijn enkel wordt toegepast voor terroristische misdrijven en ernstige vormen van criminaliteit die, minstens indirect, een objectief verband vertonen met het luchtvervoer van passagiers ».

B.44.2. Uit hetgeen voorafgaat, blijkt dat, om verenigbaar te zijn met de vereisten die met name voortvloeien uit de artikelen 7 et 8, alsook uit artikel 52, lid 1, van het Handvest van de grondrechten, de doeleinden van de verzameling en verwerking van de PNR-gegevens strikt beperkt moeten zijn tot doelen inzake het voorkomen, het opsporen — alsook inzake het onderzoeken en het vervolgen — van terroristische misdrijven en enkel ernstige vormen van criminaliteit, met verwijzing naar de categorieën van misdrijven die op exhaustieve wijze worden opgesomd in bijlage II van de PNR-richtlijn, en die, minstens indirect, een objectief verband vertonen met het betrokken vervoer, waarbij dat systeem niet kan worden uitgebreid tot misdrijven die onder de gewone criminaliteit vallen. Wat betreft die ernstige vormen van criminaliteit kan de toepassing van het PNR-systeem niet worden uitgebreid tot misdrijven die, zelfs indien zij voldoen aan het ernstcriterium waarin die richtlijn voorziet en zelfs indien zij met name worden beoogd in bijlage II ervan, onder de gewone criminaliteit vallen gelet op de bijzonderheden van het nationale strafrechtsysteem (punten 151-152).

B.45.1. Artikel 8 van de wet van 25 december 2016 definieert de doeleinden van de PNR-gegevensverwerking.

In de oorspronkelijke versie ervan bepaalde artikel 8 van de wet van 25 december 2016 :

« § 1. De passagiersgegevens worden verwerkt met het oog op :

1° het opsporen en vervolgen, met inbegrip van de uitvoering van straffen of vrijheidsbeperkende maatregelen, met betrekking tot misdrijven bedoeld in artikel 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° en § 3, van het Wetboek van Strafvordering;

2° het opsporen en vervolgen, met inbegrip van de uitvoering van straffen of vrijheidsbeperkende maatregelen, met betrekking tot misdrijven bedoeld in de artikelen 196, voor wat betreft valsheid in authentieke en openbare geschriften, 198, 199, 199*bis*, 207, 213, 375 en 505 van het Strafwetboek;

3° de preventie van ernstige inbreuken op de openbare veiligheid in het kader van gewelddadige radicalisering door het toezien op fenomenen en groeperingen overeenkomstig artikel 44/5, § 1, 2° en 3° en § 2, van de wet van 5 augustus 1992 op het politieambt;

4° het toezien op activiteiten bedoeld in de artikelen 7, 1° en 3°/1, en 11, § 1, 1° tot 3° en 5°, van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst;

5° het opsporen en vervolgen met betrekking tot de misdrijven bedoeld in artikel 220, § 2, van de algemene wet van 18 juli 1977 inzake douane en accijnzen en artikel 45, derde lid, van de wet van 22 december 2009 betreffende de algemene regeling inzake accijnzen.

§ 2. Onder de voorwaarden bepaald in hoofdstuk 11, worden de passagiersgegevens eveneens verwerkt ter verbetering van de controles van personen aan de buitengrenzen en ter bestrijding van illegale immigratie ».

Krachtens artikel 13, § 2, van de wet van 25 december 2016 « [mag,] onverminderd andere wettelijke bepalingen, [...] de PIE de gegevens die krachtens hoofdstuk 9 zijn bewaard, niet voor andere dan de in artikel 8 bedoelde doelen gebruiken ».

B.45.2.1. Zoals in B.11 is vermeld, is artikel 8, § 1, 1° en 5°, van de wet van 25 december 2016 daarenboven vervangen bij artikel 62 van de wet van 15 juli 2018.

B.45.2.2. Artikel 62 van de wet van 15 juli 2018 vervangt allereerst artikel 8, § 1, 1°, van de wet van 25 december 2016. Oorspronkelijk beoogd werden de « misdrijven bedoeld in artikel 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° en § 3, van het Wetboek van Strafvordering ». Sinds de wijziging aangebracht bij artikel 62 van de wet van 15 juli 2018 worden beoogd de « misdrijven bedoeld in artikel 90*ter*, § 2, 2°, 3°, 7°, 8°, 11°, 14°, 17° tot 20°, 22°, 24° tot 28°, 30°, 32°, 33°, 34°, 36° tot 39°, 43° tot 45° en § 3, van het Wetboek van Strafvordering ».

Gezien die wijzigingen is het beroep tot vernietiging zonder voorwerp geworden in zoverre artikel 8, § 1, 1°, van de wet van 25 december 2016 betrekking heeft op de misdrijven die zijn bedoeld in artikel 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* en 16°, van het Wetboek van strafvordering. Daarentegen behoudt het beroep tot vernietiging zijn voorwerp in zoverre het is gericht tegen artikel 8, § 1, 1°, van de wet van 25 december 2016, daar bij dat artikel de misdrijven worden beoogd die zijn bedoeld in artikel 90*ter*, § 2, 7°, 8°, 11°, 14°, 17°, 18°, 19° en § 3, van het Wetboek van strafvordering.

De misdrijven bedoeld in artikel 90*ter*, § 2, 7°, 8°, 11°, 14°, 17°, 18°, 19° en § 3, van het Wetboek van strafvordering zijn de misdrijven bedoeld in artikel 210*bis* van het Strafwetboek (valsheid in informatica), in de artikelen 246, 247, 248, 249 en 250 van hetzelfde Wetboek (corruptie van personen die een openbaar ambt uitoefenen), in de artikelen 324*bis* en 324*ter* van hetzelfde Wetboek (deelname aan een criminele organisatie), in artikel 347*bis* van hetzelfde Wetboek (gijzelneming), in de artikelen 379, 380 en 383*bis*, §§ 1 en 3, van hetzelfde Wetboek (bederf van de jeugd, prostitutie en schennis van de goede zeden), in artikel 393 van hetzelfde Wetboek (doodslag) en in de artikelen 394 en 397 van hetzelfde Wetboek (moord en vergiftiging).

B.45.2.3. Artikel 62 van de wet van 15 juli 2018 vervangt vervolgens artikel 8, § 1, 5°, van de wet van 25 december 2016. Oorspronkelijk waren beoogd de « misdrijven bedoeld in artikel 220, § 2, van de algemene wet van 18 juli 1977 inzake douane en accijnzen en artikel 45, derde lid, van de wet van 22 december 2009 betreffende de algemene regeling inzake accijnzen ». Sinds de wijziging aangebracht bij artikel 62 van de wet van 15 juli 2018 zijn beoogd de « misdrijven bedoeld in artikel 220, § 2, van de algemene wet van 18 juli 1977 inzake douane en accijnzen, in artikel 45, derde lid, van de wet van 22 december 2009 betreffende de algemene regeling inzake accijnzen, in artikel 5 van de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, in artikel 26 van het decreet van de Duitstalige gemeenschap van 20 februari 2017 ter bescherming van roerende cultuurgoederen van uitzonderlijk belang alsook in artikel 24 van het decreet van de Vlaamse gemeenschap van 24 januari 2003 houdende bescherming van het roerend cultureel erfgoed van uitzonderlijk belang, het ministerieel besluit tot wijziging van het ministerieel besluit van 7 februari 2012 waarbij de invoer van goederen van oorsprong of van herkomst uit Syrië, aan een vergunning onderworpen wordt, zoals gewijzigd bij het ministerieel besluit van 1 juli 2014, het ministerieel besluit van 23 maart 2004 tot opheffing van het ministerieel besluit van 17 januari 2003 waarbij de in–, uit– en doorvoer van goederen van oorsprong of van herkomst uit of met bestemming Irak, aan een voorafgaande machtiging onderworpen wordt en waarbij de in–, uit– en doorvoer van zekere goederen van oorsprong, van herkomst uit of met bestemming Irak aan een vergunning onderworpen wordt alsook het opsporen van misdrijven bedoeld in artikel 5 van de wet van 28 juli 1981 houdende goedkeuring van de Overeenkomst inzake de internationale handel in bedreigde in het wild levende dier– en plantensoorten, en van de Bijlagen, opgemaakt te Washington op 3 maart 1973, alsmede van de Wijziging van de Overeenkomst, aangenomen te Bonn op 22 juni 1979 ».

Aangezien de wijziging aangebracht in artikel 8, § 1, 5°, van de wet van 25 december 2016 bij artikel 62 van de wet van 15 juli 2018 enkel het toepassingsgebied van de beoogde misdrijven uitbreidt, behoudt het beroep tot vernietiging zijn voorwerp in zoverre het is gericht tegen artikel 8, § 1, 5°, van de wet van 25 december 2016, daar dat artikel betrekking heeft op de « misdrijven bedoeld in artikel 220, § 2, van de algemene wet van 18 juli 1977 inzake douane en accijnzen en artikel 45, derde lid, van de wet van 22 december 2009 betreffende de algemene regeling inzake accijnzen ».

Bij die misdrijven wordt ernstige fiscale fraude, al dan niet georganiseerd, op het vlak van de wetgeving inzake douane en accijnzen beoogd.

B.45.3. Wat de door de PNR-richtlijn ingegeven doelstellingen betreft, wordt in de memorie van toelichting bij de wet van 25 december 2016 vermeld :

« Het artikel 8 bepaalt op limitatieve wijze de doelen waarvoor de verwerking van de passagiersgegevens wordt toegelaten.

De § 1 betreft de [vijf] doeleinden die het *corpus* vormen en de essentie zelf zijn van het gebruik van de passagiersgegevens met het oog op het verbeteren van het veiligheidsniveau, in het bijzonder door een precieze, objectieve en professionele analyse van het risico en van de bedreiging die bepaalde passagiers kunnen vormen.

Het eerste doel heeft betrekking op het opsporen en vervolgen van ernstige inbreuken, met inbegrip van terroristische misdrijven die zijn opgenomen in artikel 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° en § 3 van het Wetboek van Strafvordering. Artikel 90*ter* Sv. is in ons materieel recht de referentie in het kader van de kennisname van private communicatie et telecommunicatie, maar ook in tal van andere procedures om het proportionaliteitbeginsel te waarborgen (bijvoorbeeld inzake proactief opsporen of anonieme getuigenis).

De limitatieve lijst van artikel 90*ter* Sv. geeft een opsomming van de ernstige inbreuken die de interne en Europese veiligheid ernstig kunnen bedreigen en sluit dan ook precies aan bij de doelstelling van dit ontwerp.

De uitvoering van de straffen en de vrijheidsbeperkende maatregelen die verband houden met deze inbreuken, zijn woordelijk opgenomen in het doel. Bijvoorbeeld, een passagier staat gesignaleerd omdat hij in België bij verstek veroordeeld is tot 4 jaar gevangenis voor een inbreuk inzake drugshandel en zijn onmiddellijke aanhouding wordt bevolen, of in het kader van een maatregel tot invrijheidstelling onder voorwaarden in een dossier dat verband houdt met een ' *foreign fighter* ', heeft de onderzoekrechter als voorwaarde een verbod om het grondgebied te verlaten, ingesteld.

Dit doel is van gerechtelijke aard en valt derhalve onder de bevoegdheid van de politiediensten, de Douane en de gerechtelijke overheden.

Het tweede doel heeft betrekking op de categorieën van misdrijven die zijn vermeld in bijlage II bij de Europese PNR richtlijn en die niet zijn vervat in artikel 90*ter* Sv. Het betreft de vervalsing van administratieve documenten en handel in valse documenten, verkrachting en handel in gestolen voertuigen. De verwijzing naar art. 196 van het Strafwetboek heeft dan ook betrekking op de authentieke en openbare geschriften en omvat dus niet de handels– of bankgeschriften of private geschriften waarvan sprake in artikel 196, conform de Richtlijn.

De verwerking van de passagiersgegevens voor dit doeleinde beperkt zich tot de verwerking in het kader van gerichte opzoekingen zoals geregeld in artikel 27 van de wet.

[...]

Het vijfde doel heeft betrekking op de misdrijven douane en accijnzen uit annex II van de Europese PNR Richtlijn, zijnde fraude, met inbegrip van fraude ten nadele van de financiële belangen van de Unie.

De tweede paragraaf geeft toestemming voor de verwerking van de passagiersgegevens inzake migratie en asiel.

De overheden die bevoegd zijn voor de materie, zullen deze gegevens dus kunnen verwerken in het kader van de uitvoering van de opdrachten die aan hen worden toegekend, in het bijzonder met het oog op het verbeteren van de grenscontrole en het bestrijden van illegale immigratie.

Deze verwerking zal plaatsvinden binnen de vastgelegde grenzen die voorzien worden in hoofdstuk XI » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, pp. 17-20).

B.45.4. De in artikel 8 van de wet van 25 december 2016 vermelde doeleinden bakenen op exhaustieve wijze de toegelaten verwerking van de passagiersgegevens af.

Zoals in B.10 is vermeld, moet artikel 8 van de wet van 25 december 2016 daarenboven worden geïnterpreteerd in het licht van de wet van 30 juli 2018.

In de in B.10.2 aangehaalde parlementaire voorbereiding van de wet van 30 juli 2018 wordt vermeld dat de doelen beoogd in artikel 8 van de wet van 25 december 2016 onder drie categorieën vallen :

- de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen (artikel 8, § 1, 1°, 2°, 3° en 5°, van de wet van 25 december 2016); die verwerkingen worden geregeld bij titel 2 van de wet van 30 juli 2018;

- de opdrachten van de inlichtingen– en veiligheidsdiensten als bedoeld in de artikelen 7 en 11 van de wet van 30 november 1998 (artikel 8, § 1, 4°, van de wet van 25 december 2016); die verwerkingen worden geregeld bij titel 3 van de wet van 30 juli 2018;

- de verbetering van de controles van personen aan de buitengrenzen en de strijd tegen illegale immigratie (artikel 8, § 2, van de wet van 25 december 2016); die verwerkingen worden geregeld bij titel 1 van de wet van 30 juli 2018.

B.46.1. Uit hetgeen in B.45 is vermeld, blijkt dat sommige van de in artikel 8 van de wet van 25 december 2016 beoogde verwerkingsdoelen overeenstemmen met de in bijlage II van de PNR-richtlijn bedoelde misdrijven, overeenkomstig de in de richtlijn beoogde doelstellingen inzake het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en zware criminaliteit (artikel 8, § 1, 1°, 2° en 5°), en betrekking hebben op ernstige vormen van misdrijven volgens het nationaal recht.

Zoals in B.31.1 is vermeld, vormt het nastreven van die doelstellingen, door het verzamelen en het verwerken van de PNR-gegevens, een doel van algemeen belang dat het mogelijk maakt een inmenging in het recht op eerbiediging van het privéleven en van de bescherming van persoonsgegevens, te verantwoorden.

Zoals het Hof van Justitie heeft geoordeeld in zijn arrest in zake *Ligue des droits humains t. Ministerraad*, aangehaald in B.44, is de toepassing van het PNR-systeem op dergelijke doeleinden, die strikt beperkt zijn tot het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige vormen van criminaliteit, verenigbaar met de vereisten van het « strikt noodzakelijke ».

B.46.2. De bewoordingen die worden gebruikt om die doeleinden te bepalen, zijn duidelijk en nauwkeurig gedefinieerd, aangezien zij verwijzen naar de misdrijven die zijn gedefinieerd bij de bepalingen van het Strafwetboek.

Dergelijke regels, die de misdrijven bepalen die men beoogt te voorkomen, op te sporen en te vervolgen, zijn duidelijk en nauwkeurig, en blijven beperkt tot wat strikt noodzakelijk is, overeenkomstig de in B.25 in herinnering gebrachte vereisten.

B.47.1. Daarentegen komen sommige doelstellingen van de verwerking van PNR-gegevens bovenop die waarin is voorzien bij de PNR-richtlijn. Dat geldt voor :

- de « preventie van ernstige inbreuken op de openbare veiligheid in het kader van gewelddadige radicalisering door het toezien op fenomenen en groeperingen overeenkomstig artikel 44/5, § 1, 2° en 3° en § 2, van de wet van 5 augustus 1992 op het politieambt » (artikel 8, § 1, 3°);

- het « toezien op activiteiten bedoeld in de artikelen 7, 1° en 3° /1, en 11, § 1, 1° tot 3° en 5°, van de wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst » (artikel 8, § 1, 4°);

- de « verbetering van de controles van personen aan de buitengrenzen en [de] bestrijding van illegale immigratie » (artikel 8, § 2).

B.47.2. Er dient te worden onderzocht of die andere doelstellingen neergelegd zijn in duidelijke en nauwkeurige regels die beperkt blijven tot wat strikt noodzakelijk is, overeenkomstig de in B.25 vermelde vereisten, en rekening houdend met het arrest van het Hof van Justitie, waaraan wordt herinnerd in B.44.

B.48. Wat betreft het doel van « preventie van ernstige inbreuken op de openbare veiligheid in het kader van gewelddadige radicalisering door het toezien op fenomenen en groeperingen overeenkomstig artikel 44/5, § 1, 2° en 3° en § 2, van de wet van 5 augustus 1992 op het politieambt » (artikel 8, § 1, 3°) heeft het Hof, bij zijn arrest nr. 135/2019, geoordeeld :

« B.53.1. Wat het in artikel 8, § 1, 3°, van de wet van 25 december 2016 beoogde doel betreft van preventie van ernstige inbreuken op de openbare veiligheid in het kader van gewelddadige radicalisering, wordt verwezen naar het toezien op ' fenomenen ' en ' groeperingen ' overeenkomstig artikel 44/5, § 1, 2° en 3° en § 2, van de wet van 5 augustus 1992 ' op het politieambt ' (hierna : de wet van 5 augustus 1992).

Artikel 44/1 van de wet van 5 augustus 1992 bepaalt dat, in het kader van de uitoefening van hun opdrachten, de politiediensten informatie en persoonsgegevens kunnen verwerken.

Wanneer de uitoefening van de opdrachten van bestuurlijke politie en van gerechtelijke politie vereist dat de politiediensten die persoonsgegevens en informatie structureren zodat ze rechtstreeks kunnen worden teruggevonden, worden die, overeenkomstig artikel 44/2 van de wet van 5 augustus 1992, verwerkt in een operationele politionele gegevensbank (1° de Algemene Nationale Gegevensbank, 2° de basisgegevensbanken of 3° de bijzondere gegevensbanken) volgens de eigen doelstellingen van elke categorie van gegevensbanken.

Artikel 44/5, § 1, 2° en 3° en § 2, van de wet van 5 augustus 1992 bepaalt :

' De persoonsgegevens die voor doeleinden van bestuurlijke politie verwerkt worden in de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 1° en 2°, zijn :

[...]

2° de gegevens met betrekking tot de personen die betrokken zijn bij fenomenen van bestuurlijke politie waaronder verstaan wordt het geheel van problemen die de openbare orde verstoren en die gepaste maatregelen van bestuurlijke politie vereisen omdat zij van dezelfde aard en terugkerend zijn, door dezelfde personen gepleegd worden of gericht zijn op dezelfde categorieën van slachtoffers of plaatsen;

3° de gegevens met betrekking tot de leden van een nationale of internationale groepering die de openbare orde zoals bedoeld in artikel 14 zou kunnen verstoren;

[...]

§ 2. De lijst met de fenomenen bedoeld in § 1, 2° en de groeperingen bedoeld in § 1, 3°, wordt minstens jaarlijks uitgewerkt door de minister van Binnenlandse Zaken, op basis van een gezamenlijk voorstel van de federale politie, het Coördinatieorgaan voor de dreigingsanalyse en de inlichtingen– en veiligheidsdiensten. '.

B.53.2. Wat het in artikel 8, § 1, 3°, beoogde doel betreft, wordt in de memorie van toelichting vermeld :

' Het derde doel ligt in de lijn van de uitoefening van de opdrachten van bestuurlijke politie van de politiediensten.

Overeenkomstig de wet op het politieambt kunnen de politiediensten, in het kader van de uitoefening van hun opdrachten van bestuurlijke politie, persoonsgegevens verwerken voor zover ze toereikend, ter zake dienend en niet overmatig van aard zijn.

Dit specifiek [doel] kadert binnen een globale aanpak van het fenomeen dat verbonden is met gewelddadige radicalisering die een rechtstreekse impact heeft op de bescherming van de belangen die door dit voorontwerp van wet worden verdedigd.

Omzendbrief GPI 78 van 31 januari 2014 omschrijft gewelddadige radicalisering als " een proces waardoor een individu of een groep dusdanig beïnvloed wordt dat het individu of de groep in kwestie mentaal bereid is om extremistische daden te plegen, gaande tot gewelddadige of zelfs terroristische handelingen ".

Het is essentieel dat in het kader van het volgen van het radicalisme of van de hiermee verbonden groeperingen die een ernstige bedreiging vormen voor de openbare orde, de passagiersgegevens ook beperkt kunnen worden gebruikt. Hierbij denken we bijvoorbeeld aan de aanwezigheid op ons grondgebied tijdens al dan niet geplande evenementen van leden van een groepering die extremistische ideeën uitdragen die in strijd zijn met de democratische waarden en principes.

De informatie die hierbij wordt verwerkt, mag enkel dienen om maatregelen te nemen teneinde de openbare orde te waarborgen. Indien men bijvoorbeeld te weten komt dat een 30–tal leden van een groepering van plan zijn om naar België te komen voor een samenkomst, zullen er meer aangepaste maatregelen voor de handhaving van de openbare orde kunnen worden genomen (versterking van het apparaat, speciale middelen, ...).

In dit opzicht is dit doel uiterst beperkend in de toepassing ervan.

Immers, enkel het fenomeen van gewelddadige radicalisering en de hiermee verbonden groeperingen zoals vermeld in een gesloten lijst, die jaarlijks wordt opgesteld door de minister van Binnenlandse Zaken, na advies van de Federale Politie, het OCAD en de inlichtingen– en veiligheidsdiensten, kunnen de verwerking rechtvaardigen. Het gaat hier dus niet om het verwerken van passagiersgegevens voor eender welk evenement of wanneer de openbare orde dreigt verstoord te geraken.

Bovendien beperkt het ontworpen artikel 24, § 3 sterk de verwerkingswijzen en –voorwaarden en sluit het bovenvermeld artikel het gebruik van risicoprofielen uit dit doel. Artikel 27 sluit gericht opzoekingswerk uit dit doel (*cfr. infra*) ' (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, pp. 18-19).

De minister van Veiligheid en Binnenlandse Zaken heeft ook gepreciseerd dat het begrip ' gewelddadige radicalisering ' ' in de zin van de omzendbrief [moet] worden begrepen ' (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/003, p. 31).

B.53.3. Uit het voorgaande blijkt dat het doel van preventie van ernstige inbreuken op de openbare veiligheid in het kader van gewelddadige radicalisering beperkt is tot een ernstige bedreiging voor de openbare orde die voortvloeit uit de gewelddadige radicalisering in de zin van de ministeriële omzendbrief GPI 78 van 31 januari 2014 ' betreffende de informatieverwerking ten voordele van een geïntegreerde aanpak van terrorisme en gewelddadige radicalisering door de politie ' (hierna : de ministeriële omzendbrief).

B.53.4. Dat doel maakt daarenboven, in het kader van de voorafgaande beoordeling van de passagiers, het voorwerp uit van een beperktere verwerking dan de andere doelstellingen van preventie en opsporing van de in artikel 8, § 1, van de wet van 25 december 2016 bedoelde strafrechtelijke misdrijven.

Zo bepaalt artikel 24, § 3, van de wet van 25 december 2016 dat, in het kader van de doeleinden beoogd in artikel 8, § 1, 3°, ' de voorafgaande beoordeling van de passagiers op een positieve overeenstemming [berust], voortvloeiende uit een correlatie van de passagiersgegevens met de gegevensbanken bedoeld in § 2, 1° '. Bovendien bepaalt artikel 26, § 1, van de wet van 25 december 2016 dat, voor het in artikel 8, § 1, 3°, bedoelde doel enkel de passagiersgegevens bedoeld in artikel 9, § 1, 18° (' API-gegevens ') met betrekking tot de persoon of personen voor wie een positieve overeenstemming werd gegenereerd, toegankelijk zullen zijn. Tot slot sluit artikel 27 van de wet van 25 december 2016 uit gerichte opzoekingen te verrichten voor de doelstellingen beoogd in artikel 8, § 1, 3°.

In de parlementaire voorbereiding van de wet van 25 december 2016 wordt uiteengezet :

' Paragraaf 3 van artikel 24 betreft de voorafgaande beoordeling in het kader van het doel met betrekking tot het toezien op fenomenen van bestuurlijke politie en groeperingen die verbonden zijn met gewelddadige radicalisering.

Dit doel is aan veel strengere voorwaarden onderworpen dan de andere doelen. De voorafgaande beoordeling in dit kader kan zich enkel baseren op een correlatie met de gegevensbanken van de politiediensten. Er kan geen enkel vooraf bepaald criterium worden toegepast. Deze beperkende voorwaarden zijn gewettigd door het feit dat de verwerking meestal is gelinkt aan het eventueel onmiddellijk nemen van een maatregel om de openbare orde te waarborgen. Het is bijvoorbeeld noodzakelijk dat de diensten worden ingelicht over de komst op ons grondgebied van een persoon die opgenomen is op de lijst van een op te volgen groepering. We herinneren er in dit verband aan dat het opstellen van deze lijsten aan strikte voorwaarden is onderworpen en dat enkel de personen die een ernstige dreiging vormen voor de openbare orde in verband met gewelddadige radicalisering, hierin zijn opgenomen. Het louter deelnemen aan bijvoorbeeld een antiglobalistische betoging vormt geen afdoend criterium ' (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, p. 30).

B.53.5. Hoewel de begrippen ‘ fenomenen ’ en ‘ groeperingen ’ in artikel 44/5, § 1, 2° en 3°, en § 2, van de wet van 5 augustus 1992 zijn gedefinieerd, geldt hetzelfde echter niet voor het begrip ‘ gewelddadige radicalisering ’, dat niet wettelijk is gedefinieerd.

Niettemin wordt het ‘ radicaliseringsproces ’ bij artikel 3, 15°, van de wet van 30 november 1998 ‘ houdende regeling van de inlichtingen– en veiligheidsdiensten ’ (hierna : de wet van 30 november 1998) gedefinieerd als ‘ een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen ’.

Daarenboven wordt in artikel M.1 van de ministeriële omzendbrief ‘ gewelddadige radicalisering ’ als volgt gedefinieerd :

‘ Gewelddadige radicalisering is een proces waardoor een individu of een groep dusdanig beïnvloed wordt dat het individu of de groep in kwestie mentaal bereid is om extremistische daden te plegen, gaande tot gewelddadige of zelfs terroristische handelingen. Het adjectief “ gewelddadig ” wordt hierbij gebruikt om een duidelijk onderscheid te maken tussen enerzijds niet strafbare denkbeelden en de uiting hiervan en anderzijds de misdrijven of handelingen die een gevaar zijn voor de openbare veiligheid die gepleegd worden om deze denkbeelden te realiseren of de intentie tot het plegen van deze misdrijven of handelingen.

Onder extremistisch geweld verstaan we geweld tegen personen of goederen dat wordt gepleegd vanuit een ideologische, politieke of religieuze motivatie zonder dat dit echter voldoet aan de strafrechtelijke definitie van terrorisme ’.

Hoewel het begrip ‘ gewelddadige radicalisering ’ niet wettelijk gedefinieerd is, wijst de definitie ervan door middel van de ministeriële omzendbrief erop dat het wordt begrepen via de in artikel 44/5, § 1, 2° en 3°, en § 2, van de wet van 5 augustus 1992 wettelijk gedefinieerde begrippen ‘ fenomenen ’ en ‘ groeperingen ’. Een dergelijke maatregel is dus niet zonder duidelijkheid en nauwkeurigheid.

B.53.6. Die definitie doet bovendien blijken dat ‘ gewelddadige radicalisering ’, begrepen via ‘ fenomenen ’ en ‘ groeperingen ’, in rechtstreeks verband staat met terroristische handelingen of zware criminaliteit, die zowel de ‘ PNR-richtlijn ’ als de wet van 25 december 2016 beogen te voorkomen, op te sporen en te vervolgen.

Een dergelijke maatregel is dus duidelijk en nauwkeurig en is niet onevenredig gezien de te dezen nagestreefde legitieme doelstellingen ».

B.49.1. Zoals het Hof heeft geoordeeld bij zijn voormelde arrest nr. 135/2019 is het doel van preventie van « ernstige inbreuken » op de openbare veiligheid in het kader van de « gewelddadige radicalisering » een begrip dat een groepsfenomeen betreft dat de openbare veiligheid ernstig in gevaar brengt en dat rechtstreeks verband houdt met terroristische misdrijven of ernstige vormen van criminaliteit, hetgeen zowel de PNR-richtlijn als de wet van 25 december 2016 beogen te voorkomen, op te sporen en te vervolgen.

Hieruit vloeit voort dat de preventie van « ernstige inbreuken » op de openbare veiligheid in het kader van de « gewelddadige radicalisering » die alleen in verband zou staan met het plegen van gemeenrechtelijke misdrijven, niet valt onder het doel dat wordt beoogd in artikel 8, § 1, 3°, van de wet van 25 december 2016.

De verwerking en de verzameling van PNR-gegevens voor dat aldus begrepen doel vallen bijgevolg onder de doelstellingen die worden nagestreefd met de PNR-richtlijn, zoals die in herinnering zijn gebracht door het Hof van Justitie, in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022. Zoals is vermeld in B.53.4 van het voormelde arrest nr. 135/2019, is de verwerking van PNR-gegevens, voor dat doel, bovendien beperkter dan de andere doelen van preventie en opsporing van strafrechtelijke misdrijven beoogd in artikel 8, § 1, van de wet van 25 december 2016.

B.49.2. Zoals het Hof van Justitie heeft aangegeven in zijn voormeld arrest in zake *Ligue des droits humains t. Ministerraad* van 23 juni 2022, waaraan wordt herinnerd in B.44, moeten doeleinden van verwerking van de PNR-gegevens overigens, minstens indirect, een objectief verband vertonen met het betrokken vervoer.

Hieruit vloeit voort dat de preventie van « ernstige inbreuken » op de openbare veiligheid in het kader van de « gewelddadige radicalisering » die geen gebruik zou vereisen van vervoermiddelen, niet kan vallen onder het toepassingsgebied van het doel beoogd in artikel 8, § 1, 3°, van de wet van 25 december 2016.

B.49.3. Onder voorbehoud dat het doel van preventie van « ernstige inbreuken » op de openbare veiligheid in het kader van de « gewelddadige radicalisering » zo wordt geïnterpreteerd dat het strikt is beperkt tot de doelen van preventie en opsporing van enkel terroristische misdrijven en ernstige vormen van criminaliteit, met verwijzing naar de categorieën van misdrijven die op exhaustieve wijze zijn opgesomd in bijlage II van de PNR-richtlijn, met uitsluiting van de gemeenrechtelijke misdrijven, en die, op zijn minst indirect, een objectief verband vertonen met het betrokken vervoer, overschrijdt artikel 8, § 1, 3°, van de wet van 25 december 2016 niet de grenzen van het « strikt noodzakelijke ».

B.50.1. Overeenkomstig artikel 8, § 1, 4°, van de wet van 25 december 2016 beoogt de verwerking van de PNR-gegevens het toezicht op activiteiten bedoeld in de artikelen 7, 1° en 3°/1, en 11, § 1, 1° tot 3° en 5°, van de wet van 30 november 1998.

Artikel 7 van de wet van 30 november 1998 bepaalt :

« De Veiligheid van de Staat heeft als opdracht :

1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;

[...]

3°/1 het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied;

[...] ».

Artikel 11, § 1, van de wet van 30 november 1998 bepaalt :

« De Algemene Dienst Inlichting en Veiligheid heeft als opdracht :

1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die :

a) de onschendbaarheid van het nationaal grondgebied of de bevolking,

b) de militaire defensieplannen,

c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,

d) de vervulling van de opdrachten van de strijdkrachten,

e) de veiligheid van de Belgische onderdanen in het buitenland,

f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;

en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie;

2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheerst, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten;

3° het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica– en verbindingssystemen of die systemen die de Minister van Landsverdediging beheert;

[...]

5° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied ».

B.50.2. Wat dat doel betreft, wordt in de memorie van toelichting vermeld :

« Het vierde doel heeft betrekking op de bevoegdheden van de inlichtingendiensten, namelijk de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid (ADIV). Om hun opdrachten inzake opzoeking, analyse en verwerking van inlichtingen met betrekking tot de activiteiten die de fundamentele belangen van de Staat kunnen bedreigen, uit te voeren, moeten deze diensten in staat zijn de passagiersgegevens te analyseren teneinde concrete dreigingen zo vroeg mogelijk op te sporen, verplaatsingen van specifieke personen te volgen of analyses van fenomenen of tendensen in de ruimere zin op te stellen. De opdrachten inzake het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied ressorteren ook onder dit doel.

De Veiligheid van de Staat vervult een onmisbare rol in het opsporen en bewaken van ' *foreign fighters* ', maar ook in andere destabiliserende activiteiten zoals die gelinkt aan criminele of extremistische organisaties.

De ADIV oefent in het bijzonder opdrachten uit die verband houden met de bescherming van de integriteit van het nationaal grondgebied, met de bescherming van onze strijdkrachten op missie in het buitenland en met betrekking tot de veiligheid van de Belgen in het buitenland.

Ten slotte neemt de actie van de inlichtingendiensten in tal van gevallen ook deel aan het politionele en gerechtelijke antwoord achteraf in het licht van het eerste doel » (*ibid.*, pp. 19—20).

B.51.1. Op een vraag van het Hof over het doel van toezicht op activiteiten door de inlichtingen– en veiligheidsdiensten heeft het Hof van Justitie, in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geantwoord :

« 229. Met zijn vijfde vraag wenst de verwijzende rechter te vernemen of artikel 6 van de PNR–richtlijn, gelezen in het licht van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen nationale wetgeving die toestaat dat overeenkomstig deze richtlijn verzamelde PNR–gegevens worden verwerkt zodat de inlichtingen– en veiligheidsdienst toezicht kan uitoefenen op activiteiten.

230. Uit het verzoek om een prejudiciële beslissing blijkt dat de verwijzende rechter met deze vraag meer in het bijzonder doelt op de activiteiten van de Veiligheid van de Staat (België) en de Algemene Inlichtingen– en Veiligheidsdienst (België) in het kader van hun respectieve taken op het gebied van de bescherming van de nationale veiligheid.

231. De Uniewetgever heeft ter eerbiediging van de beginselen van wettigheid en evenredigheid, waarop artikel 52, lid 1, van het Handvest met name ziet, duidelijke en nauwkeurige regels vastgesteld rond de doeleinden van de maatregelen van de PNR–richtlijn die inmengingen veroorzaken in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten.

232. Artikel 1, lid 2, van de PNR–richtlijn bepaalt namelijk uitdrukkelijk dat overeenkomstig deze richtlijn verzamelde PNR–gegevens uitsluitend mogen worden verwerkt ' om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen overeenkomstig artikel 6, lid 2, onder *a)*, *b)* en *c)*[, van deze richtlijn] '. Laatstgenoemde bepaling bevestigt het principe van artikel 1, lid 2, en hanteert systematisch de begrippen ' terroristisch misdrijf ' en ' ernstige criminaliteit '.

233. Uit de bewoordingen van deze bepalingen blijkt dus duidelijk dat de daarin gegeven opsomming van de doelstellingen die met de verwerking van PNR–gegevens krachtens de PNR–richtlijn worden nagestreefd, exhaustief is.

234. Deze uitlegging vindt onder meer steun in overweging 11 van de PNR–richtlijn, volgens welke de verwerking van PNR–gegevens evenredig moet zijn aan ' de specifieke veiligheidsdoelen ' die met deze richtlijn worden nagestreefd, en in artikel 7, lid 4, ervan, dat luidt dat PNR–gegevens en het verwerkingsresultaat daarvan die van de PIE zijn ontvangen, uitsluitend verder mogen worden verwerkt ' met als specifieke doelstellingen het voorkomen, opsporen, onderzoeken of vervolgen van terroristische misdrijven of ernstige criminaliteit '.

235. Het exhaustieve karakter van de doelstellingen in artikel 1, lid 2, van de PNR–richtlijn impliceert voorts ook dat PNR–gegevens niet mogen worden bewaard in één databank die zowel voor deze als voor andere doeleinden kan worden geraadpleegd. Dit zou immers het risico inhouden dat de gegevens worden gebruikt voor andere doeleinden dan de in artikel 1, lid 2, genoemde.

236. Voor zover volgens de in het hoofdgeding aan de orde zijnde nationale wetgeving ' toezien op activiteiten van de inlichtingen– en veiligheidsdienst ' een doelstelling van het verwerken van PNR–gegevens is, en deze doelstelling dus mee wordt begrepen in het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, zoals de verwijzende rechter meent, gaat deze wetgeving mogelijkerwijs voorbij aan het uitputtend karakter van de lijst van doeleinden die de verwerking van PNR–gegevens bij de PNR–richtlijn nastreeft. Het staat aan de verwijzende rechter om dit te verifiëren.

237. Bijgevolg dient op de vijfde vraag te worden geantwoord dat artikel 6 van de PNR–richtlijn, gelezen in het licht van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen nationale wetgeving die toestaat dat overeenkomstig deze richtlijn verzamelde PNR-gegevens worden verwerkt voor andere doeleinden dan die welke uitdrukkelijk worden genoemd in artikel 1, lid 2, van deze richtlijn ».

B.51.2. Uit hetgeen voorafgaat, vloeit voort dat, gelet op het exhaustieve karakter van de doeleinden beoogd in artikel 1, lid 2, van de PNR-richtlijn, het Hof van Justitie ervan uitgaat dat, indien het toezicht op de beoogde activiteiten door de inlichtingen– en veiligheidsdiensten, wordt gezien als een doeleinde van de verwerking van de PNR-gegevens, waardoor dat doel aldus wordt opgenomen in de preventie en opsporing van terroristische misdrijven en ernstige vormen van criminaliteit, alsook in de onderzoeken en vervolgingen ter zake, een wetgeving zoals de wet van 25 december 2016 mogelijkerwijs kan voorbijgaan aan het uitputtend karakter van de lijst van doeleinden die de verwerking van PNR-gegevens bij de PNR-richtlijn nastreeft, hetgeen door het Hof moet worden geverifieerd (punt 236).

Het Hof van Justitie onderstreept tevens dat « het exhaustieve karakter van de doelstellingen in artikel 1, lid 2, van de PNR-richtlijn [...] voorts ook [impliceert] dat PNR–gegevens niet mogen worden bewaard in één databank die zowel voor deze als voor andere doeleinden kan worden geraadpleegd. Dit zou immers het risico inhouden dat de gegevens worden gebruikt voor andere doeleinden dan de in artikel 1, lid 2, genoemde » (punt 235).

B.52.1. Hoewel, zoals het Hof heeft geoordeeld bij zijn arrest nr. 135/2019, de opdrachten van de inlichtingen– en veiligheidsdiensten, waaraan wordt herinnerd in B.50, in het algemeen bijdragen tot de nationale en internationale veiligheid (B.54.3), lijkt de verwerking van de PNR-gegevens in het licht van het doel beoogd in artikel 8, § 1, 4°, van de wet van 25 december 2016 zeer vaag en algemeen. Er kan immers niet worden aangenomen dat de door de inlichtingen– en veiligheidsdiensten beoogde activiteiten uitsluitend en steeds ertoe strekken terroristische misdrijven of ernstige vormen van criminaliteit te voorkomen. In tegenstelling tot wat de Ministerraad aanvoert in zijn aanvullende memorie, laat het « hybride » karakter van de terroristische misdrijven en ernstige vormen van criminaliteit niet toe ervan uit te gaan dat het doel van toezicht op de activiteiten beoogd in artikel 8, § 1, 4°, van de wet van 25 december 2016 de grenzen van het « strikt noodzakelijke » in acht neemt.

Het Hof stelt derhalve vast dat het « toezien op de bedoelde activiteiten door de inlichtingen– en veiligheidsdiensten » niet toelaat een rechtstreeks verband vast te stellen tussen dat doel en de preventie of de opsporing van terroristische misdrijven of ernstige vormen van criminaliteit, alsook van onderzoeken of vervolgingen ter zake, die de doeleinden zijn van de verwerking van de PNR-gegevens volgens de PNR-richtlijn.

Bovendien kan dat doel niet worden geacht, minstens indirect, een objectief verband te vertonen met het passagiersvervoer, verband dat de doeleinden van de verwerking van de PNR-gegevens moeten vertonen, zoals het Hof van Justitie dat heeft aangegeven in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, waaraan wordt herinnerd in B.44.

B.52.2. Gelet op het exhaustieve karakter van de doeleinden beoogd in artikel 1, lid 2, van de PNR-richtlijn, dient ervan te worden uitgegaan dat het doel beoogd in artikel 8, § 1, 4°, van de wet van 25 december 2016 de grenzen van het « strikt noodzakelijke » overschrijdt.

B.53.1. Wat betreft het doel van verbetering van de controles van personen aan de buitengrenzen, en meer bepaald de bestrijding van illegale immigratie, beoogd in artikel 8, § 2, van de wet van 25 december 2016, heeft het Hof, bij zijn arrest nr. 135/2019, geoordeeld :

« B.55.1. Tot slot maakt artikel 8, § 2, van de wet van 25 december 2016 het mogelijk de ' PNR-gegevens ' te verwerken, onder de voorwaarden bepaald in hoofdstuk 11 (artikelen 28 tot 31) van de wet van 25 december 2016, ter verbetering van de controles van personen aan de buitengrenzen en meer precies ter bestrijding van de illegale immigratie.

B.55.2. Wat dat doel betreft, wordt in de memorie van toelichting aangegeven :

' Het is noodzakelijk en onvermijdelijk dat de politiediensten en de Dienst Vreemdelingenzaken betrokken worden bij de aanpak van de fenomenen van gewelddadige radicalisering, van ' *foreign fighters* ', van ' *returnees* ' en bij de strijd tegen het terrorisme en de grootschalige criminaliteit, zoals de mensenhandel en de mensensmokkel

[...]

Het is dus van wezenlijk belang dat de politiediensten en de Dienst Vreemdelingenzaken in het kader van de controle aan de buitengrenzen en op het grondgebied, alsook in het kader van de verblijfs– en asielprocedures, gebruik kunnen maken van bepaalde passagiersgegevens.

Ze zullen dus toegang hebben tot bepaalde passagiersgegevens, en dit gedurende een beperkte periode. De bedoeling is dus dat de politiediensten en de Dienst Vreemdelingenzaken in staat zijn om hun wettelijke opdrachten correct uit te voeren en dat tegelijkertijd gegarandeerd wordt dat de persoonsgegevens, met het oog op de nagestreefde doelstellingen, afdoende beschermd worden.

De passagiersgegevensbank is een onontbeerlijk instrument voor hun acties. De passagiersgegevens waartoe ze toegang zullen hebben of die aan hen zullen moeten worden doorgegeven, helpen hen bij de uitvoering van hun taken, zoals de identificatie van de personen, de verificatie van de authenticiteit en de geldigheid van de documenten die gebruikt werden om België binnen te komen, er te verblijven of het land te verlaten (identiteitsdocument, paspoort, visa, verblijfsdocument of –titel, transporttickets, enz.), de verificatie van de verklaringen van de betrokken personen, de motivering en de uitvoering van de beslissingen die ter zake worden genomen.

Ze zullen dus worden gebruikt in het kader van de visumprocedures, tijdens de controles die aan de buitengrenzen en op het grondgebied worden uitgevoerd, voor de opvolging van het verblijf of voor de uitvoering van de verwijderingsmaatregelen. Ze zullen ook kunnen worden gebruikt in de asielprocedures, voor de bepaling van de Staat die verantwoordelijk is voor de asielaanvraag en voor het nemen van een beslissing, met inbegrip van de intrekking van de vluchtelingenstatus of de subsidiaire bescherming ' (*ibid.*, pp. 9-10).

' De tweede paragraaf geeft toestemming voor de verwerking van de passagiersgegevens inzake migratie en asiel.

De overheden die bevoegd zijn voor de materie, zullen deze gegevens dus kunnen verwerken in het kader van de uitvoering van de opdrachten die aan hen worden toegekend, in het bijzonder met het oog op het verbeteren van de grenscontrole en het bestrijden van illegale immigratie.

Deze verwerking zal plaatsvinden binnen de vastgelegde grenzen die voorzien worden in hoofdstuk XI ' (*ibid.*, p. 20).

' De doelen van de verwerking van de passagiersgegevens zijn identiek aan die van de richtlijn 2004/82/EG. Uit de overwegingen en het dispositief blijkt duidelijk dat de richtlijn hoofdzakelijk de controle van de migratiestromen, de strijd tegen de illegale immigratie, de verbetering van de controles aan de buitengrenzen en de bescherming van de openbare orde en de nationale veiligheid beoogt ' (*ibid.*, p. 33).

De afdeling wetgeving van de Raad van State heeft eveneens doen opmerken :

' In de artikelen 28 en 29, die behoren tot hoofdstuk XI – De verwerking van de passagiersgegevens ter verbetering van de grenscontroles en ter bestrijding van de illegale immigratie, van het voorontwerp wordt het begrip ' buitengrenzen ' van België gebruikt. Dat begrip buitengrenzen wordt gedefinieerd in artikel 2, *b)*, van richtlijn 2004/82/EG dat meer bepaald bij hoofdstuk XI van het voorontwerp wordt omgezet ' (*ibid.*, p. 97).

B.55.3. De verwerking van de passagiersgegevens wat betreft het doel beoogd in artikel 8, § 2, wordt afgebakend door de artikelen 28 tot 31 van de wet van 25 december 2016.

Enkel de passagiersgegevens bedoeld in artikel 9, § 1, 18°, van de wet van 25 december 2016 worden doorgegeven aan de politiediensten bedoeld in artikel 14, § 1, 2°, *a)* en aan de Dienst Vreemdelingenzaken, om hen in staat te stellen hun wettelijke opdrachten te vervullen (artikel 29). Enkel betrokken zijn de passagiers die van plan zijn om het grondgebied via de buitengrenzen van België te betreden of het grondgebied via de buitengrenzen van België betreden hebben (artikel 29, § 2, 1°), de passagiers die van plan zijn om het grondgebied via de buitengrenzen van België te verlaten of het grondgebied via de buitengrenzen van België verlaten hebben (artikel 29, § 2, 2°) en de passagiers die van plan zijn om via een in België gelegen internationale transitzone te passeren, die zich in een in België gelegen internationale transitzone bevinden of die via een in België gelegen transitzone gepasseerd zijn (artikel 29, § 2, 3°).

Die gegevens worden onmiddellijk na hun registratie in de passagiersgegevensbank doorgestuurd naar de politiediensten zoals bedoeld in artikel 14, § 1, 2°, *a)* en aan de Dienst Vreemdelingenzaken wanneer de dienst die gegevens nodig heeft voor de vervulling van zijn wettelijke opdrachten; die gegevens worden bewaard in een tijdelijk bestand en vernietigd binnen de vierentwintig uur na doorsturing (artikel 29, §§ 3 en 4). Na die termijn kan de Dienst Vreemdelingenzaken ook een afdoende gemotiveerde aanvraag tot de PIE richten teneinde tot die gegevens toegang te hebben (artikel 29, § 4, tweede lid). De Dienst Vreemdelingenzaken stuurt maandelijks een verslag naar de Commissie voor de bescherming van de persoonlijke levenssfeer - thans de Gegevensbeschermingsautoriteit - betreffende de toepassing van artikel 29, § 4, tweede lid (artikel 29, § 4, derde lid).

Een protocol dat de technische beveiligings– en toegangsregels preciseert, alsook de nadere regels voor de doorgifte van de passagiersgegevens aan de politiediensten belast met de grenscontroles en aan de Dienst Vreemdelingenzaken, moet worden afgesloten, in overleg met de functionaris voor de gegevensbescherming en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer (Gegevensbeschermingsautoriteit), tussen, enerzijds, de leidend ambtenaar van de PIE en, anderzijds, de Commissaris-generaal van de federale politie en de leidend ambtenaar van de Dienst Vreemdelingenzaken (artikel 30).

De vervoerders en de reisoperatoren vernietigen, binnen de vierentwintig uur na het einde van het in artikel 4, 3° tot 6°, bedoelde vervoer, alle in artikel 9, § 1, 18°, bedoelde passagiersgegevens, die ze overeenkomstig artikel 7 doorsturen (artikel 31, zoals gewijzigd bij de wet van 15 juli 2018).

B.55.4. Uit het voorgaande volgt dat alleen de ' API-gegevens ', bedoeld in artikel 9, § 1, 18°, van de wet van 25 december 2016, van sommige categorieën van passagiers, onder de voorwaarden bepaald in hoofdstuk 11 van de wet van 25 december 2016, kunnen worden verwerkt in het licht van het in artikel 8, § 2, van de wet van 25 december 2016 vermelde doel, dat verband houdt met de bestrijding van de illegale immigratie en de controle aan de buitengrenzen.

Zoals is vermeld in de in B.55.2 aangehaalde parlementaire voorbereiding, past een dergelijke maatregel in het kader van de omzetting van de richtlijn 2004/82/EG, waarvan de doelstelling, zoals aangegeven in de eerste overweging ervan, erin bestaat illegale immigratie doeltreffend te bestrijden en de grenscontroles te verbeteren. Meer in het bijzonder, neemt hoofdstuk 11 van de wet van 25 december 2016, met enkele aanpassingen, de inhoud over van het koninklijk besluit van 11 december 2006 ' betreffende de verplichting voor luchtvervoerders om passagiersgegevens door te geven ', dat, vóór de opheffing ervan bij het koninklijk besluit van 18 juli 2017, de richtlijn 2004/82/EG in intern recht omzette.

B.55.5. Gelet op de verschillende, in B.55.3 vermelde beperkingen, waarmee de verwerking van de gegevens in het kader van het doel beoogd in artikel 8, § 2, gepaard gaat, is die maatregel voldoende duidelijk, nauwkeurig en tot het strikt noodzakelijke beperkt en dus niet onevenredig ».

B.53.2. Bij dat arrest heeft het Hof geoordeeld dat het doel beoogd in artikel 8, § 2, van de bestreden wet beperkt was tot het strikt noodzakelijke door te steunen op, enerzijds, het feit dat de beoogde gegevens beperkt waren tot de API–gegevens en, anderzijds, het feit dat de verwerking van die gegevens gepaard ging met de verschillende waarborgen bepaald in de artikelen 28 tot 31 van de wet van 25 december 2016.

Het Hof heeft het Hof van Justitie niet gevraagd of de PNR-richtlijn in die zin moest worden uitgelegd dat zij zich verzet tegen een nationale wetgeving zoals de bestreden wet, die, als doel van de PNR-gegevensverwerking, het doel inzake de verbetering van de controles van personen aan de buitengrenzen en meer bepaald inzake de bestrijding van illegale immigratie aanvaardt.

Het Hof heeft zich bijgevolg definitief uitgesproken over de bestaanbaarheid, met de in het eerste middel bedoelde bepalingen, van het in artikel 8, § 2, van de bestreden wet beoogde doel.

De grieven die zijn gericht tegen de artikelen 28 tot 31, in samenhang gelezen met artikel 8, § 2, van de wet van 25 december 2016, worden in het kader van het tweede middel onderzocht.

B.54.1. Op de vraag van het Hof over de uitlegging van de API–richtlijn (negende prejudiciële vraag, *sub b)*, heeft het Hof van Justitie, in het voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geoordeeld :

« 287. Uit de in het verzoek om een prejudiciële beslissing verstrekte informatie blijkt bovendien dat met de nationale wetgeving in het hoofdgeding de PNR–richtlijn, de API–richtlijn en een deel van richtlijn 2010/65 bij een en dezelfde handeling worden omgezet. Het systeem van de PNR–richtlijn wordt daarbij toegepast op alle vluchten binnen de EU en alle vervoer over het spoor, over de weg en over het water binnen de Unie van, naar en door België, alsook op reisoperatoren, en er worden ook andere doelstellingen dan enkel het bestrijden van terroristische misdrijven en ernstige criminaliteit nagestreefd. Volgens diezelfde informatie lijkt het erop dat alle gegevens die met het bij die nationale wetgeving ingevoerde systeem worden verzameld, door de PIE worden bewaard in één databank met daarin de PNR–gegevens en de in artikel 3, lid 2, van de API–richtlijn bedoelde gegevens van alle onder die wetgeving vallende passagiers.

288. Voor zover de verwijzende rechter in zijn negende vraag, onder *b)*, verwijst naar de doelstelling grenscontroles te verbeteren en illegale immigratie te bestrijden, wat de doelstelling van de API–richtlijn is, zij eraan herinnerd dat, zoals uit de punten 233, 234 en 237 van dit arrest blijkt, de lijst van doelstellingen die de PNR–richtlijn met de verwerking van PNR–gegevens nastreeft, limitatief is. Nationale wetgeving waarbij overeenkomstig deze richtlijn verzamelde PNR–gegevens kunnen worden verwerkt voor andere dan de in deze richtlijn genoemde doeleinden, zoals het verbeteren van grenscontroles en het bestrijden van illegale immigratie, is in strijd met artikel 6 van deze richtlijn, gelezen in het licht van het Handvest.

289. Zoals uit punt 235 van dit arrest blijkt, kunnen lidstaten evenmin één enkele databank oprichten met daarin én krachtens de PNR–richtlijn verzamelde PNR–gegevens voor vluchten naar of vanuit derde landen en vluchten binnen de EU én gegevens van passagiers die andere vervoersmiddelen nemen én de in artikel 3, lid 2, van de API–richtlijn bedoelde gegevens, zeker wanneer die databank kan geraadpleegd worden voor andere dan de in artikel 1, lid 2, van de PNR–richtlijn genoemde doeleinden.

290. Tot slot kunnen de artikelen 28 tot en met 31 van de wet van 25 december 2016, zoals de advocaat–generaal in punt 281 van zijn conclusie heeft aangegeven, hoe dan ook slechts verenigbaar zijn met het Unierecht en met artikel 67, lid 2, VWEU in het bijzonder indien zij zo worden uitgelegd en toegepast dat enkel API–gegevens van passagiers die de buitengrenzen van België met derde landen overschrijden, worden doorgegeven en verwerkt. Een maatregel waarmee een lidstaat, om grenscontroles te verbeteren en illegale immigratie te bestrijden, de API–richtlijn en met name de verplichting om passagiersgegevens door te geven (artikel 3, lid 1) zou uitbreiden naar vluchten binnen de EU en zelfs naar andere transportmiddelen waarmee passagiers uit, vanuit of door die lidstaat binnen de Unie reizen, zou er immers op neerkomen dat de bevoegde autoriteiten bij overschrijding van de binnengrenzen van die lidstaat systematisch kunnen nagaan of die passagiers het grondgebied mogen binnenkomen dan wel verlaten, en zou dus een gelijke werking hebben als een controle aan de buitengrenzen met derde landen.

291. Gelet op al het voorgaande dient op de negende vraag, onder *b)*, te worden geantwoord dat het Unierecht en met name artikel 2 van de PNR–richtlijn, gelezen in het licht van artikel 3, lid 2, VEU, artikel 67, lid 2, VWEU en artikel 45 van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen :

- nationale wetgeving die ter bestrijding van terroristische misdrijven en ernstige criminaliteit een systeem invoert van doorgifte door luchtvaartmaatschappijen en reisoperatoren en verwerking door de bevoegde autoriteiten van PNR–gegevens voor alle vluchten binnen de EU en andere soorten vervoer binnen de Unie vanuit, naar of door de betrokken lidstaat, indien deze lidstaat niet met een werkelijke en actuele of voorzienbare terroristische dreiging wordt geconfronteerd. In een dergelijke situatie moet het systeem van de PNR–richtlijn worden beperkt tot het doorgeven en verwerken van PNR–gegevens voor vluchten en/of transportmiddelen die met name verband houden met bepaalde verbindingen, reisroutes of luchthavens, treinstations of zeehavens waarvoor er aanwijzingen bestaan dat deze toepassing gerechtvaardigd is. De betrokken lidstaat moet dan selecteren voor welke vluchten binnen de EU en/of andere soorten vervoer binnen de Unie er dergelijke aanwijzingen bestaan, en die toepassing regelmatig herzien in het licht van wijzigingen in de omstandigheden die die selectie rechtvaardigden, om te verzekeren dat dat systeem steeds in de mate van het strikt noodzakelijke op die vluchten en/of dat vervoer wordt toegepast, en

- nationale wetgeving die een dergelijk systeem van doorgifte en verwerking van die gegevens invoert om controles aan de buitengrenzen te verbeteren en illegale immigratie te bestrijden ».

B.54.2. Uit dat arrest vloeit voort dat, enerzijds, de verwerking van de PNR-gegevens voor andere doeleinden dan die waarin de PNR-richtlijn voorziet, met name, voor het verbeteren van de grenscontroles en het bestrijden van illegale immigratie, voorbijgaat aan het exhaustieve karakter van de opsomming van de met de verwerking van de PNR-gegevens nagestreefde doeleinden (punt 288), waardoor de lidstaten wordt belet één enkele databank op te richten met daarin zowel de PNR-gegevens die krachtens de PNR-richtlijn zijn verzameld, als de gegevens bedoeld in artikel 3, lid 2, van de API–richtlijn, met name wanneer die databank kan worden geraadpleegd niet alleen voor de in artikel 1, lid 2, van de PNR-richtlijn genoemde doeleinden, maar tevens voor andere doeleinden (punt 289), en, anderzijds, de verwerking van de API–gegevens alleen betrekking kan hebben op de passagiers die de buitengrenzen van de Unie met derde landen overschrijden, daar ze anders een gelijke werking zou hebben als de controles aan de buitengrenzen met derde landen (punt 290).

B.55.1. In tegenstelling tot wat het Hof heeft geoordeeld bij zijn arrest nr. 135/2019, lijkt het arrest van het Hof van Justitie te impliceren dat het doel van de verbetering van de grenscontroles en van de bestrijding van illegale immigratie niet kan worden nagestreefd door middel van de verwerking van de PNR-gegevens, zelfs indien die laatste worden beperkt tot de API–gegevens en zelfs indien de verwerking van die gegevens gepaard gaat met de waarborgen bepaald in de artikelen 28 tot 31 van de wet van 25 december 2016, wanneer die gegevens worden verzameld in één enkele databank in de zin van de PNR-richtlijn en zij betrekking hebben op passagiers die niet de buitengrenzen van de Unie overschrijden.

B.55.2. Het arrest nr. 135/2019 van het Hof is op dat punt evenwel definitief en niet vatbaar voor beroep (artikel 116 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof). Bij dat arrest heeft het Hof ten aanzien van het vermelde punt zijn rechtsmacht uitgeput. Het Hof vermag niet terug te komen op zijn definitieve rechterlijke beslissingen, aangezien dat « door geen enkele omstandigheid kan worden verantwoord » (zie onder andere arrest nr. 172/2008 van 3 december 2008, ECLI:BE:GHCC:2008:ARR.172, B.15). Het gaat immers om « een van de essentiële beginselen van de rechtsstaat » (arrest nr. 199/2009 van 17 december 2009, ECLI:BE:GHCC:2009:ARR.199, B.8). Evenmin gebiedt het Unierecht terug te komen op een definitieve rechterlijke beslissing, zelfs niet wanneer daardoor een schending van een Unierechtelijke bepaling kan worden verholpen (HvJ, grote kamer, 6 oktober 2015, C—69/14, *Târşia*, ECLI:EU:C:2015:662, punten 28-29; 4 maart 2020, C—34/19, *Telecom Italia*, ECLI:EU:C:2020:148, punt 69). Het Hof zou het rechtspunt niet in een andere zin kunnen beslechten zonder dat het opnieuw bij het Hof aanhangig wordt gemaakt. Het staat bijgevolg aan de wetgever de bestreden wet op het betwiste punt in overeenstemming te brengen met het arrest van het Hof van Justitie.

B.56. In zoverre het is gericht tegen artikel 8, § 1, 3°, en § 2, van de wet van 25 december 2016, is het middel niet gegrond, onder voorbehoud van de in B.49 vermelde interpretatie.

In zoverre het is gericht tegen artikel 8, § 1, 4°, van de wet van 25 december 2016, is het middel gegrond. Artikel 8, § 1, 4°, van de wet van 25 december 2016 dient derhalve te worden vernietigd.

4. *Het beheer van de passagiersgegevensbank en de verwerking van de gegevens in het kader van de voorafgaande beoordeling en van de gerichte opzoekingen (artikelen* 12 *tot* 16, 24 *tot* 27, 50 *en* 51*)*

B.57. De verzoekende partij is van mening dat de verschillende verwerkingen en stromen van persoonsgegevens kennelijk onevenredig zijn.

Enerzijds bekritiseert zij de oprichting van de passagiersgegevensbank, beheerd door de PIE, binnen de FOD Binnenlandse Zaken met het oog op de uitwisseling van inlichtingen met de buitenlandse PIE's en Europol. Zij is van mening dat de verwerking van de passagiersgegevens niet de oprichting van een gegevensbank vereiste.

Anderzijds bekritiseert zij de correlatie tussen de gegevensbanken en de methode van « *pre-screening* », die zou moeten worden uitgevoerd op grond van vooraf vastgestelde criteria die dienen als indicatoren van de dreiging.

Ten slotte bekritiseert zij het feit dat de uit de bevoegde diensten gedetacheerde leden zich kunnen uitspreken over een verzoek om individuele toegang in het kader van gerichte opzoekingen.

B.58.1. Krachtens artikel 4, lid 1, van de PNR-richtlijn richt elke lidstaat een instantie op of wijst die een bestaande instantie aan die bevoegd is terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen, of wijst die een afdeling van een dergelijke instantie aan, om op te treden als zijn PIE.

Overeenkomstig artikel 4, lid 2, van de PNR-richtlijn, heeft de PIE tot taak :

« *a)* de PNR-gegevens van de luchtvaartmaatschappijen te verzamelen, op te slaan en te verwerken, en die gegevens of het resultaat van de verwerking ervan aan de in artikel 7 bedoelde bevoegde instanties door te geven;

b) zowel de PNR-gegevens als het resultaat van de verwerking ervan met de PIE's van andere lidstaten en met Europol uit te wisselen, overeenkomstig de artikelen 9 en 10 ».

B.58.2. Ten aanzien van de gegevensverwerking bepaalt artikel 6 van de PNR-richtlijn :

« 1. De door de luchtvaartmaatschappij doorgegeven PNR-gegevens worden door de PIE van de betrokken lidstaat verzameld overeenkomstig artikel 8. Indien de door de luchtvaartmaatschappij doorgegeven PNR-gegevens andere dan de in bijlage I vermelde PNR-gegevens bevatten, worden zij door de PIE onmiddellijk na ontvangst definitief gewist.

2. De PIE verwerkt de PNR-gegevens uitsluitend voor de volgende doeleinden :

a) het beoordelen van de passagiers vóór hun geplande aankomst in of gepland vertrek uit de lidstaat, om te bepalen welke personen moeten worden onderworpen aan een nader onderzoek door de in artikel 7 bedoelde bevoegde instanties, en, in voorkomend geval, door Europol overeenkomstig artikel 10, omdat zij betrokken zouden kunnen zijn bij een terroristisch misdrijf of bij ernstige criminaliteit;

b) het per geval inwilligen van een op afdoende gronden gebaseerd, gemotiveerd verzoek van de bevoegde instanties om in bepaalde gevallen PNR-gegevens te verstrekken en te verwerken voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven of ernstige criminaliteit, en de resultaten van deze verwerking aan die instanties of, in voorkomend geval, aan Europol mee te delen; en

c) het analyseren van PNR-gegevens voor het bijstellen van bestaande of het formuleren van nieuwe criteria die moeten worden gebruikt bij de beoordelingen die worden verricht op grond van lid 3, onder *b)*, om te bepalen welke personen betrokken zouden kunnen zijn bij een terroristisch misdrijf of bij ernstige criminaliteit.

3. Bij de verrichting van de in lid 2, onder *a)*, bedoelde beoordeling kan de PIE :

a) de PNR-gegevens vergelijken met databanken die relevant zijn voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, met name databanken in verband met gezochte of gesignaleerde personen of voorwerpen, in overeenstemming met de op zulke databanken van toepassing zijnde Unie–, internationale en nationale voorschriften; of

b) de PNR-gegevens verwerken overeenkomstig vooraf bepaalde criteria.

4. Het beoordelen van passagiers vóór hun geplande aankomst in of gepland vertrek uit de lidstaat op grond van lid 3, onder *b)*, volgens vooraf bepaalde criteria wordt op niet-discriminerende wijze verricht. Deze vooraf bepaalde criteria moeten doelgericht, evenredig en specifiek zijn. De lidstaten zorgen ervoor dat deze criteria door de PIE worden vastgesteld en regelmatig worden getoetst, in samenwerking met de in artikel 7 bedoelde bevoegde instanties. Deze criteria mogen onder geen beding gebaseerd zijn op ras, etnische afstamming, religieuze, levensbeschouwelijke of politieke overtuiging, vakbondslidmaatschap, gezondheid, seksleven of seksuele geaardheid van de betrokkene.

5. De lidstaten zorgen ervoor dat elke positieve overeenkomst die voortvloeit uit het automatisch verwerkingsproces van de PNR-gegevens dat wordt uitgevoerd op grond van lid 2, onder *a)*, per geval wordt gecontroleerd op een niet-geautomatiseerde wijze om te bepalen of de in artikel 7 bedoelde bevoegde instantie maatregelen moet treffen overeenkomstig het nationale recht.

6. De PNR-gegevens van de overeenkomstig lid 2, onder *a)*, aangemerkte personen of het verwerkingsresultaat van die gegevens worden door de PIE van een lidstaat voor nader onderzoek aan de in artikel 7 bedoelde bevoegde instanties van diezelfde lidstaat doorgezonden. Tot die doorgifte kan alleen per geval worden besloten en, in geval van geautomatiseerde verwerking van PNR-gegevens, na een afzonderlijke niet-geautomatiseerde controle.

7. De lidstaten zorgen ervoor dat de functionaris voor gegevensbescherming toegang heeft tot alle gegevens die door de PIE worden verwerkt. Indien de functionaris voor gegevensbescherming oordeelt dat een verwerking van gegevens niet rechtmatig was, kan hij de zaak naar de nationale toezichthoudende autoriteit verwijzen.

8. Het opslaan, verwerken en analyseren van PNR-gegevens door de PIE geschiedt uitsluitend op een beveiligde locatie of beveiligde locaties op het grondgebied van de lidstaten.

9. Het resultaat van de in lid 2, onder *a)*, van dit artikel bedoelde beoordeling laat onverlet het in Richtlijn 2004/38/EG van het Europees Parlement en de Raad neergelegde recht van personen die het Unierecht van vrij verkeer genieten, om het grondgebied van de betrokken lidstaat te betreden. Bovendien moeten de gevolgen van die beoordeling, indien verricht met betrekking tot vluchten binnen de EU tussen lidstaten waarop Verordening (EG) nr. 562/2006 van het Europees Parlement en de Raad van toepassing is, in overeenstemming zijn met die verordening ».

B.59.1. Op een vraag van het Hof over de geldigheid van de PNR-richtlijn heeft het Hof van Justitie, in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, verschillende verduidelijkingen geformuleerd in verband met de voorafgaande beoordeling van de PNR-gegevens via geautomatiseerde verwerking (punten 176-213) – rekening houdend met (i) de vergelijking van de PNR-gegevens met de databanken, *(ii)* de verwerking van de PNR-gegevens aan de hand van vooraf bepaalde criteria en *(iii)* de waarborgen voor de geautomatiseerde verwerking van de PNR-gegevens – en het achteraf verstrekken en beoordelen van de PNR-gegevens (punten 214—227) :

« 5*) Voorafgaande beoordeling van PNR-gegevens via geautomatiseerde verwerking*

176. Volgens artikel 6, lid 2, onder *a)*, van de PNR-richtlijn strekt de daarin opgelegde voorafgaande beoordeling ertoe te bepalen welke personen nader moeten worden onderzocht door met name de in artikel 7 van deze richtlijn bedoelde bevoegde instanties, wegens hun mogelijke betrokkenheid bij een terroristisch misdrijf of bij ernstige criminaliteit.

177. De voorafgaande beoordeling verloopt in twee fasen. Eerst verwerkt de PIE van de betrokken lidstaat de PNR-gegevens op automatische wijze door ze te vergelijken met databanken of te verwerken aan de hand van vooraf bepaalde criteria (artikel 6, lid 3, van de PNR-richtlijn). Indien de geautomatiseerde verwerking een positieve overeenkomst *(hit)* oplevert, voert de PIE vervolgens op niet-geautomatiseerde wijze een controle uit om te bepalen of de in artikel 7 van deze richtlijn bedoelde bevoegde instanties maatregelen moeten treffen overeenkomstig het nationale recht (artikel 6, lid 5) *(match)*.

178. Zoals in punt 106 van dit arrest in herinnering is gebracht, hebben geautomatiseerde verwerkingen noodzakelijkerwijs een vrij grote foutenmarge, aangezien zij verricht worden met niet-geverifieerde persoonsgegevens en steunen op vooraf bepaalde criteria.

179. In die omstandigheden en gelet op de noodzaak om, zoals in de vierde overweging van de preambule van het Handvest wordt benadrukt, de bescherming van de grondrechten te versterken in het licht van onder meer de wetenschappelijke en technologische ontwikkelingen, moet er overeenkomstig overweging 20 en artikel 7, lid 6, van de PNR–richtlijn voor worden gezorgd dat de bevoegde instanties niet uitsluitend op grond van automatisch verwerkte PNR-gegevens een besluit nemen dat voor de betrokkene nadelige juridische of andere ingrijpende gevolgen heeft. Artikel 6, lid 6, van deze richtlijn bepaalt ook dat de PIE de PNR-gegevens pas aan die instanties mag doorgeven na een afzonderlijke niet-geautomatiseerde controle. Naast deze controles die de PIE en de bevoegde instanties zelf verrichten, moet de rechtmatigheid van elke geautomatiseerde verwerking ten slotte kunnen worden gecontroleerd door de functionaris voor gegevensbescherming en de nationale toezichthoudende autoriteit artikel 6, lid 7, respectievelijk artikel 15, lid 3, onder *b)*, van deze richtlijn alsook door de nationale rechterlijke instanties in het kader van de rechtsmiddelen als bedoeld in artikel 13, lid 1, ervan.

180. Zoals de advocaat-generaal in punt 207 van zijn conclusie in wezen heeft opgemerkt, moeten aan de nationale toezichthoudende autoriteit, de functionaris voor gegevensbescherming en de PIE de nodige materiële en personele middelen ter beschikking worden gesteld om het hun door de PNR-richtlijn opgedragen toezicht uit te oefenen. Ook is het van belang dat de nationale regeling waarbij deze richtlijn in nationaal recht wordt omgezet en waarbij toestemming wordt verleend voor de daarin voorgeschreven geautomatiseerde verwerking, duidelijke en nauwkeurige regels bevat voor de aanduiding van de databanken en de te hanteren beoordelingscriteria, en dat bij de voorafgaande beoordeling geen andere methoden kunnen worden gebruikt dan die welke uitdrukkelijk worden genoemd in artikel 6, lid 2, van die richtlijn.

181. Voorts blijkt uit artikel 6, lid 9, van de PNR-richtlijn dat het resultaat van de op grond van artikel 6, lid 2, onder *a)*, ervan verrichte voorafgaande beoordeling niet afdoet aan het in richtlijn 2004/38 neergelegde recht van personen die het recht van vrij verkeer genieten, om het grondgebied van de betrokken lidstaat te betreden, en bovendien in overeenstemming moet zijn met verordening nr. 562/2006. Het bij de PNR-richtlijn ingevoerde systeem staat de bevoegde autoriteiten dus niet toe dit recht verder te beperken dan in richtlijn 2004/38 en verordening nr. 562/2006 is bepaald.

i) Vergelijking van PNR-gegevens met databanken

182. Volgens artikel 6, lid 3, onder *a)*, van de PNR-richtlijn ‘ kan ’ de PIE tijdens de in artikel 6, lid 2, onder *a)*, bedoelde beoordeling de PNR-gegevens vergelijken met ‘ databanken die relevant zijn ’ voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, ‘ met name databanken in verband met gezochte of gesignaleerde personen of voorwerpen, in overeenstemming met de op zulke databanken van toepassing zijnde Unie-, internationale en nationale voorschriften ’.

183. Uit de tekst van artikel 6, lid 3, onder *a)*, van de PNR-richtlijn en meer bepaald de woorden ‘ met name ’ blijkt meteen dat databanken voor gezochte of gesignaleerde personen of voorwerpen relevante databanken zijn in de zin van deze bepaling. Verder wordt evenwel niet aangegeven welke andere databanken er nog ‘ relevant ’ zouden kunnen zijn met het oog op de doelstellingen van deze richtlijn. Zoals de advocaat-generaal in punt 217 van zijn conclusie heeft opgemerkt, wordt de aard van de gegevens die deze databanken kunnen bevatten en hun verband met die doelstellingen niet in die bepaling gepreciseerd, en wordt daarin evenmin gezegd of PNR-gegevens enkel mogen worden vergeleken met door overheidsinstanties beheerde databanken of ook met databanken die door particulieren worden beheerd.

184. Artikel 6, lid 3, onder *a)*, van de PNR-richtlijn zou dan ook op het eerste gezicht zo kunnen worden uitgelegd dat PNR-gegevens eenvoudigweg als zoekcriteria kunnen worden gebruikt en bij de beoordeling kunnen worden ingegeven in diverse databanken, ook databanken die de veiligheids– en inlichtingendiensten van lidstaten beheren en gebruiken voor andere dan de in deze richtlijn genoemde doelstellingen, en dat een dergelijke beoordeling een informatievergaring kan worden (*data mining*). De gedachte dat beoordelingen op deze manier verlopen en dat PNR-gegevens kunnen worden vergeleken met dergelijke databanken, zou luchtreizigers echter het gevoel kunnen geven dat hun privéleven onder toezicht staat. Artikel 6, lid 3, onder *a)*, van de PNR-richtlijn kan dus niet op deze manier worden uitgelegd, ook al vertrekt de in deze bepaling bedoelde voorafgaande beoordeling vanuit een relatief beperkt aantal gegevens — de PNR-gegevens. Deze uitlegging zou immers in een overmatig gebruik van deze gegevens kunnen resulteren en de mogelijkheid laten om een precies profiel op te stellen van eenieder die gewoon de intentie heeft een vliegtuig te nemen.

185. Artikel 6, lid 3, onder *a)*, van de PNR-richtlijn moet dan ook overeenkomstig de in de punten 86 en 87 van dit arrest aangehaalde rechtspraak zo worden uitgelegd dat de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten volledig worden geëerbiedigd.

186. Dienaangaande blijkt uit de overwegingen 7 en 15 van de PNR-richtlijn dat de geautomatiseerde verwerking in de zin van artikel 6, lid 3, onder *a)*, van deze richtlijn beperkt moet zijn tot wat strikt noodzakelijk is om terroristische misdrijven en ernstige criminaliteit te bestrijden, en dat een hoog niveau van bescherming van de voormelde grondrechten moet worden verzekerd.

187. Zoals de Commissie in wezen heeft aangegeven in antwoord op een vraag van het Hof, bieden de bewoordingen van deze bepaling — namelijk dat de PIE de PNR-gegevens ‘ kan ’ vergelijken met de daarin bedoelde databanken — de PIE bovendien de mogelijkheid om een verwerkingsmethode te kiezen die beperkt is tot wat in de concrete situatie strikt noodzakelijk is. Aangezien moet worden voldaan aan de vereisten van duidelijkheid en nauwkeurigheid om de bescherming van de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten te verzekeren, is de PIE verplicht om de geautomatiseerde verwerking van artikel 6, lid 3, onder *a)*, van de PNR-richtlijn te beperken tot databanken die op basis van deze bepaling kunnen worden aangewezen. In dit verband moet worden vastgesteld dat de verwijzing in deze bepaling naar ’ databanken die relevant zijn ’ moeilijk valt uit te leggen op een wijze waarbij voldoende duidelijk en nauwkeurig blijkt welke databanken daarmee bedoeld worden. Dit ligt evenwel anders voor de verwijzing naar ’ databanken in verband met gezochte of gesignaleerde personen of voorwerpen, in overeenstemming met de op zulke databanken van toepassing zijnde Unie–, internationale en nationale voorschriften ’.

188. Bijgevolg moet artikel 6, lid 3, onder *a)*, van de PNR-richtlijn in het licht van die grondrechten aldus worden uitgelegd dat laatstgenoemde databanken de enige databanken zijn waarmee de PIE de PNR-gegevens mag vergelijken, zoals ook de advocaat-generaal in punt 219 van zijn conclusie in essentie heeft aangegeven.

189. In termen van vereisten waaraan deze databanken moeten voldoen, zij opgemerkt dat artikel 6, lid 4, van de PNR-richtlijn bepaalt dat een voorafgaande beoordeling aan de hand van vooraf bepaalde criteria artikel 6, lid 3, onder *b)*, van deze richtlijn op niet-discriminerende wijzen moet gebeuren, dat deze criteria doelgericht, evenredig en specifiek moeten zijn en dat de PIE deze criteria moet vaststellen en regelmatig moet toetsen in samenwerking met de in artikel 7 van deze richtlijn bedoelde bevoegde instanties. Artikel 6, lid 4, spreekt, gelet op de verwijzing daarin naar artikel 6, lid 3, onder *b)*, enkel over het verwerken van PNR-gegevens aan de hand van vooraf bepaalde criteria, doch moet in het licht van de artikelen 7, 8 en 21 van het Handvest in die zin worden uitgelegd dat de daarin gestelde vereisten *mutatis mutandis* gelden voor het vergelijken van PNR-gegevens met de in het vorige punt van dit arrest bedoelde databanken, te meer daar deze vereisten in wezen overeenkomen met die welke voor het vergelijken van PNR–gegevens met databanken zijn aangenomen in de rechtspraak die voortvloeit uit advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017 (EU:C:2017:592, punt 172).

190. In dit verband moet worden verduidelijkt dat het vereiste dat die databanken niet-discriminatoir zijn met name impliceert dat de opname in de databanken voor gezochte of gesignaleerde personen gebaseerd moet zijn op objectieve en niet-discriminerende elementen die zijn vastgesteld bij de op zulke databanken van toepassing zijnde Unie–, internationale en nationale voorschriften (zie naar analogie arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 78).

191. Bovendien moeten de in punt 188 van het onderhavige arrest bedoelde databanken, om te voldoen aan het vereiste dat vooraf bepaalde criteria doelgericht, evenredig en specifiek zijn, worden gebruikt om terroristische misdrijven en ernstige vormen van criminaliteit te bestrijden die minstens indirect verband houden met het luchtvervoer van passagiers.

192. Voorts moeten de databanken die krachtens artikel 6, lid 3, onder *a)*, van de PNR–richtlijn worden ingezet, gelet op de overwegingen in de punten 183 en 184 van het onderhavige arrest, worden beheerd door de in artikel 7 van deze richtlijn bedoelde bevoegde instanties of, in geval van Uniedatabanken of internationale databanken, worden gebruikt in het kader van hun taak terroristische misdrijven en ernstige criminaliteit te bestrijden. Dit is het geval voor databanken in verband met gezochte of gesignaleerde personen of voorwerpen, in overeenstemming met de op zulke databanken toepasselijke Unie-, internationale en nationale voorschriften.

ii) Verwerking van PNR-gegevens aan de hand van vooraf bepaalde criteria

193. Volgens artikel 6, lid 3, onder *b)*, van de PNR-richtlijn kan de PIE de PNR-gegevens ook verwerken aan de hand van vooraf bepaalde criteria. Blijkens artikel 6, lid 2, onder *a)*, van deze richtlijn strekt het voorafgaandelijk beoordelen en dus het verwerken van PNR-gegevens met vooraf bepaalde criteria er in hoofdzaak toe personen te identificeren die betrokken zouden kunnen zijn bij een terroristisch misdrijf of bij ernstige criminaliteit.

194. Wat betreft de criteria die de PIE hiervoor kan gebruiken, zij er om te beginnen op gewezen dat de bewoordingen zelf van artikel 6, lid 3, onder *b)*, van de PNR-richtlijn aangeven dat het om ‘ vooraf bepaalde ’ criteria moet gaan. Zoals de advocaat-generaal in punt 228 van zijn conclusie heeft opgemerkt, betekent dit dat geen kunstmatige-intelligentietechnologieën zoals machinaal leren (*machine learning*) mogen worden gebruikt, aangezien die zonder menselijke tussenkomst of controle aanpassingen kunnen doorvoeren in het beoordelingsproces en met name in de beoordelingscriteria waarop de resultaten gebaseerd zijn, en in de weging van deze criteria.

195. Dergelijke technologieën dreigen trouwens de afzonderlijke controle van de positieve overeenstemmingen en de rechtmatigheidscontrole die door de PNR-richtlijn worden vereist, hun nuttig effect te ontnemen. Zoals de advocaat-generaal in punt 228 van zijn conclusie in wezen heeft opgemerkt, kan de opaciteit van de werking van kunstmatige-intelligentietechnologieën het immers onmogelijk maken te begrijpen waarom een bepaald programma een positieve overeenstemming heeft opgeleverd. Bijgevolg zouden deze technologieën de betrokkenen ook het hun door artikel 47 van het Handvest gewaarborgd recht op een doeltreffende voorziening in rechte kunnen ontnemen, dat de PNR-richtlijn volgens overweging 28 ervan op hoog niveau wil waarborgen, en dat zij met name zouden kunnen aanwenden wanneer zij de verkregen resultaten discriminerend achten.

196. Wat vervolgens de vereisten in artikel 6, lid 4, van de PNR-richtlijn betreft, luidt de eerste volzin dat de voorafgaande beoordeling volgens vooraf bepaalde criteria op niet-discriminerende wijze dient te gebeuren, en verduidelijkt de vierde volzin dat deze criteria onder geen beding mogen gebaseerd zijn op ras, etnische afstamming, religieuze, levensbeschouwelijke of politieke overtuiging, vakbondslidmaatschap, gezondheid, seksleven of seksuele geaardheid.

197. De lidstaten mogen als vooraf bepaalde criteria dus geen criteria nemen die steunen op de in het vorige punt van dit arrest genoemde kenmerken, waarvan het gebruik kan resulteren in discriminatie. In dit verband blijkt uit de bewoordingen van artikel 6, lid 4, vierde volzin, van de PNR-richtlijn — namelijk dat de vooraf bepaalde criteria ‘ onder geen beding ’ op deze kenmerken mogen gebaseerd zijn — dat zowel directe als indirecte discriminatie wordt bedoeld. Deze uitlegging vindt steun in artikel 21, lid 1, van het Handvest, in het licht waarvan die bepaling moet worden gelezen en dat bepaalt dat „iedere” discriminatie op grond van deze kenmerken verboden is. Bijgevolg moeten vooraf bepaalde criteria zo worden gekozen dat zij, zelfs indien zij neutraal zijn geformuleerd, in de praktijk niet in het bijzonder nadelig kunnen zijn voor personen met de beschermde kenmerken.

198. Uit de vereisten van doelgerichtheid, evenredigheid en specificiteit van de vooraf bepaalde criteria die zijn vervat in artikel 6, lid 4, tweede volzin, van de PNR-richtlijn, volgt dat de criteria voor de voorafgaande beoordeling zodanig moeten worden gekozen dat zij specifiek gericht zijn op personen van wie redelijkerwijs kan worden vermoed dat zij betrokken zijn bij terroristische misdrijven of ernstige criminaliteit als bedoeld in deze richtlijn. Deze lezing vindt steun in de bewoordingen van artikel 6, lid 2, onder *a)*, ervan, die de nadruk leggen op het feit betrokken te ‘ kunnen ’ zijn bij ‘ een ’ terroristisch misdrijf of bij ernstige criminaliteit. In dezelfde geest wordt in overweging 7 van deze richtlijn gepreciseerd dat beoordelingscriteria enkel mogen worden vastgesteld en toegepast voor terroristische misdrijven en ernstige criminaliteit ‘ waarvoor het gebruik van dergelijke criteria relevant is ’.

199. Gezien het gevaar voor discriminatie dat uitgaat van criteria die steunen op de in artikel 6, lid 4, vierde volzin, van de PNR-richtlijn genoemde kenmerken, mogen de PIE en de bevoegde autoriteiten zich bij het uitfilteren van die personen dus in principe niet op deze kenmerken baseren. Zoals de Duitse regering ter terechtzitting heeft aangegeven, mogen zij daarentegen wel onder meer rekening houden met bijzonderheden in de manier waarop personen zich feitelijk gedragen bij het voorbereiden en maken van vliegtuigreizen, omdat uit de vaststellingen en de ervaring van de bevoegde autoriteiten zou kunnen blijken dat personen die zich op een bepaalde manier gedragen betrokken kunnen zijn bij terroristische misdrijven of ernstige criminaliteit.

200. Zoals de Commissie in deze context heeft aangegeven in antwoord op een vraag van het Hof moeten vooraf bepaalde criteria zodanig worden gekozen dat zowel ‘ belastende ’ als ‘ ontlastende ’ elementen in aanmerking worden genomen. Dit vereiste kan de criteria betrouwbaarder maken en kan met name verzekeren dat zij evenredig zijn in de zin van artikel 6, lid 4, tweede volzin, van de PNR-richtlijn.

201. Tot slot moeten vooraf bepaalde criteria volgens artikel 6, lid 4, derde volzin, van deze richtlijn regelmatig worden getoetst. Ze moeten worden aangepast indien de omstandigheden die de initiële selectie ervan voor de voorafgaande beoordeling rechtvaardigden, wijzigen, zodat met name kan worden ingespeeld op veranderingen in de strijd tegen de in punt 157 van het onderhavige arrest bedoelde terroristische misdrijven en ernstige criminaliteit [zie naar analogie arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 82]. Bij die toetsing moet vooral rekening worden gehouden met de ervaring die bij het toepassen van de vooraf bepaalde criteria is opgedaan, om het aantal ‘ vals-positieve ’ resultaten zo veel mogelijk te beperken en er zo voor te zorgen dat de toepassing van deze criteria strikt noodzakelijk is.

iii) Waarborgen voor de geautomatiseerde verwerking van PNR-gegevens

202. De vereisten die artikel 6, lid 4, van de PNR-richtlijn stelt aan het geautomatiseerd verwerken van PNR-gegevens gelden niet slechts bij het aanwijzen en het toetsen van de databanken en de in deze bepaling bedoelde vooraf bepaalde criteria maar, zoals de advocaat-generaal in punt 230 van zijn conclusie heeft opgemerkt, gedurende het gehele verwerkingsproces van de gegevens.

203. Wat meer in het bijzonder de vooraf bepaalde criteria betreft, moet om te beginnen worden verduidelijkt dat de PIE volgens overweging 7 van de PNR-richtlijn de beoordelingscriteria weliswaar zo moet kiezen dat het door deze richtlijn ingestelde systeem zo weinig mogelijk onschuldige personen aanwijst, maar volgens artikel 6, leden 5 en 6, ervan toch elke positieve overeenkomst afzonderlijk op niet-geautomatiseerde wijze moet controleren om zo veel mogelijk ‘ vals-positieve ’ resultaten te vermijden. Ook neemt het feit dat de PIE de beoordelingscriteria op niet-discriminerende wijze moet vaststellen niet weg dat zij een dergelijke controle moet uitvoeren om eventuele discriminerende resultaten uit te sluiten. Dezelfde controleverplichting geldt wanneer zij PNR-gegevens met databanken vergelijkt.

204. Zo mag de PIE de resultaten van deze geautomatiseerde verwerkingen, gelet op hetgeen is overwogen in punt 198 van dit arrest, niet doorgeven aan de in artikel 7 van de PNR–richtlijn bedoelde bevoegde instanties wanneer die controle niet rechtens genoegzaam een redelijk vermoeden kan vestigen dat de via de geautomatiseerde verwerking geïdentificeerde personen betrokken zijn bij terroristische misdrijven of ernstige criminaliteit, of wanneer er aanwijzingen zijn dat die verwerkingen discriminerende resultaten geven.

205. In termen van verificaties die de PIE daartoe moet uitvoeren, volgt uit artikel 6, leden 5 en 6, *juncto* de overwegingen 20 en 22 van de PNR-richtlijn dat de lidstaten duidelijke en nauwkeurige richtsnoeren moeten vaststellen voor de personeelsleden die met de afzonderlijke controle zijn belast, om een volledige eerbiediging van de grondrechten van de artikelen 7, 8 en 21 van het Handvest te garanderen en, in het bijzonder, een coherente administratieve praktijk binnen de PIE die het non-discriminatiebeginsel eerbiedigt.

206. Gelet op het vrij groot aantal ' vals-positieve ' resultaten, waarover in punt 106 van dit arrest wordt gesproken, moeten de lidstaten erop toezien dat de PIE duidelijk en nauwkeurig objectieve controlecriteria vastlegt waarmee haar personeelsleden kunnen nagaan of en in hoeverre een positieve overeenkomst *(hit)* daadwerkelijk iemand betreft die mogelijk betrokken is bij de in punt 157 van dit arrest bedoelde terroristische misdrijven of ernstige criminaliteit en naar wie de bevoegde instanties als bedoeld in artikel 7 van die richtlijn bijgevolg nader onderzoek moeten verrichten, en of de automatische verwerkingen die op grond van die richtlijn worden uitgevoerd en met name de vooraf bepaalde criteria en de gehanteerde databanken niet-discriminerend zijn.

207. In deze context dienen de lidstaten ervoor te zorgen dat de PIE overeenkomstig artikel 13, lid 5, *juncto* overweging 37 van de PNR-richtlijn elke verwerking documenteert die tijdens de voorafgaande beoordeling, inclusief de afzonderlijke niet-geautomatiseerde controle, wordt verricht, zodat de rechtmatigheid ervan kan worden gecontroleerd en interne controle kan worden uitgeoefend.

208. Voorts mogen de bevoegde instanties volgens artikel 7, lid 6, eerste volzin, van de PNR-richtlijn niet uitsluitend op grond van automatisch verwerkte PNR-gegevens besluiten nemen die voor de betrokkenen nadelige juridische of andere ingrijpende gevolgen hebben, wat in het kader van de voorafgaande beoordeling impliceert dat zij rekening moeten houden met het resultaat van de afzonderlijke niet-geautomatiseerde controle van de PIE en in voorkomend geval dit resultaat moeten laten primeren op dat van de geautomatiseerde verwerking. Volgens de tweede volzin van artikel 7, lid 6, moeten dergelijke besluiten niet-discriminerend zijn.

209. De bevoegde instanties moeten zich daarbij vergewissen van de rechtmatigheid van zowel de geautomatiseerde verwerking — met name van het niet-discriminerende karakter ervan — als de afzonderlijke controle.

210. Zij moeten er inzonderheid op toezien dat de belanghebbende — zonder dat hij tijdens de administratieve procedure per se kennis moet kunnen hebben van de vooraf bepaalde beoordelingscriteria en van de programma's die met deze criteria werken — kan begrijpen hoe deze criteria en programma's functioneren, zodat hij met volledige kennis van zaken kan beslissen of hij al dan niet zijn door artikel 13, lid 1, van de PNR-richtlijn gewaarborgd recht op het aanwenden van rechtsmiddelen wenst uit te oefenen om in voorkomend geval het onrechtmatige en met name discriminerende karakter van die criteria aan te vechten (zie naar analogie arrest van 24 november 2020, Minister van Buitenlandse Zaken, C-225/19 en C—226/19, EU:C:2020:951, punt 43 en aldaar aangehaalde rechtspraak). Hetzelfde dient te gelden voor de controlecriteria als bedoeld in punt 206 van het onderhavige arrest.

211. Bij een krachtens artikel 13, lid 1, van de PNR-richtlijn ingesteld beroep moeten, ten slotte, de rechter die belast is met de wettigheidscontrole van de door de bevoegde instanties genomen beslissing en, behalve bij bedreigingen voor de staatsveiligheid, de betrokkene zelf kennis kunnen nemen van alle motieven en van de bewijzen op basis waarvan die beslissing is genomen (zie naar analogie arrest van 4 juni 2013, ZZ, C-300/11, EU:C:2013:363, punten 54-59), inclusief de vooraf bepaalde beoordelingscriteria en de werking van de programma's die deze criteria gebruiken.

212. Voorts moeten de functionaris voor gegevensbescherming en de nationale toezichthoudende autoriteit er overeenkomstig artikel 6, lid 7, respectievelijk artikel 15, lid 3, onder *b)*, van de PNR-richtlijn op toezien dat de door de PIE tijdens de voorafgaande beoordeling uitgevoerde geautomatiseerde verwerkingen rechtmatig en met name niet-discriminerend zijn. Waar de functionaris voor gegevensbescherming volgens die eerste bepaling toegang heeft tot de gegevens die de PIE heeft verwerkt, strekt deze toegang zich noodzakelijkerwijs ook uit tot de vooraf bepaalde criteria en de databanken die de PIE heeft gebruikt, zodat hij efficiëntie en een hoog niveau van gegevensbescherming kan waarborgen, zoals overweging 37 van deze richtlijn vereist. Ook de onderzoeken, inspecties en controles die de nationale toezichthoudende autoriteit krachtens die tweede bepaling uitvoert, kunnen betrekking hebben op die vooraf bepaalde criteria en databanken.

213. Uit alle voorgaande overwegingen volgt dat aan de bepalingen van de PNR-richtlijn die de in artikel 6, lid 2, onder *a)*, van deze richtlijn bedoelde voorafgaande beoordeling regelen, een uitlegging kan worden gegeven die in overeenstemming is met de artikelen 7, 8 en 21 van het Handvest, waarbij de grenzen van het strikt noodzakelijke worden gerespecteerd.

6*) Achteraf verstrekken en beoordelen van PNR-gegevens*

214. Volgens artikel 6, lid 2, onder *b)*, van de PNR-richtlijn kunnen PNR-gegevens ook, op verzoek van de bevoegde instanties, worden verstrekt en beoordeeld ná de geplande aankomst in of het geplande vertrek uit de lidstaat.

215. Wat de voorwaarden voor een dergelijke verstrekking en beoordeling betreft, blijkt uit de tekst van deze bepaling dat de PIE ' per geval ' een ' op afdoende gronden gebaseerd, gemotiveerd verzoek ' van de bevoegde instanties kan inwilligen om ' in bepaalde gevallen ' PNR-gegevens te verstrekken en te verwerken ' voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven of ernstige criminaliteit '. Voor het geval dat het verzoek wordt ingediend meer dan zes maanden nadat de PIE de PNR-gegevens heeft ontvangen — na welke termijn de PNR-gegevens overeenkomstig artikel 12, lid 2, van deze richtlijn worden gedepersonaliseerd doordat bepaalde gegevenselementen ervan worden afgeschermd — bepaalt artikel 12, lid 3, van deze richtlijn dat de volledige PNR-gegevens — dus inclusief de niet-gedepersonaliseerde versie ervan — uitsluitend mogen worden meegedeeld op de dubbele voorwaarde dat redelijkerwijs kan worden aangenomen dat dit noodzakelijk is voor de in artikel 6, lid 2, onder *b)*, van deze richtlijn genoemde doeleinden en wordt goedgekeurd door een gerechtelijke instantie of een andere volgens het nationale recht bevoegde nationale instantie.

216. In dit verband blijkt reeds uit de tekst van artikel 6, lid 2, onder *b)*, van de PNR–richtlijn dat de PIE niet systematisch de PNR-gegevens van alle luchtreizigers achteraf kan verstrekken en beoordelen, maar louter ' per geval ' ' in bepaalde gevallen ' verzoeken daartoe kan inwilligen. Toch is het niet omdat van ' bepaalde gevallen ' wordt gesproken dat noodzakelijkerwijs slechts PNR-gegevens van één vliegtuigpassagier mogen worden verwerkt. Zoals de Commissie in antwoord op een vraag van het Hof heeft aangegeven, kan het ook om meerdere personen gaan mits zij een bepaald aantal kenmerken gemeen hebben waardoor zij samen kunnen worden geacht een ' bepaald geval ' te vormen voor de gevraagde mededeling en beoordeling.

217. Wat vervolgens de materiële voorwaarden betreft om PNR-gegevens van luchtreizigers achteraf te verstrekken en beoordelen, wordt in artikel 6, lid 2, onder *b)*, en artikel 12, lid 3, onder *a)*, van de PNR-richtlijn gesproken van ' afdoende gronden ' respectievelijk ' redelijkerwijze ', maar wordt niet gepreciseerd om wat soort gronden het moet gaan. Niettemin blijkt uit de tekst van eerstgenoemde bepaling, die verwijst naar de doeleinden in artikel 1, lid 2, van deze richtlijn, dat PNR-gegevens alleen achteraf mogen worden verstrekt en beoordeeld om na te gaan of er aanwijzingen zijn dat personen mogelijkerwijs betrokken zijn bij terroristische misdrijven of ernstige vormen van criminaliteit die, zoals uit punt 157 van dit arrest blijkt, op zijn minst indirect objectief verband houden met het luchtvervoer van passagiers.

218. Volgens het door de PNR-richtlijn ingestelde systeem zijn de PNR-gegevens die krachtens artikel 6, lid 2, onder *b)*, van deze richtlijn worden verstrekt en verwerkt, gegevens van personen die reeds vóór hun geplande aankomst in of gepland vertrek uit de betrokken lidstaat zijn beoordeeld. Een verzoek om een beoordeling achteraf kan trouwens met name betrekking hebben op personen wier PNR-gegevens na de voorafgaande beoordeling niet aan de bevoegde autoriteiten werden doorgegeven, omdat er toen geen aanwijzingen waren dat zij betrokken konden zijn bij terroristische misdrijven of ernstige vormen van criminaliteit die op zijn minst indirect objectief verband hielden met het luchtvervoer van passagiers. Derhalve moet het verstrekken en verwerken van die gegevens voor een beoordeling achteraf gebaseerd zijn op nieuwe omstandigheden die dit gebruik rechtvaardigen [zie in die zin advies 1/15 (PNR–Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 200 en aldaar aangehaalde rechtspraak].

219. In termen van het soort omstandigheden dat kan rechtvaardigen dat PNR-gegevens achteraf worden verstrekt en verwerkt om te worden beoordeeld, is het vaste rechtspraak dat een algemene toegang tot alle bewaarde gegevens los van enig — zelfs ook maar indirect — verband met het nagestreefde doel niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, zodat de betrokken regeling, of dit nu de Unieregeling dan wel een nationale regeling ter omzetting daarvan is, aan de hand van objectieve criteria moet bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde instanties toegang tot de betrokken gegevens moet worden verleend. In dit verband kan in beginsel voor het doel van bestrijding van criminaliteit slechts toegang worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig strafbaar feit te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk strafbaar feit. In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, kan echter ook toegang tot de gegevens van andere personen worden verleend, wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren [arresten van 2 maart 2021, Prokuratuur (Voorwaarden voor toegang tot elektronische-communicatiegegevens), C-746/18, EU:C:2021:152, punt 50 en aldaar aangehaalde rechtspraak, en 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 105].

220. De termen ' afdoende gronden ' en ' redelijkerwijze ' in artikel 6, lid 2, onder *b)*, respectievelijk artikel 12, lid 3, onder *a)*, van de PNR-richtlijn moeten dan ook in het licht van de artikelen 7 en 8 van het Handvest in die zin worden uitgelegd dat zij verwijzen naar objectieve elementen die redelijkerwijs het vermoeden kunnen wekken dat iemand op een of andere manier betrokken is bij ernstige criminaliteit die minstens indirect een objectief verband vertoont met het luchtvervoer van passagiers. Voor terroristische misdrijven met een dergelijk verband is aan deze voorwaarde voldaan wanneer op grond van objectieve elementen kan worden geoordeeld dat de PNR-gegevens in een concreet geval een daadwerkelijke bijdrage tot de bestrijding van die misdrijven zouden kunnen leveren.

221. Wat tot slot de procedurele voorwaarden betreft voor het achteraf verstrekken en verwerken van PNR-gegevens voor een beoordeling, is het zo dat ingeval het verzoek wordt ingediend meer dan zes maanden nadat de gegevens aan de PIE zijn doorgegeven — en deze dus overeenkomstig artikel 12, lid 2, van de PNR-richtlijn reeds zijn gedepersonaliseerd door afscherming van de in dit lid genoemde elementen – artikel 12, lid 3, onder *b)*, van deze richtlijn vereist dat een mededeling van de volledige PNR-gegevens — dat wil zeggen inclusief een niet-gedepersonaliseerde versie ervan — wordt goedgekeurd door een gerechtelijke instantie of een andere nationale instantie die volgens het nationale recht bevoegd is. Deze instanties dienen daarbij na te gaan of het verzoek gegrond is en meer bepaald of de ter ondersteuning van dit verzoek aangevoerde elementen kunnen aantonen dat voldaan is aan de in het vorige punt van dit arrest genoemde materiële voorwaarde dat er ' afdoende gronden ' bestaan.

222. Artikel 6, lid 2, onder *b)*, van de PNR-richtlijn stelt deze procedurele voorwaarde niet uitdrukkelijk voor het geval dat een verzoek om PNR-gegevens achteraf mee te delen en te beoordelen wordt ingediend vóórdat de termijn van zes maanden na doorgifte ervan verstrijkt. Toch moet bij de uitlegging van deze bepaling rekening worden gehouden met overweging 25 van deze richtlijn, waaruit blijkt dat de Uniewetgever met die procedurele voorwaarde „het hoogste niveau van gegevensbescherming" heeft willen verzekeren bij toegang tot PNR-gegevens in een vorm waarmee de betrokkene rechtstreeks kan worden geïdentificeerd. Elk verzoek om mededeling en beoordeling achteraf impliceert een dergelijke toegang, ongeacht of het verzoek vóór dan wel ná het verstrijken van de periode van zes maanden na doorgifte van de PNR–gegevens aan de PIE wordt ingediend.

223. Om in de praktijk te garanderen dat de grondrechten en met name de voorwaarden in de punten 218 en 219 van dit arrest volledig worden geëerbiedigd in het door de PNR-richtlijn ingestelde systeem, is het van essentieel belang dat het achteraf ter beoordeling meedelen van PNR-gegevens in beginsel — behalve in naar behoren gerechtvaardigde dringende gevallen — wordt onderworpen aan een voorafgaande controle door hetzij een rechterlijke instantie, hetzij een onafhankelijke bestuurlijke entiteit, en dat de beslissing van deze rechterlijke instantie of deze entiteit wordt gegeven naar aanleiding van een gemotiveerd verzoek dat de bevoegde autoriteiten met name in het kader van een procedure ter voorkoming, opsporing of vervolging van strafbare feiten hebben ingediend. In naar behoren gemotiveerde urgente gevallen dient die controle op korte termijn plaats te vinden [zie naar analogie advies 1/15 (PNR–Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 202 en aldaar aangehaalde rechtspraak, en arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 110].

224. Derhalve moet het vereiste van een voorafgaande controle waarin artikel 12, lid 3, onder *b)*, van de PNR-richtlijn voorziet voor verzoeken om mededeling van PNR-gegevens ná het verstrijken van de termijn van zes maanden na doorgifte ervan aan de PIE, *mutatis mutandis* ook gelden voor het geval waarin dat verzoek vóór het verstrijken van deze termijn wordt gedaan.

225. Artikel 12, lid 3, onder *b)*, van de PNR-richtlijn preciseert niet uitdrukkelijk aan welke vereisten de met de voorafgaande toetsing belaste instantie moet voldoen. Het is evenwel vaste rechtspraak dat die instantie, om te verzekeren dat de uit de toegang tot de persoonsgegevens voortvloeiende inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten beperkt blijft tot het strikt noodzakelijke, over alle bevoegdheden moet beschikken en alle noodzakelijke waarborgen moet bieden om ervoor te zorgen dat de verschillende betrokken belangen en rechten met elkaar in overeenstemming worden gebracht. In het specifieke geval van een strafrechtelijk onderzoek vereist een dergelijke toetsing dat die instantie in staat is een juist evenwicht te verzekeren tussen, enerzijds, de legitieme belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft (arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 107 en aldaar aangehaalde rechtspraak).

226. Daartoe moet die instantie een zodanige status hebben dat zij bij de uitoefening van haar taken objectief en onpartijdig kan handelen, en moet zij vrij zijn van elke invloed van buitenaf. Dit vereiste van onafhankelijkheid impliceert dat zij de hoedanigheid van derde moet hebben ten opzichte van de instantie die om toegang tot de gegevens verzoekt, zodat zij de toetsing zonder beïnvloeding van buitenaf kan verrichten. In het bijzonder impliceert het vereiste van onafhankelijkheid op strafrechtelijk gebied dat die instantie enerzijds niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en anderzijds neutraal moet zijn ten opzichte van de partijen in de strafprocedure (zie in die zin arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 108 en aldaar aangehaalde rechtspraak).

227. Bijgevolg kan aan de bepalingen van de PNR-richtlijn die de verstrekking en beoordeling achteraf van PNR-gegevens als bedoeld in artikel 6, lid 2, onder *b)*, van deze richtlijn regelen, een met de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest conforme uitlegging worden gegeven, waarbij zij binnen de grenzen van het strikt noodzakelijke blijven ».

B.59.2. Uit dat arrest blijkt dat het Hof van Justitie verschillende verduidelijkingen formuleert in verband met de uitlegging van de verschillende verwerkingen van PNR–gegevens, opdat die in overeenstemming zouden zijn met de artikelen 7 en 8, alsook met artikel 52, lid 1, van het Handvest, met inachtneming van de grenzen van het « strikt noodzakelijke ».

Allereerst, wat betreft de voorafgaande beoordeling van de PNR-gegevens, die tot doel heeft de personen te identificeren voor wie een grondiger onderzoek vereist is vóór hun aankomst of hun vertrek en die, in een eerste fase, gebeurt via geautomatiseerde verwerkingen, kan de PIE die gegevens alleen vergelijken met de databanken betreffende de gezochte of gesignaleerde personen of voorwerpen. Die databanken moeten niet-discriminerend zijn en door de bevoegde autoriteiten worden gebruikt in verband met de strijd tegen terroristische misdrijven of ernstige vormen van criminaliteit die, minstens indirect, een objectief verband vertonen met het vervoer van de passagiers (punten 186-191).

Wat vervolgens de vooraf bepaalde criteria betreft waarop de voorafgaande beoordeling steunt, kan de PIE geen gebruikmaken van kunstmatige-intelligentietechnologieën zoals machinaal leren (*machine learning*), die, zonder menselijke tussenkomst en controle, aanpassingen kunnen doorvoeren in het beoordelingsproces en met name in de beoordelingscriteria waarop het resultaat van de toepassing van dat proces gebaseerd is, alsook in de weging van die criteria. Die criteria moeten zodanig worden gekozen dat zij specifiek gericht zijn op personen van wie redelijkerwijs kan worden vermoed dat zij betrokken zijn bij terroristische misdrijven of ernstige vormen van criminaliteit, en dat zowel « belastende » als « ontlastende » elementen in aanmerking worden genomen, zonder aanleiding te geven tot rechtstreekse of indirecte discriminaties (punten 194-200).

Om de foutenmarge met « vals-positieve » resultaten, die noodzakelijkerwijs voortvloeien uit geautomatiseerde verwerkingen, te beperken, is het van wezenlijk belang dat de PIE, in een tweede fase, een individueel heronderzoek uitvoert aan de hand van niet-geautomatiseerde middelen, volgens duidelijke en nauwkeurige regels voor de personeelsleden van de PIE die met dat individuele heronderzoek zijn belast, om een coherente administratieve praktijk binnen de PIE die het non-discriminatiebeginsel eerbiedigt, te waarborgen (punten 178-180). Inzonderheid moeten de lidstaten zich ervan vergewissen dat de PIE objectieve controlecriteria vastlegt op basis waarvan haar personeelsleden kunnen nagaan, enerzijds, of en in hoeverre een positieve overeenkomst (*hit*) daadwerkelijk iemand betreft die mogelijk betrokken is bij terroristische misdrijven of ernstige vormen van criminaliteit, alsook, anderzijds, dat de geautomatiseerde verwerkingen een niet-discriminerend karakter hebben (punten 203-209). De PIE moet elke verwerking van de PNR-gegevens documenteren die tijdens de voorafgaande beoordeling, inclusief de afzonderlijke niet-geautomatiseerde controle, wordt verricht, zodat de rechtmatigheid ervan kan worden gecontroleerd en een interne controle kan worden uitgeoefend (punt 207).

De bevoegde overheden moeten ook erop toezien dat de belanghebbende de werking van de vooraf bepaalde beoordelingscriteria en de programma's die met die criteria werken, kan begrijpen zodat hij met volledige kennis van zaken kan beslissen of hij al dan niet zijn recht op een jurisdictioneel beroep uitoefent, waarbij de rechter die belast is met de wettigheidscontrole van de door de bevoegde instanties genomen beslissing en, behalve bij bedreigingen voor de Staatsveiligheid, de betrokkene zelf kennis moeten kunnen nemen van alle motieven en van de bewijzen op basis waarvan die beslissing is genomen, inclusief de vooraf bepaalde beoordelingscriteria en de werking van de programma's die die criteria gebruiken (punten 210-211).

Wat betreft het achteraf verstrekken en beoordelen van de PNR-gegevens, met andere woorden na de aankomst of het vertrek van de betrokkene, is het Hof van Justitie van oordeel dat zij alleen kunnen plaatshebben op basis van nieuwe omstandigheden en objectieve elementen op grond waarvan ofwel redelijkerwijs kan worden vermoed dat die persoon betrokken is bij ernstige vormen van criminaliteit die, op zijn minst indirect, een objectief verband vertonen met het vervoer van passagiers, ofwel ervan kan worden uitgegaan dat die gegevens, in een concreet geval, een daadwerkelijke bijdrage zouden kunnen leveren tot de bestrijding van terroristische misdrijven die een dergelijk verband vertonen (punten 217-220). Het verstrekken van PNR-gegevens voor een dergelijke beoordeling achteraf moet, in beginsel, behalve in naar behoren gerechtvaardigde dringende gevallen, worden onderworpen aan een voorafgaande controle door hetzij een rechterlijke instantie, hetzij een onafhankelijke bestuurlijke entiteit, naar aanleiding van een gemotiveerd verzoek van de bevoegde autoriteiten, ongeacht of dat verzoek is ingediend vóór of na het verstrijken van de termijn van zes maanden na doorgifte van die gegevens aan de PIE (punten 221-226).

B.59.3. Uit hetgeen voorafgaat, vloeit voort dat de verenigbaarheid van de PNR–richtlijn met de artikelen 7 en 8 van het Handvest van de grondrechten en met de vereisten van het strikt noodzakelijke afhankelijk is van de naleving van de verschillende in B.59.2 opgesomde waarborgen, die voortvloeien uit de conforme interpretatie van het Hof van Justitie in het voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022. De verenigbaarheid van de nationale reglementeringen die de PNR-richtlijn omzetten, met de artikelen 7 en 8 van het Handvest van de grondrechten en met de vereisten van het strikt noodzakelijke, is dus in dezelfde mate hiervan afhankelijk.

B.59.4. De verenigbaarheid van het systeem dat is ingevoerd bij de wet van 25 december 2016 met de verschillende referentienormen die worden beoogd in het middel, vereist dus de wet van 25 december 2016 zo te interpreteren dat zij de waarborgen integreert die in B.59.2 worden opgesomd en onder de omzetting van de PNR-richtlijn vallen, zoals ze werd geïnterpreteerd door het Hof van Justitie.

Het staat aan de PIE en aan de verschillende betrokken autoriteiten te waken over de naleving van die waarborgen, bij de tenuitvoerlegging van de wet van 25 december 2016.

a) Het beheer van de passagiersgegevensbank door de PIE (artikelen 12 *tot* 16*)*

B.60.1. Krachtens artikel 5 van de wet van 25 december 2016 verzamelt en stuurt iedere vervoerder en reisoperator de gegevens van de passagiers van, naar en op doorreis over het nationaal grondgebied, waarover hij beschikt, door, met het oog op de registratie ervan in de passagiersgegevensbank bedoeld in artikel 15 van die wet. Krachtens artikel 6 van de wet van 25 december 2016 informeren de vervoerders en de reisoperatoren de betrokken personen dat hun gegevens doorgestuurd worden naar de PIE en achteraf kunnen worden verwerkt voor de in artikel 8 van dezelfde wet beoogde doelen.

Die passagiersgegevensbank wordt beheerd door de PIE, opgericht binnen de Federale Overheidsdienst Binnenlandse Zaken (artikel 12). De PIE is belast met het verzamelen, het bewaren en het verwerken van passagiersgegevens, alsook met het beheer van de passagiersgegevensbank, en met de uitwisseling van de gegevens en de resultaten van de verwerking ervan met de PIE's van andere lidstaten van de Europese Unie en met Europol (artikel 13). De PIE is samengesteld uit een leidend ambtenaar, bijgestaan door een ondersteunende dienst, en uit de bevoegde diensten gedetacheerde leden (artikel 14).

Het koninklijk besluit van 21 december 2017 « ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende diverse bepalingen betreffende de Passagiersinformatie-eenheid en de functionaris voor de gegevensbescherming » (hierna : koninklijk besluit van 21 december 2017) definieert onder meer de voorwaarden inzake de samenstelling en de organisatie van de PIE.

B.60.2. Overeenkomstig artikel 15, § 1, van de wet van 25 december 2016 wordt een passagiersgegevensbank opgericht die door de Federale Overheidsdienst Binnenlandse Zaken wordt beheerd en waarin passagiersgegevens worden geregistreerd. De leidend ambtenaar van de PIE is de verantwoordelijke voor de verwerking van de passagiersgegevens in de zin van artikel 26, 8°, van de wet van 30 juli 2018 « betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens » (artikel 15, § 2, van de wet van 25 december 2016, gewijzigd bij de wet van 2 mei 2019).

De verwerkingen van de passagiersgegevens uitgevoerd volgens de bestreden wet worden onderworpen aan de voormelde wet van 30 juli 2018 (artikel 15, § 4, van de wet van 25 december 2016, gewijzigd bij de wet van 2 mei 2019).

In het kader van de doelstellingen beoogd in artikel 8, § 1, van de wet van 25 december 2016 is de passagiersgegevensbank rechtstreeks toegankelijk door de PIE voor de verwerkingen bedoeld in de artikelen 24 tot 27 van dezelfde wet, overeenkomstig de bepalingen waarin hoofdstuk 9 voorziet (artikel 16). Hoofdstuk 9, dat de artikelen 18 tot 23 bevat, van de wet van 25 december 2016 bepaalt de termijnen gedurende welke de passagiersgegevens worden bewaard.

Een protocol waarbij de technische beveiligings– en toegangsregels worden uitgewerkt, wordt gesloten door de leidend ambtenaar van de PIE en de bevoegde diensten, na overleg met de functionaris voor de gegevensbescherming en na advies van de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens (artikel 17, zoals vervangen bij de wet van 15 juli 2018).

B.60.3. In verband met de oprichting van de passagiersgegevensbank wordt in de parlementaire voorbereiding uiteengezet :

« De eerste paragraaf voorziet in de oprichting van de Passagiersgegevensbank. Om de in artikel 9 bedoelde passagiersgegevens te verwerken en te analyseren, is het immers noodzakelijk deze in een specifieke gegevensbank te verwerken, om ze te kunnen structureren, exploiteren en vernietigen na een bepaalde termijn.

Aangezien het ultieme doel van de gegevensverwerking erin bestaat de veiligheid van de burgers te verzekeren, wordt de gegevensbank beheerd door de FOD Binnenlandse Zaken. De leidend ambtenaar wordt aangewezen als verantwoordelijke voor de verwerking van deze gegevensbank zoals bedoeld in artikel 1, § 4 van de Wet tot bescherming van persoonsgegevens. Hij zal bijgevolg in het door de wet bepaalde kader verantwoordelijk zijn voor het opstellen en de opvolging van de strategische plannen voor de verwerking van de gegevens en zal de nodige middelen bepalen om zijn strategische doelstellingen te bereiken » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, p. 24).

B.61.1. Door een passagiersgegevensbank op te richten, waarvan het beheer is toevertrouwd aan de PIE, voorziet de wet van 25 december 2016 in een centralisatie van de opslag van de passagiersgegevens, onder de verantwoordelijkheid van de PIE, en voorziet daarbij in talrijke waarborgen op het vlak van de beveiliging, de toegang en de bewaring van die gegevens, waarbij de verwerkingen van de gegevens die de PIE in het kader van de in artikel 8, § 1, beoogde doelstellingen kan uitvoeren, worden beperkt. Door de plaats van registratie van die gegevens nauwkeurig te identificeren, laat de oprichting van een dergelijke gegevensbank aldus toe de gegevensstromen te beperken.

Hoewel de PNR-richtlijn daarin niet uitdrukkelijk voorziet, vormt de oprichting van een passagiersgegevensbank, zoals die gepaard gaat met de in B.60 in herinnering gebrachte waarborgen, een essentieel element van het systeem dat is ingevoerd door de PNR-richtlijn, die door de wet van 25 december 2016 wordt omgezet.

B.61.2.1. Zoals is vermeld in B.60.1 is de PIE samengesteld uit een leidend ambtenaar, bijgestaan door een ondersteunende dienst, en uit de bevoegde diensten gedetacheerde leden, opgesomd in artikel 14, § 1, eerste lid, 2°, van de wet van 25 december 2016, namelijk *a)* de politiediensten, bedoeld in de wet van 7 december 1998 « tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus »; *b)* de Veiligheid van de Staat, bedoeld in de wet van 30 november 1998 « houdende regeling van de inlichtingen– en veiligheidsdiensten »; *c)* de Algemene Dienst Inlichting en Veiligheid, bedoeld in de dezelfde wet van 30 november 1998, en *d)* de onderzoeksdiensten, de opsporingsdiensten en de diensten belast met het toezicht, de controle en de vaststelling van de Algemene Administratie van douane en accijnzen.

De leidend ambtenaar van de PIE heeft de eindverantwoordelijkheid voor de taken en de opdrachten die de wet aan de PIE toevertrouwt en neemt hiertoe de nodige beslissingen (artikel 3 van het koninklijk besluit van 21 december 2017); hij moet houder zijn van een nationale en EU-veiligheidsmachtiging van het niveau « ZEER GEHEIM », zoals bedoeld in de wet van 11 december 1998 (artikel 11, eerste lid, van het koninklijk besluit van 21 december 2017).

Vanaf hun indiensttreding moeten de leden van de ondersteunende dienst houder zijn van een nationale en EU-veiligheidsmachtiging van minstens het niveau « GEHEIM », zoals bedoeld in de wet van 11 december 1998 (artikel 11, tweede lid, van het koninklijk besluit van 21 december 2017).

De leden van de bevoegde diensten worden gedurende de periode van hun detachering onder het functioneel en hiërarchisch toezicht geplaatst van de leidend ambtenaar van de PIE (artikel 14, § 1, tweede lid, van de wet van 25 december 2016). Die gedetacheerde leden worden geselecteerd op basis van hun profiel en onderworpen aan een gesprek voor een commissie van drie personen, voorgezeten door de leidend ambtenaar van de PIE, die, na afloop van het gesprek, een gemotiveerde rangorde van de kandidaten opstelt, op basis waarvan de gedetacheerde leden worden aangesteld (artikel 12 van het koninklijk besluit van 21 december 2017). Op het moment van zijn aanstelling moet het gedetacheerde lid in het kader van de opdrachten van de PIE minstens drie jaar nuttige ervaring hebben en bereid zijn om zich toe te leggen op de analyse van passagiersgegevens en op de samenwerking met de bevoegde diensten (artikel 13, 3°, van het koninklijk besluit van 21 december 2017) en houder zijn van een nationale en EU-veiligheidsmachtiging van minstens het niveau « GEHEIM » zoals bedoeld in de wet van 11 december 1998 (artikel 14 van het koninklijk besluit van 21 december 2017).

B.61.2.2. De samenstelling van de PIE en de definitie van de « bevoegde diensten » bieden waarborgen inzake expertise en vertrouwelijkheid betreffende het beheer van de passagiersgegevensbank, in het licht van de doelen die strikt zijn beperkt tot preventie en opsporing, alsook onderzoek en vervolging, van terroristische misdrijven en ernstige vormen van criminaliteit, met verwijzing naar de categorieën van misdrijven die op exhaustieve wijze zijn opgesomd in bijlage II van de PNR-richtlijn, en die, op zijn minst indirect, een objectief verband vertonen met het betrokken vervoer. Zulks geldt ook in zoverre naar de PIE leden worden gedetacheerd van de Veiligheid van de Staat en de Algemene Inlichtingen- en Veiligheidsdienst. Hetgeen is geoordeeld in B.52 betreffende het doel van toezicht op de beoogde activiteiten door de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 8, § 1, 4°, van de wet van 25 december 2016, doet aan die vaststelling geen afbreuk.

De leden van de voormelde diensten kunnen immers worden geacht over een algemene expertise inzake de bestrijding van criminaliteit te beschikken, en bijgevolg de vereiste competenties te hebben om de doeleinden na te streven die op exhaustieve wijze worden opgesomd in de PNR-richtlijn. Uit hetgeen voorafgaat, blijkt daarnaast dat de gedetacheerde personeelsleden worden geselecteerd en aangesteld op basis van een profiel dat rechtstreeks in verband staat met het beheer van de passagiersgegevensbank, en dat zij hun opdrachten, in dat kader, enkel onder het functionele en hiërarchische gezag van de leidend ambtenaar van de PIE uitoefenen.

Wanneer die personeelsleden hun opdrachten inzake het beheer van de passagiersgegevensbank uitvoeren, kunnen zij hun opdrachten dus alleen uitvoeren voor de verwerking van uitsluitend de door de PNR-richtlijn toegestane doeleinden.

B.61.3. Gelet op hetgeen is vermeld in B.61.2.2, en in het licht van de verschillende waarborgen, opgesomd in B.60, betreffende de oprichting en het beheer van de passagiersgegevensbank, is die maatregel niet onevenredig.

b) De verwerking van de passagiersgegevens in het kader van de voorafgaande beoordeling van de passagiers (artikelen 24 *tot* 26*)*

B.62.1. Artikel 16 van de wet van 25 december 2016 bepaalt dat, in het kader van de doelstellingen beoogd in artikel 8, § 1, de passagiersgegevens het voorwerp uitmaken van de verwerkingen bedoeld in de artikelen 24 tot 27.

De artikelen 24 tot 26 betreffen de verwerking van de passagiersgegevens in het kader van de voorafgaande beoordeling van de passagiers.

B.62.2. Overeenkomstig artikel 24, § 1, van de wet van 25 december 2016 worden de passagiersgegevens verwerkt met het oog op het uitvoeren van een voorafgaande beoordeling van de passagiers vóór hun geplande aankomst in, vertrek uit of doorreis over het nationaal grondgebied om te bepalen welke personen moeten worden onderworpen aan een nader onderzoek (artikel 24, § 1).

In de parlementaire voorbereiding van de wet van 25 december 2016 wordt uitgelegd :

« Artikel 24 betreft de voorafgaande beoordeling (*prescreening*) van het risico dat de passagiers vormen. Het is de bedoeling de potentiële dreiging te beoordelen en te bepalen welke passagiers belangrijk zijn voor de uitoefening van hun opdrachten of bijvoorbeeld een te nemen maatregel vereisen (uitvoering van een aanhoudingsmandaat, fouillering, ...).

Deze voorafgaande beoordeling wordt toegepast vóór de aankomst, de doorreis of het vertrek op het nationaal grondgebied » (*ibid.*, p. 28).

B.62.3.1. De voorafgaande beoordeling steunt op twee krachtlijnen : enerzijds de correlatie van de passagiersgegevens met de gegevensbanken en, anderzijds, de correlatie van de gegevens met vooraf bepaalde criteria.

Die beoordeling berust op een positieve overeenstemming, die voortvloeit uit een correlatie van de passagiersgegevens met :

- de gegevensbanken die door de bevoegde diensten worden beheerd en door de PIE vooraf bepaalde beoordelingscriteria, in het kader van de doelstellingen beoogd in artikel 8, § 1er, 1°, 2°, 4° et 5°, of met betrekking tot de bedreigingen vermeld in de artikelen 8, 1°, *a)*, *b)*, *c)*, *d)*, *f)*, *g)*, en 11, § 2, van de wet van 30 november 1998 (artikel 24, § 2, zoals vervangen bij de wet van 15 juli 2018); voor die doelstellingen zijn alle in artikel 9 bedoelde passagiersgegevens toegankelijk (artikel 26, § 2, zoals vervangen bij de wet van 15 juli 2018);

- de gegevensbanken die door de bevoegde diensten worden beheerd, in het kader van de doelstellingen beoogd in artikel 8, § 1, 3° (artikel 24, § 3). Voor dat doel zijn alleen de passagiersgegevens bedoeld in artikel 9, § 1, 18°, met betrekking tot de persoon of personen voor wie een positieve overeenstemming werd gegenereerd, toegankelijk (artikel 26, § 1).

De positieve overeenstemming wordt gevalideerd door de PIE binnen vierentwintig uur na ontvangst van het geautomatiseerd bericht van de positieve overeenstemming (artikel 24, § 4). Vanaf het moment van die validatie geeft de bevoegde dienst, die aan de basis ligt van de positieve overeenstemming, een nuttig gevolg binnen de kortst mogelijke termijn (artikel 24, § 5).

Tot slot is artikel 24, § 2, van de wet van 25 december 2016, krachtens artikel 5 van de wet van 2 mei 2019, aangevuld met een nieuw lid. Die wijziging « beoogt in artikel 24, § 2, te voorzien dat de voorafgaande beoordeling van passagiers ook berust op een analyse van andere passagiersgegevens die verband houden met een positieve overeenstemming » (*Parl. St.*, Kamer, 2018-2019, DOC 54—3652/001, p. 5)

B.62.3.2. Ten aanzien van de correlatie met de gegevensbanken wordt in de parlementaire voorbereiding van de wet van 25 december 2016 uiteengezet :

« De eerste factor bestaat uit het zoeken naar positieve overeenstemmingen door middel van verbanden van passagiersgegevens met de gegevens verwerkt in de gegevensbanken die door de bevoegde diensten worden beheerd. Dit maakt het bijvoorbeeld mogelijk om te beoordelen of een persoon een hoge gevaarlijkheidsgraad heeft, omdat hij is bekend in een politionele gegevensbank in het kader van een terroristisch dossier en waarvoor uit de analyse van zijn passagiersgegevens blijkt dat hij zich regelmatig naar landen begeeft die trainingskampen voor terroristen hebben of naar landen om door te reizen naar dergelijke plaatsen. Het kan bijvoorbeeld ook gaan om een persoon over wie beschikbare inlichtingen bij de inlichtingendiensten aangeven dat hij een gijzeling zou voorbereiden en dat hij zich, op basis van de vervoersgegevens, naar een land begeeft waarvan de inlichtingendiensten, op basis van de ontvangen inlichtingen, weten dat deze persoon er zou kunnen rekruteren om zijn plannen tot uitvoering te brengen. Hoe meer positieve overeenstemmingen bovendien ontdekt worden door verschillende diensten voor één en dezelfde persoon, hoe waarschijnlijker de reële dreiging.

De positieve overeenstemming kan eveneens het nemen van een maatregel vergen op bevel van de gerechtelijke overheden, zoals het uitvoeren van een aanhoudingsbevel ten aanzien van een persoon die klaar staat om België te verlaten.

De positieve overeenstemming kan eveneens blijken uit een verband met internationale gegevensbanken, zoals SIS II, Interpol (SLTD).

Het is natuurlijk niet de bedoeling om alle gegevensbanken van de diensten te linken met de passagiersgegevensbank, maar wel om de correlaties met de gegevensbanken die rechtstreeks verband houden met de door de wet bepaalde doelen, technisch te beperken.

[...]

Deze correlatie zal eveneens moeten worden gemaakt via lijsten van personen die specifiek zijn opgesteld door de bevoegde diensten voor dit doel. Overeenkomstig de wet tot bescherming van de persoonlijke levenssfeer en meer in het bijzonder artikel 4, § 1, 4°, zullen deze lijsten regelmatig moeten worden bijgewerkt » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, pp. 28—29).

Wat betreft de correlatie met de vooraf bepaalde criteria wordt in de parlementaire voorbereiding van de wet van 25 december 2016 uiteengezet :

« De tweede factor bestaat uit het zoeken naar positieve overeenstemmingen via (één of meerdere) door de PIE vooraf bepaalde criteria die worden toegepast op de passagiersgegevens. Deze criteria bestaan uit één of meerdere objectieve indicatoren waaruit kan worden afgeleid dat de personen die er het voorwerp van uitmaken, een specifiek risicogedrag vertonen, dat een dreiging kan vormen in het licht van de doelen in artikel 8, § 1, punten 1, 4 en 5, van de wet.

In deze criteria kunnen bijvoorbeeld bepaalde specifieke reserverings– of reisgedragingen worden opgenomen.

Het gebruik van deze criteria biedt het voordeel dat risicovolle passagiersprofielen tevoorschijn kunnen treden, die niet noodzakelijkerwijze zijn gekend of opgenomen in de gegevensbanken van de diensten

Deze criteria kunnen bijvoorbeeld betrekking hebben op een bepaald land van bestemming of vertrek, in combinatie met bepaalde reisgegevens, zoals de betaalmethode en de datum van reservering » (*ibid.*, pp. 29-30).

« De voorafgaande beoordeling in het kader van het doel met betrekking tot het toezien op fenomenen van bestuurlijke politie en groeperingen die verbonden zijn met gewelddadige radicalisering, is aan veel strengere voorwaarden onderworpen dan de andere doelen :

- ze kan zich enkel baseren op een correlatie met de gegevensbanken van de politiediensten;

- Enkel de gegevens bedoeld in artikel 9, § 1, 18° van de wet zijn toegankelijk.

Voor de voorafgaande beoordeling in het kader van de andere doelen is de toegang tot alle in artikel 9 opgesomde passagiersgegevens toegelaten » (*ibid.*, p. 31).

« De positieve overeenstemming moet in elk geval worden gevalideerd door de PIE. Immers, om de volstrekte naleving van het recht op de bescherming van persoonsgegevens, en meer bepaald van artikel 12*bis* van de privacywet en het recht op non-discriminatie, te waarborgen, mag geen enkele beslissing met juridische gevolgen worden genomen voor een persoon of die deze persoon ernstig nadeel kan berokkenen, op de loutere basis van de geautomatiseerde verwerking van de gegevens van het bestand met informatie over zijn reis. Daarom moet de menselijke beoordeling steeds voorafgaan aan elke bindende beslissing voor de betrokken persoon.

Deze validatie moet gebeuren binnen de 24 uur teneinde het recht op toegang tot de passagiersgegevensbank te openen.

§ 5. Na deze validatie van de positieve overeenstemming komt het aan de diensten die aan de basis liggen van de positieve overeenstemming toe om een nuttige actie te nemen binnen een passende termijn. Een nuttige actie kan een actieve interventie (fouille, arrestatie, ...) betekenen, maar kan evengoed een beslissing zijn om voorlopig geen actieve interventie te ondernemen. Deze operationele beoordeling komt volledig aan de bevoegde diensten toe » (*ibid.*, pp. 30-31).

B.62.4.1. Wat betreft de door de PIE vooraf bepaalde beoordelingscriteria voorziet artikel 25 van de wet van 25 december 2016 erin dat die criteria niet gebaseerd mogen zijn op gegevens die de raciale of etnische oorsprong van een persoon, zijn religieuze of levensbeschouwelijke overtuigingen, zijn politieke opvattingen, zijn vakbondslidmaatschap, zijn gezondheidstoestand, zijn seksleven of zijn seksuele geaardheid onthullen (artikel 25, § 3).

De beoordeling van de passagiers vóór hun aankomst, doorreis of vertrek op grond van de vooraf bepaalde criteria wordt op niet-discriminerende wijze verricht. Die criteria mogen niet gericht zijn op de identificatie van een individu en moeten doelgericht, evenredig en specifiek zijn (artikel 25, § 2).

De passagiersgegevens kunnen door de PIE worden gebruikt voor het bijstellen van bestaande criteria of het formuleren van nieuwe criteria die bestemd zijn om zich te richten op individuen bij de voorafgaande beoordelingen van de passagiers (artikel 25, § 1).

B.62.4.2. In de parlementaire voorbereiding van de wet van 25 december 2016 wordt in dat verband uiteengezet :

« Voor alle raadplegingsmodaliteiten geldt op technisch vlak een eenvormig verwerkingsprincipe: op basis van een correlatie met een operationeel risicoprofiel of databank worden ' *hits* ' gegenereerd ten aanzien van een uniek PNR-record. Deze hit is enkel zichtbaar voor de desbetreffende dienst. Elke hit moet manueel gevalideerd worden door het gedetacheerde lid van de desbetreffende bevoegde dienst om te worden omgezet in een ' *match* ' [...].

[...]

Zodra een positieve overeenstemming is gevalideerd, wordt automatisch een encryptiecode gegenereerd, die zal worden gekruist met de codes van alle bevoegde diensten. Indien twee codes overeenkomen, worden twee of meerdere betrokken diensten op de hoogte gebracht dat er gedeelde positieve overeenstemmingen bestaan voor deze unieke PNR-record. Deze diensten dienen dan een nuttig gevolg te geven binnen een gepaste termijn » (*ibid.*, p. 23; zie eveneens *Parl. St.*, Kamer, 2015-2016, DOC 54—2069/003, p. 7).

« Artikel 25 bepaalt de derde wijze voor de verwerking van de gegevens : de PIE verwerkt de passagiersgegevens om de bestaande criteria bij te werken of om nieuwe criteria te bepalen, die gebruikt moeten worden tijdens de voorafgaande beoordelingen van de passagiers, teneinde de beoordeling te objectiveren en bijgevolg een strikte selectie van enkel de risicopassagiers uit te voeren.

Aangezien de verwerking van de passagiersgegevens een inmenging in hun privéleven inhoudt, zal de garantie op een objectivering van de vooraf bepaalde criteria het eveneens mogelijk maken om het toereikende, ter zake dienende en niet bovenmatige karakter van de inmenging in het privéleven te waarborgen.

De vooraf bepaalde criteria moeten doelgericht, evenredig en specifiek zijn. Bovendien mogen criteria niet gericht zijn op de identificatie van één individu. Daarom wordt gesteld dat deze niet nominatief zijn.

Ze mogen onder geen beding gebaseerd zijn op gegevens die het ras, de etnische afstamming, de religieuze, levensbeschouwelijke of politieke overtuiging, het vakbondslidmaatschap, de gezondheid, het seksleven of de seksuele geaardheid van de betrokkene onthullen » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, p. 31).

B.63.1. Het systeem van de voorafgaande beoordeling impliceert de vergelijking van de PNR-gegevens van alle passagiers met databanken of vooraf bepaalde criteria, om overeenstemmingen te vinden teneinde die personen te identificeren die aan een grondiger onderzoek moeten worden onderworpen.

Uit de voorgaande elementen, geïnterpreteerd in het licht van hetgeen is vermeld in B.59, blijkt dat de artikelen 24 tot 26 van de wet van 25 december 2016 binnen de grenzen van het « strikt noodzakelijke » blijven.

B.63.2.1. De databanken waarmee de PNR–gegevens kunnen worden vergeleken, zijn nauwkeurig gedefinieerd en opgesomd in artikel 24 van de wet van 25 december 2016. Worden beoogd, de databanken van de « bevoegde diensten », namelijk de politiediensten, de Veiligheid van de Staat, de Algemene Dienst Inlichting en Veiligheid en de Douane, maar het kan ook, zoals is gepreciseerd in de parlementaire voorbereiding aangehaald in B.62.3.2, gaan om een vergelijking met de internationale databanken, zoals SIS II, Interpol (SLTD), waartoe de bevoegde diensten toegang hebben in het kader van de uitoefening van hun opdrachten.

Artikel 24, § 2, 1°, van de wet van 25 december 2016 laat tevens een correlatie toe met « lijsten van personen die worden opgesteld door de bevoegde diensten in het kader van hun opdrachten ». Zoals is vermeld in B.61.2.2, kunnen de leden van de voormelde diensten immers worden geacht te beschikken over een algemene expertise inzake de bestrijding van criminaliteit, en bijgevolg de vereiste competenties te hebben om de doeleinden na te streven die op exhaustieve wijze zijn opgesomd in de PNR–richtlijn.

B.63.2.2. Uit de in B.62.3.2 aangehaalde parlementaire voorbereiding blijkt dat het nagestreefde doel niet erin bestaat alle databanken van de diensten te koppelen aan de passagiersgegevensbank, maar wel de correlaties met de databanken die rechtstreeks in verband staan met de doeleinden die strikt zijn beperkt tot de bestrijding van terroristische misdrijven en ernstige vormen van criminaliteit met een, op zijn minst indirect, een objectief verband met het vervoer van passagiers, technisch te beperken.

De wetgever beoogde dus de technische correlaties in het kader van de voorafgaande beoordeling duidelijk te beperken, teneinde alleen de profielen te identificeren waarvoor een grondiger onderzoek nodig is in het licht van uitsluitend de doeleinden die op exhaustieve wijze worden opgesomd in de PNR–richtlijn.

B.63.2.3. Rekening houdend met het arrest van het Hof van Justitie in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, waaraan wordt herinnerd in B.59, moet de vergelijking van de PNR–gegevens met de databanken en lijsten bedoeld in artikel 24, § 2, 1°, van de wet van 25 december 2016 derhalve zo worden geïnterpreteerd dat die technisch gezien strikt is beperkt tot uitsluitend de databanken betreffende de gezochte of gesignaleerde personen of voorwerpen, waarbij die databanken door de bevoegde autoriteiten op niet-discriminerende wijze worden gebruikt in verband met de strijd tegen terroristische misdrijven en ernstige vormen van criminaliteit met een, op zijn minst indirect, een objectief verband met het vervoer van passagiers.

Het staat aan de PIE erover te waken dat, vanuit technisch oogpunt, de geautomatiseerde verwerking welke die correlaties mogelijk maakt, de grenzen van het strikt noodzakelijke niet overschrijdt.

B.63.3.1. In verband met de vooraf bepaalde beoordelingscriteria vereist artikel 6, lid 4, van de PNR-richtlijn dat die vooraf bepaalde criteria « doelgericht, evenredig en specifiek » zijn en dat de lidstaten ervoor zorgen dat die criteria « door de PIE worden vastgesteld en regelmatig worden getoetst ».

Artikel 25 van de wet van 25 december 2016 waarborgt uitdrukkelijk dat de beoordeling van de passagiers vóór hun aankomst, doorreis of vertrek op grond van vooraf bepaalde criteria op niet-discriminerende wijze wordt verricht en dat die criteria niet gericht mogen zijn op de identificatie van een individu en doelgericht, evenredig en specifiek moeten zijn (§ 2). In de in B.62.4.2 aangehaalde parlementaire voorbereiding wordt gepreciseerd dat zij niet nominatief zijn. Bovendien mogen die criteria niet gebaseerd zijn op gegevens die de raciale of etnische oorsprong van een persoon, zijn religieuze of levensbeschouwelijke overtuigingen, zijn politieke opvattingen, zijn vakbondslidmaatschap, zijn gezondheidstoestand, zijn seksleven of zijn seksuele geaardheid onthullen (§ 3).

Analoog met de correlaties met de databanken, is de totstandkoming van vooraf bepaalde criteria opgevat als technisch beperkt tot de identificatie van personen ten aanzien van wie een grondiger onderzoek moet worden gevoerd in het licht van de doeleinden die strikt zijn beperkt tot de bestrijding van terroristische misdrijven en ernstige vormen van criminaliteit met een, op zijn minst indirect, objectief verband met het passagiersvervoer.

B.63.3.2. Rekening houdend met het arrest van het Hof van Justitie in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, waaraan wordt herinnerd in B.59, dient de totstandkoming van vooraf bepaalde criteria bedoeld in artikel 25 van de wet van 25 december 2016 zo te worden geïnterpreteerd dat die de PIE belet om gebruik te maken van kunstmatige-intelligentietechnologieën in het kader van machinaal leren (*machine learning*), die, zonder menselijke tussenkomst of controle, aanpassingen kunnen doorvoeren. Bovendien moeten de beoordelingscriteria waarop het resultaat van de toepassing van dat proces steunt, alsook de weging van die criteria zo worden gekozen dat zij specifiek gericht zijn op personen van wie redelijkerwijs kan worden vermoed dat zij betrokken zijn bij terroristische misdrijven of ernstige vormen van criminaliteit, en dat zowel « belastende » als « ontlastende » elementen in aanmerking worden genomen, zonder daarbij aanleiding te geven tot rechtstreekse of indirecte discriminaties.

Het staat aan de PIE erover te waken dat, vanuit technisch oogpunt, de totstandkoming van de vooraf bepaalde criteria de grenzen van het strikt noodzakelijke niet overschrijdt.

B.63.4.1. Ten aanzien van de zorg om de foutenmarge door « vals-positieve » resultaten te beperken, dient te worden vastgesteld dat artikel 24, §§ 4 en 5, van de wet van 25 december 2016 erin voorziet dat de PIE een individueel heronderzoek uitvoert door de positieve overeenstemming binnen vierentwintig uur te valideren, waardoor aldus, in geval van een positieve overeenstemming, aan de hand van niet-geautomatiseerde middelen een individuele verificatie wordt verricht van de geautomatiseerde systematische verwerking, teneinde te beoordelen of de bevoegde autoriteit maatregelen dient te nemen op grond van het nationaal recht, zoals artikel 6, lid 5, van de PNR–richtlijn dat vereist.

Bovendien waarborgt artikel 21, § 3, tweede lid, van de wet van 25 december 2016 dat, wanneer, naar aanleiding van het in artikel 24, § 4, bedoelde individuele heronderzoek, het resultaat van de verwerking negatief blijkt, het niettemin kan worden bewaard zolang de basisgegevens niet werden gewist op basis van artikel 18, om foutieve positieve overeenstemmingen te vermijden.

Rekening houdend met het voormelde arrest van het Hof van Justitie in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, waaraan wordt herinnerd in B.59, dient dat individuele heronderzoek zo te worden geïnterpreteerd dat het wordt uitgevoerd volgens duidelijke en nauwkeurige regels die toelaten een coherente administratieve praktijk binnen de PIE te waarborgen waarbij het beginsel van niet-discriminatie in acht wordt genomen, en na te gaan of en in welke mate een positieve overeenstemming (*hit*) effectief betrekking heeft op een persoon die kan worden betrokken bij terroristische misdrijven of ernstige vormen van criminaliteit.

Het staat aan de PIE te waken over de naleving van die vereisten.

B.63.4.2. Artikel 23, § 1, van de wet van 25 december 2016 waarborgt dat de gegevensverwerking het voorwerp uitmaakt van een « oplijsting » gedefinieerd in artikel 4, 11°, van dezelfde wet als « het mechanisme bedoeld in artikel 23, § 2, dat toelaat de uitgevoerde gegevensverwerkingen op te sporen, opdat het identificeerbaar is welke persoon, op welk moment, welke gegevens heeft geraadpleegd en met welk doel ».

Artikel 23, § 2, van de wet van 25 december 2016 waarborgt dat de PIE gedurende vijf jaar een documentair spoor bewaart van alle behandelsystemen en –procedures onder haar verantwoordelijkheid. Dat documentair spoor omvat minstens : de naam en contactgegevens van de organisatie en van het personeel belast met het verwerken van de passagiersgegevens binnen de PIE, alsook hun aanvragen en de verschillende niveaus van toegangsmachtigingen (1°), een register van de verwerkingsactiviteiten dat minstens de identiteit aanduidt van de persoon die de passagiersgegevens verwerkt heeft (2°), de aanvragen van de bevoegde overheden en de PIE's van andere lidstaten van de Europese Unie (3°), en alle aanvragen en alle overdrachten van gegevens naar een derde land (4°). De PIE stelt die documentaire sporen ter beschikking van de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens, op haar verzoek (artikel 23, § 2, tweede lid).

Die bepaling waarborgt aldus dat de PIE een documentair spoor bewaart van elke verwerking van PNR–gegevens in het kader van de voorafgaande beoordeling, inclusief in het kader van het individuele heronderzoek door niet-geautomatiseerde middelen, teneinde de rechtmatigheid ervan te controleren en een interne controle uit te oefenen.

B.63.5. Wat betreft de rechten van en de informatie aan de betrokken personen heeft het Hof van Justitie ten slotte, in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, aangehaald in B.59, gepreciseerd dat de bevoegde autoriteiten eveneens zich ervan moeten vergewissen dat de betrokkene de werking van de vooraf bepaalde beoordelingscriteria en van de programma's die die criteria toepassen, moet kunnen begrijpen, zodat hij, met volle kennis van zaken, kan beslissen of hij al dan niet zijn bij artikel 13, lid 1, van de PNR–richtlijn gewaarborgde recht op een jurisdictioneel beroep uitoefent, in het kader waarvan de rechter die belast is met de wettigheidscontrole van de door de bevoegde instanties genomen beslissing, alsook, behalve bij bedreigingen voor de Staatsveiligheid, de betrokkene zelf moet kunnen kennisnemen van alle motieven en van de bewijzen op basis waarvan die beslissing is genomen, inclusief de vooraf bepaalde beoordelingscriteria en de werking van de programma's die deze criteria gebruiken (punten 210-211).

Het staat aan de bevoegde autoriteiten te waken over de naleving van die vereisten.

c) De gerichte opzoekingen (artikelen 27, 50 *en* 51*)*

B.64.1. Artikel 27 van de wet van 25 december 2016, in de oorspronkelijke versie ervan, laat de verwerking van de persoonsgegevens toe om gerichte opzoekingen te verrichten voor de doelstellingen beoogd in artikel 8, § 1, 1°, 2°, 4° en 5°, van dezelfde wet en onder de voorwaarden bepaald in artikel 46*septies* van het Wetboek van strafvordering of in artikel 16/3 van de wet van 30 november 1998, respectievelijk ingevoegd bij de artikelen 50 en 51 van de wet van 25 december 2016. Artikel 6 van de wet van 2 mei 2019, dat niet wordt bestreden, heeft artikel 27 van de wet van 25 december 2016 gewijzigd om die gerichte opzoekingen toe te laten onder de voorwaarden bepaald in artikel 281, § 4, van de algemene wet inzake douane en accijnzen, gecoördineerd op 18 juli 1977.

Overeenkomstig artikel 20 van de wet van 25 december 2016 gelden de toepassingsvoorwaarden van artikel 27 van diezelfde wet eveneens voor de mededeling van alle gegevens van de passagiers na de termijn van zes maanden bedoeld in artikel 19 van die wet.

B.64.2. Zoals ingevoegd bij artikel 50 van de wet van 25 december 2016, bepaalt artikel 46*septies* van het Wetboek van strafvordering :

« Bij het opsporen van de misdaden en wanbedrijven bedoeld in artikel 8, § 1, 1°, 2° en 5°, van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, kan de procureur des Konings, bij een schriftelijke en met redenen omklede beslissing, de officier van gerechtelijke politie opdragen om de PIE te vorderen tot het meedelen van de passagiersgegevens overeenkomstig artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

De maatregel kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek onderzoek. In dit geval preciseert de procureur des Konings de duur van de maatregel die niet langer kan zijn dan een maand, te rekenen vanaf de beslissing, onverminderd hernieuwing.

In geval van uiterst dringende noodzakelijkheid kan iedere officier van gerechtelijke politie, na mondelinge en voorafgaande instemming van de procureur des Konings, en bij een gemotiveerde en schriftelijke beslissing, de leidend ambtenaar van de PIE vorderen tot het meedelen van de passagiersgegevens. De officier van de gerechtelijke politie deelt deze gemotiveerde en schriftelijke beslissing en de verkregen informatie binnen vierentwintig uur mee aan de procureur des Konings en motiveert tevens de uiterst dringende noodzakelijkheid ».

Die bepaling heeft dus betrekking op de gerichte opzoekingen in het kader van de doelen beoogd in artikel 8, § 1, 1°, 2° en 5°, van de wet van 25 december 2016. Die maatregel wordt omgeven met verschillende waarborgen, waaronder de voorafgaande toestemming van de procureur des Konings.

B.64.3. Zoals ingevoegd bij artikel 51 van de wet van 25 december 2016 bepaalt artikel 16/3 van de wet van 30 november 1998 :

« § 1. De inlichtingen– en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, mits afdoende motivering, beslissen om toegang te hebben tot de passagiersgegevens bedoeld in artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

§ 2. De in § 1 bedoelde beslissing, wordt door een diensthoofd genomen en schriftelijk overgemaakt aan de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van voormelde wet. De beslissing wordt met de motivering van deze beslissing aan het Vast Comité I betekend.

Het Vast Comité I verbiedt de inlichtingen– en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.

De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt de lijst van de raadplegingen van de passagiersgegevens een keer per maand aan het Vast Comité I doorgegeven ».

Die bepaling betreft dus de gerichte opzoekingen in het kader van het doel beoogd in artikel 8, § 1, 4°, van de wet van 25 december 2016. Die maatregel wordt omgeven met verschillende waarborgen, waaronder het inlichten van en de controle door het Vast Comité I.

B.64.4. Wat betreft de gerichte opzoekingen wordt in de parlementaire voorbereiding van de wet van 25 december 2016 uiteengezet :

« Artikel 27 bepaalt de verwerkingswijze die er voor de PIE in bestaat geval per geval te reageren op de afdoende gemotiveerde aanvragen van bevoegde overheden tot het verkrijgen van passagiersgegevens en de verwerking ervan in specifieke gevallen. Deze verwerkingswijze is beperkt tot vier doelen en sluit die uit die gepaard gaat met het toezien op fenomenen van bestuurlijke politie en de leden van een groepering zoals bedoeld in artikel 8, § 1, punt 3.

Volgens de diensten houdt de hypothese in dat een onderzoeks– of inlichtingendossier wordt geopend naar aanleiding van een positieve voorafgaande beoordeling of op basis van andere concrete elementen los van de passagiersgegevens.

Op politioneel vlak wordt bijvoorbeeld een strafonderzoek ingesteld naar aanleiding van een positieve fouillering van een passagier die in het bezit was van verdovende middelen, zoals bleek uit een voorafgaande beoordeling of naar aanleiding van een voertuig– of persoonscontrole op de openbare weg. In beide gevallen kan het noodzakelijk blijken om de passagiersgegevens ' met terugwerkende kracht ' te raadplegen voor de noden van het onderzoek teneinde de eventuele verplaatsingen van de verdachte na te gaan.

Het raadplegen van de passagiersgegevensbank gebeurt hier eigenlijk niet meer op basis van de vooraf bepaalde criteria of op basis van een automatische correlatie, maar op basis van opzoekingen met behulp van elementen afkomstig uit het dossier. Bijvoorbeeld een naam, het paspoortnummer van de verdachte, gsm-nummer, bestemming, ...

In dat kader is het nog belangrijker om te kunnen terugvallen op een historiek van de passagiersgegevens, rekening houdend met de duur en de complexiteit van bepaalde onderzoeken, en het feit dat er inbreuken veel later na de verplaatsingen worden ontdekt. Daarom moeten de gegevens over een periode van 5 jaar toegankelijk zijn om bewijzen te vergaren, eventuele mededaders of kompanen te vinden en criminele netwerken te ontmantelen.

Bijvoorbeeld : naar aanleiding van nieuwe elementen in een terrorismeonderzoek vindt de behandelende magistraat dat hij bepaalde reisgegevens van geïdentificeerde verdachten moet raadplegen.

De toelating van de procureur des Konings is op elk moment noodzakelijk om toegang te krijgen tot alle informatie, met inbegrip van de afgeschermde informatie voor wat betreft de finaliteiten van artikel 8 § 1, 1°, 2° en 5°. Voor wat betreft de finaliteit van artikel 8 § 1, 4° is de toelating van het diensthoofd vereist zoals omschreven in artikel 51 » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, pp. 32-33).

« De artikelen 50 en 51 betreffen de bepalingen tot wijziging van het Wetboek van Strafvordering en de organieke wet van 30 november 1998 houdende regeling van de inlichtingen– en veiligheidsdienst met betrekking tot de nadere regels voor toegang tot de passagiersgegevens in het kader van de *a posteriori* analyse » (*ibid.*, p. 43).

B.65.1. De verzoekende partij is bovendien van mening dat de uit de politiediensten gedetacheerde leden die deel uitmaken van de PIE onvoldoende onafhankelijk zijn om de verzoeken om toegang in het kader van die gerichte opzoekingen te beantwoorden.

B.65.2. Krachtens artikel 14, § 1, van de wet van 25 december 2016 is de PIE samengesteld uit een leidend ambtenaar, bijgestaan door een ondersteunende dienst (artikel 14, § 1, 1°), alsook uit leden die zijn gedetacheerd uit de politiediensten, de Veiligheid van de Staat, de Algemene Inlichtingen– en Veiligheidsdienst, en de onderzoeksdiensten, opsporingsdiensten en diensten belast met het toezicht, de controle en vaststelling van de Algemene Administratie van de Douane en Accijnzen (artikel 14, § 1, 2°, zoals gewijzigd bij de wet van 15 juli 2018).

Ten aanzien van de samenstelling van de PIE wordt in de parlementaire voorbereiding uiteengezet :

« Het Belgisch model is gebaseerd op een concept van multidisciplinaire eenheid, samengesteld uit een leidend ambtenaar die een leidinggevende functie vervult, alsook uit administratieve leden en gedetacheerde leden afkomstig uit de bevoegde diensten.

De PIE is samengesteld uit :

- een leidend ambtenaar, bijgestaan door een ondersteuningsdienst, die binnen de FOD Binnenlandse Zaken verantwoordelijk zal zijn voor het beheer van de gegevensbank, het naleven van de verplichtingen van de vervoerders en reisoperatoren, de rapportering, het afsluiten van protocollen met de bevoegde diensten en het naleven van de verwerkingsvoorwaarden. De ondersteunende dienst zal met name worden samengesteld uit analisten, juristen, ICT-experten, een functionaris voor de gegevensbescherming en administratieve ondersteuning.

- gedetacheerde leden die afkomstig zijn uit de bevoegde diensten die limitatief zijn opgesomd in punt 2 van § 1, namelijk de politiediensten, de inlichtingendiensten en de Douane. De precieze doelen vormen op zich de eerste beperking. Op het niveau van de diensten van de geïntegreerde politie spreekt het bijvoorbeeld voor zich dat een wijkagent bij de lokale politie nooit kennis zal kunnen nemen van de passagiersgegevens, aangezien de doelen niet tot zijn opdrachten behoren.

De detachering van de bevoegde diensten heeft tot doel enige graad van expertise te garanderen, maar sluit geenszins uit dat er tussen de bevoegde diensten akkoorden worden gesloten met het oog op de onderlinge afstemming van de detacheringen » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, p. 22).

De minister van Veiligheid en Binnenlandse Zaken heeft eveneens gepreciseerd :

« In totaal zullen vijftien personen toegang hebben tot de gegevens. De vier bevoegde diensten zullen elk twee personen detacheren die de zeven personeelsleden van de PIE vervoegen. Er zal ook een *data protection officer* toegevoegd worden die verslag uitbrengt aan de Commissie voor de bescherming van de persoonlijke levenssfeer » (*Parl. St.*, Kamer, 2015—2016, DOC 54—2069/003, p. 24).

B.65.3. Ter uitvoering van artikel 14, § 4, van de wet van 25 december 2016 regelt het koninklijk besluit van 21 december 2017 « ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende diverse bepalingen betreffende de Passagiersinformatie-eenheid en de functionaris voor de gegevensbescherming » de voorwaarden inzake de samenstelling en de organisatie van de PIE.

In het verslag aan de Koning dat aan dat koninklijk besluit voorafgaat, wordt gepreciseerd :

« De gegevensbank kan dus enkel geraadpleegd worden binnen de PIE, uitsluitend door leden van de PIE in het kader van hun opdrachten, alsook door de functionaris voor de gegevensbescherming » (*Belgisch Staatsblad* van 29 december 2017, tweede editie, p. 116833).

De detacheringsprocedure is geregeld bij de artikelen 12 tot 21 van het voormelde koninklijk besluit van 21 december 2017.

B.65.4. Zoals is vermeld in B.61.2, strekt het feit dat de uit bevoegde diensten gedetacheerde leden deelnemen aan de werking van de PIE, ertoe te waarborgen dat die PIE is samengesteld uit personen met een zekere expertise, teneinde aldus de doeltreffendheid van de PIE te versterken.

Artikel 4, lid 3, van de PNR-richtlijn voorziet overigens uitdrukkelijk in die detacheringsmogelijkheid. Die bepaling luidt :

« Het personeel van een PIE kan uit bevoegde instanties worden gedetacheerd [...] ».

Niets laat toe ervan uit te gaan dat die personen, ook al behouden zij hun statuut in hun oorspronkelijke dienst, hun functies binnen de PIE niet onafhankelijk uitoefenen. Artikel 14, § 1, tweede lid, van de wet van 25 december 2016 preciseert trouwens dat, gedurende de periode van hun detachering, « de leden van de bevoegde diensten [...] onder het functioneel en hiërarchisch toezicht [worden] geplaatst van de leidend ambtenaar van de PIE ».

De leden van de PIE kunnen bovendien strafrechtelijk worden gestraft wanneer zij het beroepsgeheim niet naleven of wanneer zij informatie, gegevens en inlichtingen willens en wetens achterhouden waardoor de in artikel 8 bepaalde doelen worden verhinderd (artikelen 48 en 49 van dezelfde wet).

B.65.5.1. Wat betreft de toegang tot de PNR–gegevens na het verstrijken van een termijn van zes maanden bepaalt artikel 12, lid 3, van de PNR–richtlijn :

« Wanneer de in lid 2 bedoelde termijn van zes maanden is verstreken, wordt mededeling van de volledige PNR-gegevens uitsluitend toegestaan als :

a) er redelijkerwijze wordt aangenomen dat zulks noodzakelijk is voor de in artikel 6, lid 2, onder *b)*, bedoelde doeleinden en

b) goedgekeurd door :

i) een gerechtelijke instantie, of

ii) een andere nationale instantie die volgens het nationale recht bevoegd is om na te gaan of aan de voorwaarden voor mededeling is voldaan, onder voorbehoud van kennisgeving aan, en controle achteraf door, de functionaris voor gegevensbescherming van de PIE ».

B.65.5.2. Overeenkomstig artikel 20 van de wet van 25 december 2016 gelden de toepassingsvoorwaarden van artikel 27 van dezelfde wet eveneens voor de mededeling van alle passagiersgegevens na de periode van zes maanden bedoeld in artikel 19. Door de regeling van de gerichte opzoekingen bedoeld in artikel 27 van die wet uit te breiden tot de mededeling van alle passagiersgegevens na de termijn van zes maanden, wijkt artikel 20 af van het beginsel vastgelegd in artikel 19 van de wet van 25 december 2016, volgens hetwelk, na een periode van zes maanden, te rekenen vanaf de registratie van de passagiersgegevens in de passagiersgegevensbank, alle passagiersgegevens worden gedepersonaliseerd.

In de parlementaire voorbereiding van de wet van 25 december 2016 wordt in dat verband uiteengezet :

« Na 6 maanden kunnen de passagiersgegevens enkel nog volledig zichtbaar worden gemaakt wanneer er redelijke motieven bestaan om te denken dat ze noodzakelijk zijn voor de toepassing van artikel 27 en enkel onder de voorwaarden bepaald in artikel 27.

Deze verwerkingswijze sluit dus het doel verbonden aan het toezien op fenomenen van bestuurlijke politie en leden van een groepering zoals bepaald in artikel 8, § 1, punt 3, uit.

De toelating van de procureur des Konings is noodzakelijk » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, p. 26).

Uit de combinatie van de artikelen 20 en 27 van de wet van 25 december 2016 blijkt derhalve dat de voorwaarden inzake de toegang tot de PNR–gegevens in het kader van gerichte opzoekingen worden overgenomen voor de mededeling van gegevens na een termijn van zes maanden volgend op het doorgeven van de gegevens aan de PIE, termijn waarna die gegevens zouden moeten worden gedepersonaliseerd.

B.66.1. Aangezien, zoals is geoordeeld in B.52, het doel beoogd in artikel 8, § 1, 4°, van de wet van 25 december 2016 de vereisten van het « strikt noodzakelijke » overschrijdt, geldt hetzelfde voor de bepalingen die de inlichtingen– en veiligheidsdiensten zouden toestaan om, bij eenvoudig gemotiveerde beslissing, toegang te hebben tot de gegevens van de passagiersgegevensbank, voor dat doel dat verder gaat dan de doeleinden die op exhaustieve wijze worden opgesomd in de PNR–richtlijn.

B.66.2. Om dezelfde redenen als die welke zijn uiteengezet betreffende artikel 8, § 1, 4°, van de wet van 25 december 2016 overschrijdt artikel 51 van de wet van 25 december 2016 de vereisten van het « strikt noodzakelijke ».

B.67. Het Hof moet thans onderzoeken of de regeling inzake de mededeling van de PNR–gegevens bepaald in de artikelen 27 en 50 van de wet van 25 december 2016 voldoet aan de vereisten van het strikt noodzakelijke, alsook aan de waarborgen van onafhankelijkheid van de autoriteit die is belast met het toestaan van die toegang.

B.68.1. Zoals is vermeld in B.59, in verband met het achteraf verstrekken en beoordelen van de PNR–gegevens, met andere woorden na de aankomst of het vertrek van de betrokken persoon, is het Hof van Justitie van oordeel dat zulks alleen kan plaatshebben op basis van nieuwe omstandigheden en objectieve elementen op grond waarvan ofwel redelijkerwijs kan worden vermoed dat die persoon is betrokken bij ernstige vormen van criminaliteit die een, op zijn minst indirect, objectief verband vertonen met het vervoer van de passagiers, ofwel ervan kan worden uitgegaan dat die gegevens, in een concreet geval, effectief zouden kunnen bijdragen tot de bestrijding van terroristische misdrijven die een dergelijk verband vertonen.

De mededeling van PNR–gegevens met het oog op een dergelijke beoordeling achteraf moet, in beginsel, behalve in naar behoren gerechtvaardigde dringende gevallen, worden onderworpen aan een voorafgaande controle door hetzij een rechterlijke instantie, hetzij een onafhankelijke bestuurlijke entiteit, naar aanleiding van een gemotiveerd verzoek van de bevoegde autoriteiten, ongeacht of dat verzoek is ingediend vóór of na het verstrijken van de termijn van zes maanden volgend op de doorgifte van die gegevens aan de PIE.

Meer bepaald preciseert het Hof van Justitie dat de vereiste van een voorafgaande controle bepaald in artikel 12, lid 3, *b)*, van de PNR–richtlijn, voor de verzoeken om mededeling van de PNR–gegevens ingediend na het verstrijken van de termijn van zes maanden volgend op de doorgifte van die gegevens aan de PIE, eveneens *mutatis mutandis* moet gelden voor het geval waarin dat verzoek vóór het verstrijken van die termijn wordt gedaan (punt 224).

B.68.2. Op een vraag van het Hof over de uitlegging van een « andere bevoegde nationale instantie » in de zin van artikel 12, lid 3, van de PNR–richtlijn, heeft het Hof van Justitie, in zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geoordeeld :

« 241. Ten gronde zij erop gewezen dat artikel 12, lid 3, onder *b)*, van de PNR-richtlijn, waarin in de punten *i)* en ii) wordt gesproken van ‘ een gerechtelijke instantie ’ respectievelijk ‘ een andere nationale instantie die volgens het nationale recht bevoegd is om na te gaan of aan de voorwaarden voor mededeling is voldaan ’, deze twee instanties op hetzelfde niveau plaatst, zoals blijkt uit het voegwoord ‘ of ’ tussen punt *i)* en punt ii). Uit deze bewoordingen blijkt dus dat de ‘ andere ’ bevoegde nationale instantie die hier wordt bedoeld, een alternatief is voor de gerechtelijke instantie en derhalve een vergelijkbaar niveau van onafhankelijkheid en onpartijdigheid moet hebben.

242. Deze analyse vindt steun in de in overweging 25 van de PNR-richtlijn genoemde doelstelling van deze richtlijn om het hoogste niveau van gegevensbescherming te waarborgen wanneer toegang tot de volledige PNR-gegevens wordt verleend en de betrokkene dus rechtstreeks kan worden geïdentificeerd. In diezelfde overweging wordt trouwens verduidelijkt dat ná de termijn van zes maanden na de doorgifte van de PNR-gegevens aan de PIE, een dergelijke volledige toegang slechts onder zeer strikte voorwaarden kan worden verleend.

243. Deze analyse wordt ook bevestigd door de ontstaansgeschiedenis van de PNR–richtlijn. Terwijl het in punt 155 van dit arrest vermelde voorstel van richtlijn, dat aan de PNR–richtlijn ten grondslag ligt, louter bepaalde dat ‘ toegang tot de volledige PNR-gegevens enkel kan worden verleend door de verantwoordelijke van de passagiersinformatie-eenheid ’, worden in de versie van artikel 12, lid 3, onder *b)*, van deze richtlijn waarvoor de Uniewetgever uiteindelijk heeft gekozen enerzijds de gerechtelijke instanties aangewezen en anderzijds ‘ andere nationale [instanties] ’ die bevoegd zijn om na te gaan of de voorwaarden voor mededeling van de integrale PNR-gegevens zijn vervuld en om deze mededeling toe te staan, waarbij deze twee soorten instanties op hetzelfde niveau worden geplaatst.

244. Voorts is het overeenkomstig de in de punten 223, 225 en 226 van dit arrest aangehaalde rechtspraak vooral essentieel dat de toegang van de bevoegde autoriteiten tot de bewaarde gegevens wordt onderworpen aan een voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van die autoriteiten dat met name wordt ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Het vereiste van onafhankelijkheid voor de instantie die de voorafgaande toetsing moet verrichten, impliceert ook dat zij de hoedanigheid van derde moet hebben ten opzichte van de autoriteit die om toegang tot de gegevens verzoekt, zodat zij de toetsing objectief en onpartijdig en zonder beïnvloeding van buitenaf kan verrichten. In het bijzonder impliceert het vereiste van onafhankelijkheid op strafrechtelijk gebied dat de instantie die belast is met die voorafgaande toetsing enerzijds niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en anderzijds neutraal moet zijn ten opzichte van de partijen in de strafprocedure.

245. Zoals de advocaat-generaal in punt 271 van zijn conclusie heeft opgemerkt, bepaalt artikel 4 van de PNR-richtlijn in de leden 1 en 3 dat de PIE die in elke lidstaat wordt opgericht of aangewezen een instantie moet zijn die bevoegd is om terroristische misdrijven en ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen, en dat het personeel van de PIE kan worden gedetacheerd uit de in artikel 7 van deze richtlijn bedoelde bevoegde instanties. De PIE lijkt dan ook noodzakelijkerwijs verbonden te zijn aan deze instanties. De PIE kan volgens artikel 6, lid 2, onder *b)*, van deze richtlijn ook PNR-gegevens verwerken en het resultaat daarvan aan hen doorgeven. Bijgevolg kan de PIE niet worden geacht de hoedanigheid van derde ten aanzien van die instanties te hebben en dus over de nodige onafhankelijkheid en onpartijdigheid te beschikken om de in het vorige punt van dit arrest genoemde voorafgaande toetsing te verrichten en na te gaan of voldaan is aan de voorwaarden om de volledige PNR–gegevens mee te delen als bedoeld in artikel 12, lid 3, onder *b)*, ervan.

246. Hieraan wordt niet afgedaan door het feit dat laatstgenoemde bepaling in punt ii) vereist dat wanneer de mededeling van de volledige PNR-gegevens wordt goedgekeurd door een ‘ andere nationale instantie ’, de functionaris voor gegevensbescherming van de PIE hiervan in kennis wordt gesteld en een controle achteraf verricht, terwijl dit niet wordt vereist wanneer een gerechtelijke instantie die goedkeuring verleent. Volgens vaste rechtspraak kan met een latere controle — zoals die welke de functionaris voor gegevensbescherming verricht — immers niet worden tegemoetgekomen aan het doel van een voorafgaande toetsing, dat erin bestaat te verhinderen dat tot de betrokken gegevens een toegang wordt verleend die verder gaat dan strikt noodzakelijk is (zie in die zin arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 110 en aldaar aangehaalde rechtspraak).

247. Gelet op al deze overwegingen dient op de zevende vraag te worden geantwoord dat artikel 12, lid 3, onder *b)*, van de PNR-richtlijn aldus moet worden uitgelegd dat het zich verzet tegen nationale wetgeving waarbij de instantie die wordt opgericht om als PIE op te treden ook de hoedanigheid heeft van nationale instantie die bevoegd is om de mededeling van PNR-gegevens na het verstrijken van de periode van zes maanden na doorgifte ervan aan de PIE goed te keuren ».

B.68.3. Uit hetgeen voorafgaat, vloeit voort dat het achteraf verstrekken en beoordelen van de PNR–gegevens gepaard gaat met zowel organieke als substantiële vereisten.

Enerzijds, op organiek niveau, kan de PIE niet worden geacht de hoedanigheid te hebben van een « bevoegde nationale instantie » die ertoe gemachtigd is de mededeling van PNR–gegevens, zij het vóór of na het verstrijken van de periode van zes maanden na de doorgifte van die gegevens aan de PIE, goed te keuren. Volgens het Hof van Justitie moet een dergelijke bevoegde nationale instantie een niveau van onafhankelijkheid en onpartijdigheid vertonen dat vergelijkbaar is met dat van een rechterlijke instantie, hetgeen impliceert dat de instantie die belast is met die voorafgaande controle, enerzijds, niet betrokken is bij de uitvoering van het betrokken strafrechtelijk onderzoek en, anderzijds, neutraal moet zijn ten opzichte van de partijen in de strafprocedure (punt 244). Een latere controle, zoals die door de functionaris voor gegevensbescherming, laat niet toe tegemoet te komen aan het doel van een voorafgaande toetsing (punt 246).

Anderzijds, op substantieel niveau, kan die mededeling alleen worden beslist op basis van nieuwe omstandigheden en objectieve elementen op grond waarvan ofwel redelijkerwijs kan worden vermoed dat die persoon is betrokken bij ernstige vormen van criminaliteit die een, op zijn minst indirect, objectief verband vertonen met het passagiersvervoer, ofwel ervan kan worden uitgegaan dat die gegevens, in een concreet geval, effectief zouden kunnen bijdragen tot het bestrijden van de terroristische misdrijven die een dergelijk verband vertonen.

B.69.1. Zoals is vermeld in B.64.1 en B.64.2, laat artikel 27 van de wet van 25 december 2016 toe PNR–gegevens te verstrekken om gerichte opzoekingen te verrichten onder de voorwaarden die met name zijn bepaald in artikel 46*septies* van het Wetboek van strafvordering, ingevoegd bij artikel 50 van de wet van 25 december 2016.

Die bepaling beperkt het gebruik van het voormelde artikel 27 tot de doelen beoogd in artikel 8, § 1, 1°, 2° en 5°, van de wet van 25 december 2016, en voorziet in de voorafgaande instemming van de procureur des Konings, bij een gemotiveerde en schriftelijke beslissing, die de evenredigheid van de maatregel weerspiegelt met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad; die maatregel mag niet langer zijn dan een maand na de beslissing, onverminderd vernieuwing.

Vanuit substantieel oogpunt dient de regeling van de voorafgaande instemming bepaald in artikel 27 van de wet van 25 december 2016, rekening houdend met het arrest van het Hof van Justitie in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, waaraan in B.59 wordt herinnerd, zo te worden geïnterpreteerd dat zij vereist dat de autoriteit die de voorafgaande controle van de noodzakelijkheid van het verstrekken van de PNR–gegevens, op gemotiveerd verzoek van de bevoegde autoriteiten, zal uitvoeren, geval per geval het bestaan beoordeelt van nieuwe omstandigheden en objectieve elementen op grond waarvan ofwel redelijkerwijs kan worden vermoed dat die persoon betrokken is bij ernstige vormen van criminaliteit die een, op zijn minst indirect, objectief verband vertonen met het passagiersvervoer, ofwel ervan kan worden uitgegaan dat die gegevens, in een concreet geval, effectief zouden kunnen bijdragen tot de bestrijding van terroristische misdrijven die een dergelijk verband vertonen.

Aldus geïnterpreteerd is de regeling bepaald in artikel 27 van de wet van 25 december 2016, vanuit substantieel oogpunt, in overeenstemming met de in het middel beoogde bepalingen.

B.69.2. Vanuit organiek oogpunt daarentegen laat de in artikel 27 van de wet van 25 december 2016 bepaalde regeling, die van toepassing is op de gerichte opzoekingen en die, zoals in B.65.5 is vermeld, bij artikel 20 van dezelfde wet is uitgebreid tot het verstrekken van gegevens na het verstrijken van een termijn van zes maanden, niet toe ervan uit te gaan dat een voorafgaande controle van de beslissing tot verstrekken is toevertrouwd aan een « onafhankelijke nationale instantie ».

Allereerst, zoals in B.68.3 is vermeld, kan de PIE niet worden beschouwd als een « onafhankelijke nationale instantie » wanneer zij passagiersgegevens verstrekt op verzoek van bevoegde autoriteiten.

Vervolgens voorziet artikel 46*septies* van het Wetboek van strafvordering, dat werd ingevoegd bij artikel 50 van de wet van 25 december 2016 en waarnaar artikel 27 van dezelfde wet verwijst, weliswaar in een voorafgaand optreden van de procureur des Konings, maar, overeenkomstig het voormelde artikel 46*septies*, is het die laatstgenoemde die zelf beslist, bij een schriftelijk en gemotiveerde beslissing, om de officier van gerechtelijke politie op te dragen de PIE te vorderen tot het meedelen van de passagiersgegevens overeenkomstig artikel 27 van de wet van 25 december 2016. Bovendien kan de procureur des Konings, daar hij belast is met het onderzoek van de misdrijven, niet worden beschouwd als een onafhankelijke nationale instantie die de toetsing mag uitvoeren die voorafgaat aan het verstrekken van de gegevens, zoals vereist door het Hof van Justitie in punt 244 van zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022.

Voor het overige dient te worden vastgesteld dat artikel 281, § 4, van de algemene wet inzake douane en accijnzen, gecoördineerd op 18 juli 1977, dat is ingevoegd bij artikel 6 van de wet van 2 mei 2019, en waarnaar artikel 27 van de wet van 25 december 2016 verwijst, zoals gewijzigd bij diezelfde wet van 2 mei 2019, erin voorziet dat de adviseur-generaal die aangewezen is voor het departement geschillen bij een schriftelijk en met redenen omklede beslissing een ambtenaar van de douane en accijnzen kan opdragen de PIE te vorderen tot het meedelen van de passagiersgegevens. De regeling bepaald in artikel 16/3 van de wet van 30 november 1998 « houdende regeling van de inlichtingen– en veiligheidsdiensten », ingevoegd bij artikel 51 van de wet van 25 december 2016 – dat de vereisten van het strikt noodzakelijke overschrijdt, zoals het Hof heeft geoordeeld in B.66 –, voorzag daarentegen erin dat de inlichtingen– en veiligheidsdiensten, in het belang van de uitoefening van hun opdrachten, mits afdoende motivering, konden beslissen om toegang te hebben tot de passagiersgegevens bedoeld in artikel 27 van de wet van 25 december 2016.

Dergelijke procedures, waarnaar artikel 27 van de wet van 25 december 2016 verwijst, komen bijgevolg niet tegemoet aan de vereiste van een controle die voorafgaat aan het verstrekken van de gegevens, door een onafhankelijke administratieve instantie, zoals gedefinieerd door het Hof van Justitie in de punten 244 tot 246 van zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022.

B.69.3. In zoverre het, behalve in naar behoren gerechtvaardigde dringende gevallen, de verstrekking van de PNR–gegevens met het oog op een beoordeling achteraf, niet ondergeschikt maakt aan een voorafgaande controle die wordt uitgevoerd door ofwel een rechtscollege, ofwel een « onafhankelijke bestuurlijke entiteit », op gemotiveerd verzoek van de bevoegde autoriteiten, schendt artikel 27 van de wet van 25 december 2016 de in het middel beoogde bepalingen.

B.69.4. Het staat aan de wetgever het orgaan te bepalen dat belast is met de uitvoering van die voorafgaande controle, rekening houdend met hetgeen het Hof van Justitie heeft geoordeeld bij zijn arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022 ten aanzien van zowel de omvang van de controle als de voorwaarden inzake onpartijdigheid en onafhankelijkheid van het met die controle belaste orgaan.

B.69.5. In afwachting van dat optreden van de wetgever, dat geacht wordt de verstrekking van de PNR–gegevens met het oog op een latere beoordeling mogelijk te maken, dient ervan te worden uitgegaan dat de Gegevensbeschermingsautoriteit – die overeenkomstig artikel 4, § 2, tweede lid, van de wet van 3 december 2017 « tot oprichting van de Gegevensbeschermingsautoriteit », beschikt over een residuaire bevoegdheid ten aanzien van de verwerking van persoonsgegevens – een « onafhankelijke bestuurlijke entiteit » is die voldoet aan de door het Hof van Justitie gestelde vereisten van onpartijdigheid en onafhankelijkheid.

Vooraleer PNR–gegevens worden verstrekt met het oog op een latere beoordeling, dient bijgevolg, voor de toepassing van artikel 27 van de wet van 25 december 2016, vooraf een beroep te worden gedaan op de Gegevensbeschermingsautoriteit, rekening houdend met hetgeen is vermeld in B.69.1 en in voorkomend geval door zich te inspireren op de regeling bepaald in artikel 46*septies* van het Wetboek van strafvordering.

B.70. In zoverre het is gericht tegen artikel 51 van de wet van 25 december 2016, en tegen artikel 27 van de wet van 25 december 2016, doordat die laatste, behalve in naar behoren gerechtvaardigde dringende gevallen, de verstrekking van de PNR–gegevens met het oog op een beoordeling achteraf, niet ondergeschikt maakt aan een voorafgaande toetsing uitgevoerd door ofwel een rechtscollege ofwel een « onafhankelijke bestuurlijke instantie », op gemotiveerd verzoek van de bevoegde autoriteiten, is het middel gegrond.

Voor het overige, onder voorbehoud van de interpretaties vermeld in B.63.2.3, B.63.3.2, B.63.4.1, B.69.1 en rekening houdend met hetgeen is vermeld in B.61.2.2, is het middel, in zoverre het is gericht tegen de artikelen 12 tot 16 en 24 tot 26 en 50 van de wet van 25 december 2016, niet gegrond.

5. *De bewaartermijn van de PNR–gegevens (artikel* 18*)*

B.71. De verzoekende partij bekritiseert artikel 18 van de wet van 25 december 2016 in zoverre de termijn van vijf jaar gedurende welke de PNR–gegevens worden bewaard, onevenredig zou zijn.

B.72.1. Artikel 12 van de PNR-richtlijn, met als opschrift « Bewaartermijn van de gegevens en anonimisering », bepaalt :

« 1. De lidstaten zorgen ervoor dat de door de luchtvaartmaatschappijen aan de PIE verstrekte PNR-gegevens bij die PIE in een databank worden bewaard gedurende een termijn van vijf jaar nadat de gegevens zijn doorgegeven aan de PIE van de lidstaat waar de vlucht aankomt of vertrekt.

2. Wanneer een termijn van zes maanden is verstreken nadat de PNR-gegevens overeenkomstig lid 1 zijn doorgegeven, worden de PNR-gegevens gedepersonaliseerd door afscherming van de volgende gegevenselementen waaruit de identiteit van de passagier op wie de PNR-gegevens betrekking hebben, rechtstreeks zou kunnen worden afgeleid :

a) naam/namen, waaronder de namen van andere passagiers in het PNR en het aantal reizigers in het PNR dat samen reist;

b) adres en contactgegevens;

c) alle betalingsinformatie, met inbegrip van het factuuradres, voor zover daarin informatie is vervat waaruit de identiteit van de passagier op wie het PNR betrekking heeft of van andere personen rechtstreeks zou kunnen worden afgeleid;

d) informatie betreffende reizigers die gebruikmaken van een loyaliteitsprogramma voor frequent reizen;

e) algemene opmerkingen, voor zover deze informatie bevatten waaruit rechtstreeks de identiteit zou kunnen worden afgeleid van de passagier op wie het PNR betrekking heeft; en

f) verzamelde API-gegevens.

3. Wanneer de in lid 2 bedoelde termijn van zes maanden is verstreken, wordt mededeling van de volledige PNR-gegevens uitsluitend toegestaan als :

a) er redelijkerwijze wordt aangenomen dat zulks noodzakelijk is voor de in artikel 6, lid 2, onder *b)*, bedoelde doeleinden en

b) goedgekeurd door :

i) een gerechtelijke instantie, of

ii) een andere nationale instantie die volgens het nationale recht bevoegd is om na te gaan of aan de voorwaarden voor mededeling is voldaan, onder voorbehoud van kennisgeving aan, en controle achteraf door, de functionaris voor gegevensbescherming van de PIE.

4. De lidstaten zorgen ervoor dat de PNR-gegevens na het verstrijken van de in lid 1 bedoelde termijn definitief worden gewist. Deze verplichting geldt niet indien bepaalde PNR–gegevens zijn doorgegeven aan een bevoegde instantie en worden gebruikt in het kader van een specifieke zaak met het oog op het voorkomen, opsporen, onderzoeken of vervolgen van terroristische misdrijven of ernstige criminaliteit; in dat geval beheerst het nationale recht het bewaren van de gegevens door de bevoegde instantie.

5. De PIE bewaart het resultaat van de in artikel 6, lid 2, onder *a)*, bedoelde verwerking niet langer dan noodzakelijk is om een overeenstemming te kunnen melden aan de bevoegde instanties en, overeenkomstig artikel 9, lid 1, aan de PIE's van andere lidstaten. Indien het resultaat van geautomatiseerde verwerking na een afzonderlijke niet-geautomatiseerde controle als bedoeld in artikel 6, lid 5, negatief blijkt te zijn, kan dit niettemin worden opgeslagen om ' valse ' overeenkomsten in de toekomst te voorkomen, voor zover de onderliggende gegevens niet op grond van lid 4 van dit artikel worden gewist ».

Considerans 25 van de PNR-richtlijn bepaalt :

« De bewaartermijn voor PNR-gegevens dient zo lang te zijn als noodzakelijk is voor en evenredig te zijn aan de doelstellingen, namelijk het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit. Gezien de aard van de gegevens en het gebruik ervan dienen de PNR-gegevens lang genoeg te worden bewaard om er een analyse mee te kunnen uitvoeren en ze bij onderzoek te kunnen gebruiken. Ter voorkoming van onevenredig gebruik dienen de gegevens na de initiële bewaartermijn door afscherming van gegevenselementen te worden gedepersonaliseerd. Om te zorgen voor het hoogste niveau van gegevensbescherming, dient toegang tot de volledige PNR-gegevens, waarmee de betrokkene rechtstreeks kan worden geïdentificeerd, uitsluitend onder zeer strikte en restrictieve voorwaarden te worden toegestaan na die initiële bewaartermijn ».

B.72.2. Artikel 18 van de wet van 25 december 2016 voorziet erin dat de passagiersgegevens in de passagiersgegevensbank bewaard worden gedurende een maximale termijn van vijf jaar, te rekenen vanaf de registratie ervan, en dat ze aan het einde van die termijn worden vernietigd.

Overeenkomstig artikel 21, § 1, van de wet van 25 december 2016 zorgt de PIE ervoor dat de passagiersgegevens definitief uit haar gegevensbank worden verwijderd na de periode bedoeld in artikel 18.

B.72.3. In de parlementaire voorbereiding van de wet van 25 december 2016 wordt uiteengezet :

« Artikel 18 bepaalt de bewaartermijn voor de gegevens in de passagiersgegevensbank.

Overeenkomstig artikel 4, 4° van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, worden de persoonsgegevens bewaard onder een vorm die toelaat de betrokken personen te identificeren gedurende een termijn die niet langer is dan deze die noodzakelijk is om de doelstellingen waarvoor ze werden verzameld of waarvoor ze later worden verwerkt, te verwezenlijken.

Daarom worden de gegevens van het bestand met reisgegevens, zoals bedoeld in artikel 9, bewaard gedurende een maximale termijn van 5 jaar voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, alsook voor de bescherming van de fundamentele belangen van de staat, en vervolgens worden ze definitief gewist uit de Passagiersgegevensbank. Na afloop van deze termijn worden ze vernietigd.

Deze termijn van maximum 5 jaar moet het mogelijk maken om de noodzakelijke analyses en verificaties uit te voeren met het oog op het ontdekken van nieuwe fenomenen of het opsporen van nieuwe tendensen die verbonden zijn aan de doelen van de wet, om de bestaande risicoprofielen aan te passen of nieuwe risicoprofielen te bepalen, en om desgevallend bewijzen te verzamelen, eventuele mededaders of medeplichtigen te vinden en criminele netwerken te ontmantelen » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, pp. 25-26).

B.72.4.1. De bewaartermijn van vijf jaar waarin artikel 18 van de wet van 25 december 2016 voorziet, dient evenwel te worden gelezen in samenhang met de artikelen 19 en volgende van dezelfde wet, die ook de voorwaarden inzake de bewaring van de gegevens regelen.

B.72.4.2. Artikel 19 van de wet van 25 december 2016 bepaalt :

« Na een periode van zes maanden vanaf het registreren van de passagiersgegevens in de passagiersgegevensbank, worden alle passagiersgegevens gedepersonaliseerd, door afscherming van de volgende gegevenselementen waaruit de identiteit van de passagier op wie de gegevens betrekking hebben, rechtstreeks zou kunnen worden afgeleid :

1° naam/namen, waaronder de namen van andere passagiers en het aantal passagiers dat samen reist;

2° adres– en contactgegevens;

3° alle betalingsinformatie, met inbegrip van het factureringsadres, voor zover daarin informatie is vervat waaruit de identiteit van de passagier of elke andere persoon rechtstreeks zou kunnen worden afgeleid;

4° informatie betreffende reizigers die gebruikmaken van een loyaliteitsprogramma voor frequent reizen;

5° algemene opmerkingen, voor zover deze informatie bevatten waaruit de identiteit van de passagier rechtstreeks zou kunnen worden afgeleid; en

6° alle gegevens bedoeld in artikel 9, § 1, 18° ».

Die bepaling dient te worden gelezen in samenhang met artikel 4, 14°, van de wet van 25 december 2016, dat het « depersonaliseren door afscherming van gegevenselementen » definieert als « het voor een gebruiker onzichtbaar maken van de gegevenselementen waaruit de identiteit van de betrokken persoon rechtstreeks zou kunnen worden afgeleid, bedoeld in artikel 19 ».

B.72.4.3. Zoals is vermeld in B.64.1 en B.65.5, bepaalt artikel 20 van de wet van 25 december 2016 dat, na de periode van zes maanden bedoeld in artikel 19, de mededeling van alle passagiersgegevens uitsluitend wordt toegestaan voor de door artikel 27 voorgeschreven verwerking van de gegevens en enkel onder de daarin bepaalde voorwaarden.

Overigens, het resultaat van de verwerking bedoeld in artikel 24 wordt door de PIE enkel bewaard voor de tijd die noodzakelijk is om de bevoegde diensten te informeren en, overeenkomstig artikel 36, om de PIE's van de andere lidstaten van de Europese Unie te informeren over het bestaan van een positieve overeenstemming (artikel 21, § 3, eerste lid).

B.72.4.4. Artikel 22 van de wet van 25 december 2016 waarborgt dat de leidend ambtenaar en de functionaris voor de gegevensbescherming alleen toegang hebben tot alle gegevens die voor het uitvoeren van hun opdracht relevant zijn.

Ten slotte worden de verwerkte gegevens opgelijst en staan zij rechtstreeks in correlatie met de doelstellingen bepaald in artikel 8 (artikel 23, § 1). De PIE zorgt voor de oplijsting door een documentair spoor gedurende vijf jaar te bewaren voor alle behandelsystemen en –procedures onder haar verantwoordelijkheid (artikel 23, § 2, eerste lid).

B.73.1. Op een vraag van het Hof over de bewaartermijn van de PNR–gegevens heeft het Hof van Justitie, in het voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geoordeeld :

« 249. Er zij aan herinnerd dat volgens artikel 12, leden 1 en 4, van deze richtlijn de PIE van de lidstaat waar de betrokken vlucht aankomt of vertrekt, de door de luchtvaartmaatschappijen doorgegeven PNR-gegevens gedurende vijf jaar na doorgifte bewaart in een databank, en daarna definitief wist.

250. Zoals in overweging 25 van de PNR-richtlijn in herinnering wordt gebracht, dient ' de bewaartermijn voor PNR-gegevens [...] zo lang te zijn als noodzakelijk is voor en evenredig te zijn aan de doelstellingen, namelijk het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit '.

251. Bijgevolg kan het krachtens artikel 12, lid 1, van de PNR-richtlijn bewaren van PNR–gegevens niet worden gerechtvaardigd indien er geen objectief verband is tussen de bewaring en de met deze richtlijn nagestreefde doelstellingen, namelijk het bestrijden van terroristische misdrijven en ernstige vormen van criminaliteit die minstens indirect een objectief verband vertonen met het luchtvervoer van passagiers.

252. Blijkens overweging 25 van de PNR-richtlijn moet een onderscheid worden gemaakt tussen de initiële bewaartermijn van zes maanden, zoals bedoeld in artikel 12, lid 2, van deze richtlijn, en de periode daarna, zoals bedoeld in artikel 12, lid 3.

253. Bij de uitlegging van artikel 12, lid 1, van de PNR-richtlijn moet rekening worden gehouden met de leden 2 en 3 van dit artikel, die de bewaring van en toegang tot PNR-gegevens na de initiële bewaartermijn van zes maanden regelen. Zoals uit overweging 25 van deze richtlijn volgt, geven deze bepalingen enerzijds het belang weer dat PNR-gegevens ' lang genoeg [...] worden bewaard om er een analyse mee te kunnen uitvoeren en ze bij onderzoek te kunnen gebruiken ', wat reeds tijdens de initiële bewaartermijn van zes maanden kan, en anderzijds de noodzaak om ' onevenredig gebruik ' te voorkomen, door deze gegevens af te schermen, en „te zorgen voor het hoogste niveau van gegevensbescherming" door toegang in een vorm waardoor de betrokkene rechtstreeks kan worden geïdentificeerd, ' uitsluitend onder zeer strikte en restrictieve voorwaarden [toe te staan] na die initiële bewaartermijn ' en er aldus rekening mee te houden dat hoe langer de PNR-gegevens worden bewaard, hoe ernstiger de inmenging is.

254. Het onderscheid tussen de initiële bewaartermijn van zes maanden, (artikel 12, lid 2, van de PNR-richtlijn) en de periode daarna (artikel 12, lid 3, ervan) moet worden doorgetrokken naar het in punt 251 van dit arrest genoemde vereiste.

255. Gelet op de doelstellingen van de PNR-richtlijn en de noden die bestaan bij het onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, moet dan ook worden geoordeeld dat het gedurende de initiële termijn van zes maanden bewaren van PNR–gegevens van alle luchtreizigers die onder het systeem van deze richtlijn vallen, ook zonder enige aanwijzing dat zij betrokken zijn bij terroristische misdrijven of ernstige criminaliteit, in beginsel niet verder lijkt te gaan dan strikt noodzakelijk is, aangezien op die manier de nodige opzoekingen kunnen worden gedaan teneinde personen te identificeren die nog niet van terroristische misdrijven of ernstige criminaliteit worden verdacht.

256. Wat de periode daarna betreft daarentegen (artikel 12, lid 3, van de PNR-richtlijn), houdt het bewaren van PNR-gegevens van alle luchtreizigers die onder het systeem van deze richtlijn vallen niet alleen — gezien de aanzienlijke hoeveelheid gegevens die continu kunnen worden bewaard — inherente risico's van onevenredig gebruik en misbruik in (zie naar analogie arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 119), maar druist het ook in tegen het vereiste van overweging 25 van deze richtlijn, namelijk dat de gegevens niet langer worden bewaard dan noodzakelijk is voor en evenredig is aan de nagestreefde doelstellingen. De Uniewetgever heeft immers het hoogste niveau van gegevensbescherming willen invoeren voor PNR-gegevens waarmee de betrokkenen rechtstreeks kunnen worden geïdentificeerd.

257. Wat luchtreizigers betreft waarvoor noch uit de voorafgaande beoordeling [artikel 6, lid 2, onder *a)*, van de PNR-richtlijn] noch uit eventuele controles in de periode van zes maanden (artikel 12, lid 2, van deze richtlijn) noch uit andere omstandigheden is gebleken dat er objectieve aanwijzingen bestaan dat zij een gevaar vormen op het gebied van terroristische misdrijven of ernstige criminaliteit met een minstens indirect objectief verband met de door hen genomen vlucht, lijkt er tussen hun PNR-gegevens en de doelstelling van deze richtlijn immers geen verband — zelfs geen indirect verband — te bestaan dat de bewaring van deze gegevens rechtvaardigt [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 204 en 205].

258. De duurzame opslag van de PNR-gegevens van alle reizigers na de initiële periode van zes maanden is dus niet beperkt tot wat strikt noodzakelijk is [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 206].

259. Wanneer in specifieke gevallen op basis van objectieve elementen, zoals PNR–gegevens die een geverifieerde positieve overeenkomst opleveren, kan worden aangenomen dat bepaalde reizigers een risico kunnen vormen op het gebied van terrorisme of ernstige criminaliteit, lijkt het echter wel toelaatbaar hun PNR-gegevens langer dan die initiële periode op te slaan [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 207 en aldaar aangehaalde rechtspraak].

260. Deze objectieve elementen leggen immers een verband met de doeleinden die de PNR-richtlijn met de verwerking nastreeft, zodat het gerechtvaardigd is de PNR-gegevens van die passagiers te bewaren gedurende de door deze richtlijn toegestane maximumtermijn, te weten vijf jaar.

261. Aangezien de wetgeving in het hoofdgeding lijkt te voorzien in een algemene bewaartermijn voor PNR-gegevens van vijf jaar die zonder onderscheid geldt voor alle passagiers, ook passagiers waarvoor noch uit de voorafgaande beoordeling [artikel 6, lid 2, onder *a)*, van de PNR-richtlijn] noch uit eventuele controles tijdens de initiële periode van zes maanden noch uit andere omstandigheden is gebleken dat er objectieve aanwijzingen bestaan dat zij een gevaar vormen op het gebied van terroristische misdrijven of ernstige criminaliteit, is die wetgeving mogelijkerwijs in strijd met artikel 12, lid 1, van deze richtlijn, gelezen in het licht van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, tenzij daaraan een met deze bepalingen conforme uitlegging kan worden gegeven, wat de verwijzende rechter dient na te gaan.

262. Gelet op het voorgaande dient op de achtste vraag te worden geantwoord dat artikel 12, lid 1, van de PNR-richtlijn, gelezen in samenhang met de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen nationale wetgeving die voor PNR-gegevens een algemene bewaartermijn van vijf jaar voorschrijft die zonder onderscheid geldt voor alle luchtreizigers, ook luchtreizigers van wie noch uit de voorafgaande beoordeling [artikel 6, lid 2, onder *a)*, van deze richtlijn], noch uit eventuele controles tijdens de periode van zes maanden (artikel 12, lid 2, van deze richtlijn), noch uit andere omstandigheden is gebleken dat er objectieve aanwijzingen bestaan dat zij een gevaar vormen op het gebied van terroristische misdrijven of ernstige criminaliteit met een minstens indirect objectief verband met het luchtvervoer van passagiers ».

B.73.2. Uit dat arrest vloeit voort dat, wat betreft de bewaartermijn van de PNR–gegevens, een onderscheid dient te worden gemaakt tussen, enerzijds, de initiële bewaartermijn van zes maanden, bedoeld in artikel 12, lid 2, van die richtlijn en, anderzijds, de periode daarna, zoals bedoeld in artikel 12, lid 3, van diezelfde richtlijn (punt 252) : hoewel het bewaren, gedurende de initiële termijn van zes maanden, van de PNR–gegevens van alle passagiers die onder het systeem van die richtlijn vallen, zonder enige aanwijzing dat zij betrokken zijn bij terroristische misdrijven of ernstige

vormen van criminaliteit, in beginsel niet verder lijkt te gaan dan het strikt noodzakelijke, aangezien op die manier de nodige opzoekingen kunnen worden gedaan teneinde personen te identificeren die niet van terroristische misdrijven of ernstige vormen van criminaliteit werden verdacht (punt 255), overschrijdt het bewaren van de PNR–gegevens van alle passagiers die vallen onder het systeem van die richtlijn, na die initiële periode van zes maanden, de grenzen van het strikt noodzakelijke, met name wegens de aanzienlijke hoeveelheid gegevens die continu kunnen worden bewaard en de inherente risico's van onevenredig gebruik en misbruik (punt 256).

Wat betreft de passagiers voor wie noch uit de voorafgaande beoordeling bedoeld in artikel 6, lid 2, onder *a)*, van de PNR–richtlijn, noch uit de eventuele controles in de periode van zes maanden bedoeld in artikel 12, lid 2, van die richtlijn, noch uit andere omstandigheden is gebleken dat er objectieve aanwijzingen bestaan dat zij een gevaar vormen op het gebied van terroristische misdrijven of ernstige vormen van criminaliteit die een minstens indirect objectief verband vertonen met de reis van die passagiers, blijkt er, in die omstandigheden, immers geen verband, zelfs geen indirect verband, te bestaan tussen de PNR–gegevens van die passagiers en het door die richtlijn nagestreefde doel, dat de bewaring van diezelfde gegevens zou rechtvaardigen (punt 257).

Het Hof van Justitie laat aan het rechtscollege dat de vragen stelt de zorg over om na te gaan of de wet van 25 december 2016 conform de vereisten van de artikelen 7 en 8 van het Handvest van de grondrechten, in samenhang gelezen met artikel 52, lid 1, van het Handvest, kan worden uitgelegd (punt 261).

B.74.1. Zoals is vermeld in B.72.2, bepaalt artikel 18 van de wet van 25 december 2016 dat de passagiersgegevens worden bewaard in de passagiersgegevensbank voor een maximumtermijn van vijf jaar te rekenen vanaf de registratie ervan, en dat zij na die termijn worden vernietigd.

Die bepaling beperkt zich ertoe een maximale bewaartermijn vast te stellen, zonder de gegevens te identificeren die gedurende die maximale termijn moeten worden bewaard.

Artikel 18 van de wet van 25 december 2016 kan bijgevolg zo worden geïnterpreteerd dat, na de initiële termijn van zes maanden te rekenen vanaf de registratie van de passagiersgegevens in de passagiersgegevensbank, alleen in de passagiersgegevensbank, gedurende een termijn van vijf jaar, de gegevens worden bewaard van de personen voor wie de voorafgaande beoordeling bedoeld in artikel 6, lid 2, *a)*, van de PNR–richtlijn, ofwel de eventuele verificaties uitgevoerd gedurende de termijn van zes maanden bedoeld in artikel 12, lid 2, van die richtlijn, ofwel andere omstandigheden het bestaan hebben aangetoond van objectieve elementen die kunnen aantonen dat een gevaar bestaat op het gebied van terroristische misdrijven of ernstige vormen van criminaliteit met een minstens indirect objectief verband met de reis van die passagiers.

De gegevens die niet zouden voldoen aan die interpretatie, dienen te worden vernietigd.

B.74.2. In de in B.74.1 vermelde interpretatie overschrijdt artikel 18 van de wet van 25 december 2016 de vereisten van het strikt noodzakelijke niet.

B.75. Onder voorbehoud van de in B.74.1 vermelde interpretatie is het middel, in zoverre het is gericht tegen artikel 18 van de wet van 25 december 2016, niet gegrond.

Ten aanzien van het tweede middel

B.76. Het tweede middel, in ondergeschikte orde geformuleerd, is afgeleid uit de schending van artikel 22 van de Grondwet, in samenhang gelezen met artikel 3, lid 2, van het Verdrag betreffende de Europese Unie en met artikel 45 van het Handvest van de grondrechten van de Europese Unie. Dat middel is gericht tegen artikel 3, § 1, artikel 8, § 2, en hoofdstuk 11, dat de artikelen 28 tot 31 bevat, van de wet van 25 december 2016.

De verzoekende partij is van mening dat de bestreden bepalingen, door het PNR-systeem uit te breiden tot de vluchten binnen de Europese Unie, indirect de grenscontroles herinvoeren die in strijd zouden zijn met de vrijheid van verkeer van de personen.

B.77.1. Artikel 3, § 1, van de wet van 25 december 2016 bepaalt :

« Deze wet bepaalt de verplichtingen van de vervoerders en de reisoperatoren inzake de doorgifte van gegevens van passagiers van, naar en op doorreis over het nationaal grondgebied ».

De inhoud van de artikelen 8, § 2, en 28 tot 31 van de wet van 25 december 2016 wordt in herinnering gebracht in B.55.

B.77.2. Ten aanzien van het toepassingsgebied van de wet van 25 december 2016 wordt in de parlementaire voorbereiding uiteengezet :

« De inclusie intra-EU in de verzameling van gegevens zal het mogelijk maken een vollediger beeld te krijgen van de verplaatsingen van passagiers die een potentiële bedreiging vormen voor de intracommunautaire en nationale veiligheid. De praktijk heeft reeds aangetoond dat bepaalde ' *returnees* ' (zogenaamde ' *foreign fighters* ' die terugkeren naar Europa) verscheidene vluchten nemen alvorens aan te komen op hun eindbestemming.

De EU PNR Richtlijn voorziet expliciet de mogelijkheid voor lidstaten om eveneens passagiersgegevens voor internationaal verkeer binnen de Europese Unie te verwerken. Bovendien verklaarden alle Europese lidstaten via een gemeenschappelijke verklaring goedgekeurd op de Raad 21 april 2016 van de ministers van Binnenlandse Zaken en Justitie om de EU PNR richtlijn in nationaal recht om te zetten eveneens voor het intra-EU-verkeer » (*Parl. St.*, Kamer, 2015-2016, DOC 54—2069/001, p. 7).

B.77.3. Zoals eerder is vermeld, staat considerans 10 van de PNR-richtlijn de uitbreiding van het PNR-systeem tot de vluchten binnen de EU toe. Artikel 2 van de PNR-richtlijn regelt de procedure om het toepassingsgebied uit te breiden.

Bij zijn arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022 heeft het Hof van Justitie in dat verband eraan herinnerd dat de uitbreiding van het PNR–systeem voor de vluchten binnen de EU een optie is van de lidstaten om het systeem vastgelegd bij die richtlijn voor de vluchten binnen de EU toe te passen (punt 162), en, zoals is vermeld in B.36.4.1, heeft de Commissie vastgesteld dat alle lidstaten, op één uitzondering na, gebruik hebben gemaakt van die optie.

B.77.4. Wat betreft de uitvoering van die mogelijkheid heeft het Hof van Justitie, bij zijn arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geoordeeld :

« 274. Om te beginnen voorziet artikel 45 van het Handvest in het vrije verkeer van personen, dat overigens een van de fundamentele vrijheden binnen de interne markt is [zie in die zin arrest van 22 juni 2021, Ordre des barreaux francophones et germanophone e.a. (Preventieve maatregelen met het oog op verwijdering), C-718/19, EU:C:2021:505, punt 54].

275. Lid 1 van dit artikel garandeert elke burger van de Unie het recht om zich vrij op het grondgebied van de lidstaten te verplaatsen en er vrij te verblijven. Dit recht stemt volgens de toelichtingen bij het Handvest voor de grondrechten (PB 2007, C 303, blz. 17) overeen met het recht dat door artikel 20, lid 2, eerste alinea, onder *a)*, VWEU wordt gewaarborgd, en vindt overeenkomstig artikel 20, lid 2, tweede alinea, VWEU en artikel 52, lid 2, van het Handvest toepassing onder de voorwaarden en binnen de grenzen die in de Verdragen en de maatregelen ter uitvoering daarvan zijn vastgesteld.

276. Voorts biedt de Unie haar burgers overeenkomstig artikel 3, lid 2, VEU een ruimte van vrijheid, veiligheid en recht zonder binnengrenzen, waarin het vrije verkeer van personen gewaarborgd is in combinatie met passende maatregelen met betrekking tot onder meer controles aan de buitengrenzen en voorkoming en bestrijding van criminaliteit. Evenzo zorgt de Unie er overeenkomstig artikel 67, lid 2, VWEU voor dat aan de binnengrenzen geen personencontroles worden verricht en ontwikkelt zij een gemeenschappelijk beleid op het gebied van onder meer controle aan de buitengrenzen.

277. Volgens vaste rechtspraak van het Hof vormt een nationale wettelijke regeling die bepaalde nationale onderdanen benadeelt louter omdat zij hun recht om in een andere lidstaat vrij te reizen en te verblijven hebben uitgeoefend, een beperking van de vrijheden die elke burger van de Unie op grond van artikel 45, lid 1, van het Handvest geniet (zie in die zin voor artikel 21, lid 1, VWEU, arresten van 8 juni 2017, *Freitag*, C-541/15, EU:C:2017:432, punt 35 en aldaar aangehaalde rechtspraak, en 19 november 2020, ZW, C-454/19, EU:C:2020:947, punt 30).

278. Nationale wetgeving als die in het hoofdgeding, waarbij het systeem van de PNR–richtlijn niet alleen op vluchten naar of vanuit derde landen wordt toegepast maar ook, op grond van artikel 2, lid 1, van deze richtlijn, op vluchten binnen de EU alsook — en daarbij verdergaand dan deze bepaling — op andere soorten vervoer binnen de Unie, resulteert in een systematische en continue doorgifte en verwerking van PNR-gegevens van elke passagier die zijn vrijheid van verkeer uitoefent door zich met deze vervoersmiddelen te verplaatsen binnen de Unie.

279. Zoals in de punten 98 tot en met 111 van het onderhavige arrest is vastgesteld, veroorzaakt het doorgeven en verwerken van passagiersgegevens van vluchten naar of vanuit derde landen en vluchten binnen de EU volgens het systeem van de PNR-richtlijn, een inmenging van een zekere ernst in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de betrokkenen. Deze inmenging is des te ernstiger wanneer dit systeem bij uitbreiding wordt toegepast op andere soorten vervoer binnen de Unie. Om dezelfde redenen als die in de voormelde punten kunnen dergelijke inmengingen ook onderdanen van lidstaten met dergelijke wetgeving en, in het algemeen, Unieburgers die zich met deze transportmiddelen binnen de Unie verplaatsen van en naar dergelijke lidstaten, benadelen en dus ontmoedigen om hun vrijheid van verkeer uit te oefenen in de zin van artikel 45 van het Handvest. Dergelijke wetgeving houdt dan ook een beperking op deze fundamentele vrijheid in.

280. Volgens vaste rechtspraak kan een belemmering van het vrije verkeer van personen enkel worden gerechtvaardigd indien zij gebaseerd is op objectieve overwegingen en evenredig is aan het door het nationale recht rechtmatig nagestreefde doel. Een maatregel is evenredig wanneer hij geschikt is om het nagestreefde doel te verwezenlijken en niet verder gaat dan nodig is om dat doel te bereiken (zie in die zin arrest van 5 juni 2018, *Coman e.a.*, C-673/16, EU:C:2018:385, punt 41 en aldaar aangehaalde rechtspraak).

281. Hieraan dient te worden toegevoegd dat een nationale maatregel die de uitoefening van het vrije verkeer van personen kan belemmeren, slechts kan worden gerechtvaardigd indien deze maatregel in overeenstemming is met de door het Handvest gewaarborgde grondrechten waarvan het Hof de eerbiediging verzekert (arrest van 14 december 2021, *Stolichna obshtina, rayon ' Pancharevo '*, C-490/20, EU:C:2021:1008, punt 58 en aldaar aangehaalde rechtspraak).

282. Volgens de in de punten 115 en 116 van het onderhavige arrest aangehaalde rechtspraak kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande rechten. Bij de beoordeling of lidstaten een beperking op het door artikel 45, lid 1, van het Handvest gewaarborgde grondrecht kunnen rechtvaardigen, moet worden bepaald wat de ernst is van de inmenging die een dergelijke beperking meebrengt, en worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst.

283. Zoals in punt 122 van dit arrest in herinnering is gebracht, is de met de PNR–richtlijn nagestreefde doelstelling van bestrijding van terroristische misdrijven en ernstige criminaliteit beslist een doelstelling van algemeen belang van de Unie.

284. Wat betreft de vraag of nationale wetgeving die is vastgesteld ter omzetting van de PNR-richtlijn en die het systeem van deze richtlijn uitbreidt naar vluchten binnen de EU en ook naar andere soorten vervoer binnen de Unie, geschikt is om het nagestreefde doel te bereiken, blijkt uit de informatie uit het dossier waarover het Hof beschikt dat dankzij PNR-gegevens personen kunnen worden geïdentificeerd die nog niet van terroristische misdrijven of ernstige criminaliteit werden verdacht maar die nader moeten worden onderzocht. Dergelijke nationale wetgeving lijkt dan ook geschikt om het beoogde doel van bestrijding van terroristische misdrijven en ernstige criminaliteit te bereiken.

285. Wat de vraag naar de noodzakelijkheid van dergelijke wetgeving betreft, zij erop gewezen dat de lidstaten de hun door artikel 2, lid 1, van de PNR-richtlijn, gelezen in het licht van de artikelen 7 en 8 van het Handvest, geboden mogelijkheid slechts mogen uitoefenen in de mate van wat strikt noodzakelijk is om dat doel te bereiken, gelet op de vereisten genoemd in de punten 163 tot en met 174 van dit arrest.

286. Deze vereisten gelden des te meer wanneer het systeem van de PNR-richtlijn wordt toegepast op andere vervoersmiddelen binnen de Unie ».

B.77.5. Zoals het Hof heeft geoordeeld in B.40, verantwoordt het reële karakter van de terroristische dreiging, met name in het licht van de geografische situering van het land, dat het PNR–systeem wordt toegepast op verschillende vervoermiddelen binnen de grenzen van de Unie.

Om dezelfde redenen dient ervan te worden uitgegaan dat de beperking van de vrijheid van verkeer waartoe de wet van 25 december 2016 zou leiden, verantwoord wordt door het feit dat het PNR–systeem, toegepast op de vluchten binnen de EU, en uitgebreid tot andere vervoermiddelen, bijdraagt aan het doel inzake de bestrijding van terroristische misdrijven en ernstige vormen van criminaliteit dat met de PNR–richtlijn wordt nagestreefd, wat ongetwijfeld een doel van algemeen belang van de Unie is, en dat het PNR–systeem de grenzen van het strikt noodzakelijke niet overschrijdt.

B.77.6. Het middel, in zoverre het is gericht tegen artikel 3, § 1, van de wet van 25 december 2016, is niet gegrond.

B.78.1. Artikel 8, § 2, van de wet van 25 december 2016 laat toe de PNR–gegevens te verwerken ter verbetering van de controles van personen aan de buitengrenzen, en inzonderheid ter bestrijding van illegale immigratie, onder de voorwaarden bepaald in hoofdstuk 11 (artikelen 28 tot 31) van de wet van 25 december 2016.

B.78.2.1. Op een vraag van het Hof over het toepassingsgebied van de API-richtlijn heeft het Hof van Justitie, bij zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geoordeeld :

« 263. Met zijn negende vraag, onder *a)*, wenst de verwijzende rechter in wezen te vernemen of de API-richtlijn geldig is in het licht van artikel 3, lid 2, VEU en artikel 45 van het Handvest, er daarbij van uitgaande dat de bij deze richtlijn opgelegde verplichtingen gelden voor vluchten binnen de EU.

264. Zoals de advocaat-generaal in punt 277 van zijn conclusie heeft aangegeven en de Raad, de Commissie en verschillende regeringen hebben opgemerkt, is deze premisse echter onjuist.

265. Artikel 3, lid 1, van de API-richtlijn bepaalt namelijk dat de lidstaten de nodige maatregelen moeten nemen om vervoerders te verplichten aan de autoriteiten die belast zijn met de controle van personen aan de buitengrenzen, vóór het eind van de instapcontroles desgevraagd informatie te verstrekken over de passagiers die zij zullen vervoeren naar een aangewezen grensdoorlaatpost via welke deze personen het grondgebied van een lidstaat binnenkomen. Deze gegevens worden volgens artikel 6, lid 1, van deze richtlijn verstrekt aan de autoriteiten die belast zijn met de controle aan de buitengrenzen via welke de passagier dit grondgebied zal binnenkomen, en worden onder de in deze bepaling genoemde voorwaarden verwerkt.

266. Uit deze bepalingen, gelezen in het licht van artikel 2, onder *a)*, *b)* en *d)*, van de API–richtlijn, waarin de begrippen ‘ vervoerder ’, ‘ buitengrenzen ’ en ‘ grensdoorlaatpost ’ worden gedefinieerd, blijkt duidelijk dat deze richtlijn luchtvaartmaatschappijen enkel verplicht de in artikel 3, lid 2, ervan bedoelde gegevens door te geven aan de met de controle van de buitengrenzen belaste autoriteiten indien passagiers worden gevlogen naar een aangewezen doorlaatpost aan de buitengrenzen van een lidstaat met een derde land, en dat enkel voor deze vluchten gegevens worden verwerkt.

267. Deze richtlijn legt geen enkele verplichting op voor gegevens van passagiers die enkel over interne grenzen van de lidstaten vliegen.

268. Hieraan moet worden toegevoegd dat de PNR-richtlijn, zoals uit overweging 9 en artikel 8, lid 2, ervan blijkt, de in artikel 3, lid 2, van de API-richtlijn genoemde gegevens die overeenkomstig deze richtlijn worden verzameld en door bepaalde luchtvaartmaatschappijen worden bewaard, tot PNR-gegevens rekent, en de lidstaten de mogelijkheid biedt om de PNR–richtlijn op grond van artikel 2 ervan toe te passen op door hen aan te wijzen vluchten binnen de EU. De PNR-richtlijn heeft dus niets veranderd aan de draagwijdte van de bepalingen van de API-richtlijn of aan de uit deze richtlijn voortvloeiende beperkingen.

269. Gelet op het voorgaande dient op de negende vraag, onder *a)*, te worden geantwoord dat de API-richtlijn aldus moet worden uitgelegd dat zij niet van toepassing is op vluchten binnen de EU ».

B.78.2.2. Uit het voorgaande blijkt dat het Hof van Justitie bevestigt dat het feit dat, voor de PNR–richtlijn, de API-gegevens tot de PNR–gegevens worden gerekend, niets verandert aan de draagwijdte van de bepalingen van de API-richtlijn, noch aan de beperkingen die voortvloeien uit die richtlijn, die zo moet worden geïnterpreteerd dat zij niet van toepassing is op de vluchten binnen de EU (punten 268-269). Zoals in B.54.2 is vermeld, is het Hof van Justitie immers van oordeel dat de verwerking van de API–gegevens alleen betrekking kan hebben op de passagiers die de buitengrenzen van de Unie met derde landen overschrijden, zo niet zou ze een gelijke werking hebben als de controles aan de buitengrenzen met derde landen (punt 290).

B.78.3. Daarenboven dient rekening te worden gehouden met punt 235 van het voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, waarbij het Hof van Justitie van oordeel is dat « het exhaustieve karakter van de doelstellingen in artikel 1, lid 2, van de PNR–richtlijn [...] ook [impliceert] dat PNR–gegevens niet mogen worden bewaard in één databank die zowel voor deze als voor andere doeleinden kan worden geraadpleegd. Dit zou immers het risico inhouden dat de gegevens worden gebruikt voor andere doeleinden dan de in artikel 1, lid 2, genoemde ».

Het is trouwens door zich te baseren op de onverenigbaarheid van één enkele databank met de vereisten van het strikt noodzakelijke dat het Hof van Justitie heeft geoordeeld, zoals in B.54.2 is vermeld, dat de verwerking van de PNR–gegevens voor andere doeleinden dan die waarin de PNR–richtlijn voorziet, met name, voor het verbeteren van de grenscontroles en het bestrijden van illegale immigratie, het exhaustieve karakter van de opsomming van de met de verwerking van de PNR–gegevens nagestreefde doeleinden aantast (punt 288), waardoor de lidstaten wordt belet één enkele databank op te richten met daarin zowel de PNR–gegevens die krachtens de PNR–richtlijn zijn verzameld, als de gegevens bedoeld in artikel 3, lid 2, van de « API–richtlijn », met name wanneer die databank kan worden geraadpleegd niet alleen voor de in artikel 1, lid 2, van de PNR–richtlijn genoemde doeleinden, maar tevens voor andere doeleinden (punt 289).

B.78.4. Ten aanzien van het bestaan van één enkele databank die zowel de PNR–gegevens als de API–gegevens bevat, is het niet mogelijk om het toepassingsgebied van de artikelen 28 tot 31 van de wet van 25 december 2016 uit te leggen op een wijze die bestaanbaar is met het Unierecht.

B.78.5. Door, in het kader van het PNR–systeem, de verwerking van de API–gegevens, bedoeld in artikel 9, § 1, 18°, van de wet van 25 december 2016, toe te staan voor de vluchten binnen de EU, schenden de artikelen 28 tot 31, die hoofdstuk 11 vormen, van de wet van 25 december 2016 de in het middel beoogde bepalingen, en dienen zij te worden vernietigd. Artikel 8, § 2, van de wet van 25 december 2016, dat onlosmakelijk verbonden is met die bepalingen, dient eveneens te worden vernietigd.

B.78.6. Het staat aan de wetgever de verzameling van de API–gegevens in een van de « PNR–gegevensbank » onderscheiden gegevensbank te organiseren, onder de voorwaarden die voldoen aan de doeleinden, de beperkingen en het toepassingsgebied van de verplichtingen die voortvloeien uit de API-richtlijn.

B.79. Het middel, in zoverre het is gericht tegen de artikelen 8, § 2, en 28 tot 31 van de wet van 25 december 2016, is gegrond.

Ten aanzien van de draagwijdte van de vernietiging

B.80.1. Het Hof heeft de middelen gegrond bevonden in zoverre zij de volgende artikelen beogen :

- artikel 8, § 1, 4°, en artikel 8, § 2, van de wet van 25 december 2016;

- artikel 27 van de wet van 25 december 2016, in zoverre het, behalve in naar behoren gerechtvaardigde dringende gevallen, de verstrekking van de PNR–gegevens met het oog op een beoordeling achteraf, niet afhankelijk maakt van een voorafgaande controle die wordt uitgevoerd door ofwel een rechtscollege, ofwel een « onafhankelijke bestuurlijke entiteit », naar aanleiding van een gemotiveerd verzoek van de bevoegde autoriteiten;

- de artikelen 28 tot 31 van de wet van 25 december 2016 en

- artikel 51 van de wet van 25 december 2016.

B.80.2. De voormelde bepalingen dienen derhalve te worden vernietigd, in de mate van het gegronde karakter van de middelen.

B.81.1. Die vernietiging heeft tot gevolg dat de bepalingen van de wet van 25 december 2016 of andere wetsbepalingen die zouden verwijzen naar de vernietigde bepalingen, in die mate, zonder voorwerp worden.

B.81.2. Die vernietiging heeft tevens tot gevolg dat de verwerkingen van de gegevens die zijn uitgevoerd op basis van de vernietigde doeleinden of de verstrekkingen van gegevens die zijn uitgevoerd zonder voorafgaande controle, als onwettig dienen te worden beschouwd.

De identificatie van de onwettige verwerkingen is mogelijk daar artikel 23, § 1, van de wet van 25 december 2016 voorziet in een « oplijsting » die in artikel 4, 11°, van dezelfde wet wordt gedefinieerd als « het mechanisme bedoeld in artikel 23, § 2, dat toelaat de uitgevoerde gegevensverwerkingen op te sporen, opdat het identificeerbaar is welke persoon, op welk moment, welke gegevens heeft geraadpleegd en met welk doel ».

Die oplijsting laat aldus toe de verwerkingen te identificeren die het « strikt noodzakelijke » zouden overschrijden.

B.81.3. Voor het overige doet die gedeeltelijke vernietiging van de wet van 25 december 2016 geen afbreuk aan de andere verwerkingen van passagiersgegevens.

Ten aanzien van de handhaving van de gevolgen

B.82.1. Artikel 8, derde lid, van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof bepaalt :

« Zo het Hof dit nodig oordeelt, wijst het, bij wege van algemene beschikking, die gevolgen van de vernietigde bepalingen aan welke als gehandhaafd moeten worden beschouwd of voorlopig gehandhaafd worden voor de termijn die het vaststelt ».

B.82.2. Het Hof dient ter zake rekening te houden met de beperkingen die uit het recht van de Europese Unie voortvloeien inzake de handhaving van de gevolgen van nationale normen die dienen te worden vernietigd omdat zij in strijd zijn met dat recht (HvJ, grote kamer, 8 september 2010, C—409/06, *Winner Wetten*, punten 53-69; HvJ, grote kamer, 28 februari 2012, C—41/11, *Inter-Environnement Wallonie* en *Terre wallonne*, punten 56-63).

In de regel kan dit enkel onder de voorwaarden die door het Hof van Justitie in antwoord op een prejudiciële vraag worden vastgesteld.

B.83.1. Op de vraag van het Hof over een eventuele handhaving van de gevolgen van de bestreden wet heeft het Hof van Justitie, bij zijn voormelde arrest in zake *Ligue des droits humains t. Ministerraad* van 21 juni 2022, geoordeeld :

« 293. Het beginsel van voorrang van het Unierecht houdt in dat dit recht voorrang heeft op het recht van de lidstaten. Dit beginsel verplicht dus alle instanties van de lidstaten om volle werking te verlenen aan de verschillende bepalingen van het Unierecht, aangezien het recht van de lidstaten niet kan afdoen aan de werking die op het grondgebied van die staten aan deze bepalingen is verleend. Dit beginsel brengt mee dat, indien nationale wetgeving niet in overeenstemming met de vereisten van het Unierecht kan worden uitgelegd, de nationale rechter die in het kader van zijn bevoegdheid is belast met de toepassing van de bepalingen van het Unierecht, verplicht is de volle werking van deze bepalingen te verzekeren en daarbij zo nodig, op eigen gezag, elke, zelfs latere, strijdige bepaling van de nationale wetgeving buiten toepassing te laten, zonder dat hij de voorafgaande opheffing hiervan via de wetgeving of enige andere constitutionele procedure hoeft te vragen of af te wachten (arresten van 15 juli 1964, *Costa*, 6/64, EU:C:1964:66, blz. 1159 en 1160; 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C—512/18 en C-520/18, EU:C:2020:791, punten 214 en 215, en 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 118).

294. Enkel het Hof kan, bij wijze van uitzondering en om dwingende redenen van rechtszekerheid, een voorlopige opschorting toestaan van het effect dat een regel van het Unierecht op het daarmee strijdige nationale recht heeft, namelijk de terzijdestelling daarvan. Een dergelijke beperking in de tijd van de werking van de door het Hof aan het Unierecht gegeven uitlegging kan slechts worden vastgesteld in het arrest waarin de gevraagde uitlegging wordt gegeven. Aan de voorrang en de uniforme toepassing van het Unierecht zou afbreuk worden gedaan indien de nationale rechterlijke instanties bevoegd waren om, al was het maar tijdelijk, aan nationale bepalingen voorrang te geven boven het Unierecht waarmee deze bepalingen in strijd zijn (arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C—140/20, EU:C:2022:258, punt 119 en aldaar aangehaalde rechtspraak).

295. Anders dan de niet-nakoming van een procedurele verplichting als de voorafgaande beoordeling van de gevolgen van een project voor het milieu, waarover het ging in de zaak die heeft geleid tot het arrest van 29 juli 2019, *Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen* (C-411/17, EU:C:2019:622, punten 175, 176, 179 en 181), en waarin het Hof een voorlopige opschorting heeft toegestaan van voormeld effect van terzijdestelling, kan een schending van de bepalingen van de PNR-richtlijn, gelezen in het licht van de artikelen 7, 8 en 45 en artikel 52, lid 1, van het Handvest, niet worden geregulariseerd via een procedure die vergelijkbaar is met die welke in die zaak werd aanvaard. Handhaving van de gevolgen van nationale wetgeving als de wet van 25 december 2016 zou immers betekenen dat die regeling luchtvaartmaatschappijen, andere vervoerders en reisoperatoren verplichtingen blijft opleggen die in strijd zijn met het Unierecht en die leiden tot ernstige inmengingen in de grondrechten van de personen van wie de gegevens zijn doorgegeven, bewaard en verwerkt en tot beperkingen op hun vrijheid van verkeer die verder gaan dan noodzakelijk is (zie naar analogie arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 122 en aldaar aangehaalde rechtspraak).

296. Bijgevolg mag de verwijzende rechter niet de werking in de tijd beperken van een door hem op grond van het nationale recht uit te spreken ongeldigverklaring van de in het hoofdgeding aan de orde zijnde nationale wetgeving (zie naar analogie arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 123 en aldaar aangehaalde rechtspraak).

297. Voor zover de verwijzende rechter zich tot slot afvraagt wat de gevolgen zijn van de vaststelling van een eventuele onverenigbaarheid van de wet van 25 december 2016 met de PNR–richtlijn, gelezen in het licht van het Handvest, voor de ontvankelijkheid en het gebruik in strafprocedures van de bewijzen en inlichtingen die via de door de vervoerders en reisoperatoren doorgegeven gegevens zijn verkregen, volstaat het te verwijzen naar de rechtspraak van het Hof hierover en met name naar de beginselen in de punten 41 tot en met 44 van het arrest van 2 maart 2021, *Prokuratuur* (Voorwaarden voor toegang tot elektronische-communicatiegegevens) (C—746/18, EU:C:2021:152), waaruit blijkt dat die ontvankelijkheidskwestie overeenkomstig het beginsel van de procedurele autonomie van de lidstaten onder het nationale recht valt, op voorwaarde dat met name de beginselen van gelijkwaardigheid en doeltreffendheid worden geëerbiedigd (zie naar analogie arrest van 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 127).

298. Gelet op de voorgaande overwegingen dient op de tiende vraag te worden geantwoord dat het Unierecht aldus moet worden uitgelegd dat het zich ertegen verzet dat een nationale rechter de werking in de tijd beperkt van de ongeldigverklaring, die hij op grond van het nationale recht dient uit te spreken, van nationale wetgeving die luchtvaartmaatschappijen, spoorwegvervoerders, wegvervoerders en reisoperatoren verplicht om PNR-gegevens door te geven en die een verwerking en bewaring van deze gegevens voorschrijft die onverenigbaar is met de bepalingen van de PNR-richtlijn, gelezen in het licht van artikel 3, lid 2, VEU, artikel 67, lid 2, VWEU en de artikelen 7, 8 en 45 en artikel 52, lid 1, van het Handvest. De ontvankelijkheid van de op deze manier verkregen bewijzen is een kwestie die overeenkomstig het beginsel van de procedurele autonomie van de lidstaten onder het nationale recht valt, op voorwaarde dat met name de beginselen van gelijkwaardigheid en doeltreffendheid worden geëerbiedigd ».

B.83.2. Uit het voormelde arrest blijkt dat het Hof de gevolgen van de vernietigde bepalingen niet voorlopig vermag te handhaven.

Zoals is vermeld in B.81, brengt die beperkte vernietiging de verwerkingen die zijn uitgevoerd overeenkomstig de in de middelen aangevoerde grondwets– en verdragsbepalingen niet in het geding.

B.83.3. Het staat aan de bevoegde strafrechter, in voorkomend geval, uitspraak te doen over de toelaatbaarheid van de bewijzen die werden verzameld bij de tenuitvoerlegging van de vernietigde bepalingen, overeenkomstig artikel 32 van de voorafgaande titel van het Wetboek van stafvordering en in het licht van de door het Hof van Justitie in het voormelde arrest van 21 juni 2022 aangebrachte verduidelijkingen.

Om die redenen,

het Hof

- vernietigt artikel 8, § 1, 4°, en § 2, van de wet van 25 december 2016 « betreffende de verwerking van passagiersgegevens »;

- vernietigt artikel 27 van de voormelde wet van 25 december 2016, in zoverre het, behalve in naar behoren gerechtvaardigde dringende gevallen, de verstrekking van de PNR–gegevens met het oog op een beoordeling achteraf, niet ondergeschikt maakt aan een voorafgaande controle die wordt uitgevoerd ofwel door een rechtscollege, ofwel door een onafhankelijke bestuurlijke entiteit, naar aanleiding van een gemotiveerd verzoek van de bevoegde autoriteiten;

- vernietigt de artikelen 28 tot 31 van de wet van 25 december 2016;

- vernietigt artikel 16/3 van de wet van 30 november 1998 « houdende regeling van de inlichtingen– en veiligheidsdiensten », zoals ingevoegd bij artikel 51 van de voormelde wet van 25 december 2016;

- onder voorbehoud van de interpretaties vermeld in B.33.2 tot B.33.5, B.49, B.63.2.3, B.63.3.2, B.63.4.1, B.69.1 en B.74.1, en rekening houdend met hetgeen is vermeld in B.40.3.2, in B.40.3.3 en in B.61.2.2, verwerpt het beroep voor het overige.

Aldus gewezen in het Frans, het Nederlands en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 12 oktober 2023.

De griffier, De voorzitter,

F. Meersschaut P. Nihoul

VERFASSUNGSGERICHTSHOF

[C − 2023/46645]

Auszug aus dem Entscheid Nr. 131/2023 vom 12. Oktober 2023

Geschäftsverzeichnisnummer 6713

In Sachen: Klage auf völlige oder teilweise Nichtigerklärung des Gesetzes vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten », erhoben von der VoG « Ligue des Droits de l'Homme » (nunmehr « Ligue des droits humains »).

Der Verfassungsgerichtshof,

zusammengesetzt aus dem Präsidenten P. Nihoul, der vorsitzenden Richterin J. Moerman, und den Richtern T. Giet, M. Pâques, Y. Kherbache, D. Pieters, S. de Bethune, E. Bribosia, W. Verrijdt und K. Jadin, unter Assistenz des Kanzlers F. Meersschaut, unter dem Vorsitz des Präsidenten P. Nihoul,

erlässt nach Beratung folgenden Entscheid:

I. *Gegenstand der Klage und Verfahren*

Mit einer Klageschrift, die dem Gerichtshof mit am 24. Juli 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 26. Juli 2017 in der Kanzlei eingegangen ist, erhob die VoG « Ligue des Droits de l'Homme » (nunmehr « Ligue des droits humains »), unterstützt und vertreten durch RÄin C. Forget, in Brüssel zugelassen, Klage auf völlige oder teilweise (Artikel 3 § 1, 8 § 2 und Kapitel 11) Nichtigerklärung des Gesetzes vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten » (veröffentlicht im *Belgischen Staatsblatt* vom 25. Januar 2017).

In seinem Zwischenentscheid Nr. 135/2019 vom 17. Oktober 2019 (ECLI:BE:GHCC:2019:ARR.135), veröffentlicht im *Belgischen Staatsblatt* vom 6. März 2020, hat der Verfassungsgerichtshof dem Gerichtshof der Europäischen Union folgende Vorabentscheidungsfragen gestellt:

« 1. Ist Artikel 23 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 ' zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG ' (Datenschutz-Grundverordnung - DSGVO) in Verbindung mit Artikel 2 Absatz 2 Buchstabe d dieser Verordnung so auszulegen, dass er auf einzelstaatliche Rechtsvorschriften wie das Gesetz vom 25. Dezember 2016 ' über die Verarbeitung von Passagierdaten ', mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 ' über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität ', sowie die Richtlinie 2004/82/EG des Rates vom 29. April 2004 ' über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln ' und die Richtlinie 2010/65/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 ' über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG ' umgesetzt wird, anwendbar ist?

2. Ist Anhang I der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union in dem Sinne vereinbar, dass die darin aufgeführten Daten sehr weitgehend sind – insbesondere die in Nummer 18 von Anhang I der Richtlinie (EU) 2016/681 erwähnten Daten, die über die in Artikel 3 Absatz 2 der Richtlinie 2004/82/EG erwähnten Daten hinausgehen – insofern sie zusammen genommen sensible Daten offenlegen könnten und so über das ' absolut Notwendige ' hinausgehen könnten?

3. Sind die Nummern 12 und 18 von Anhang I der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern unter Berücksichtigung des Wortes ' einschließlich ' die dort aufgeführten Daten in beispielhafter und nicht erschöpfender Weise genannt werden, was somit gegen die Anforderung der Präzision und Klarheit der Regeln, die einen Eingriff in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten nach sich ziehen, verstoßen könnte?

4. Sind Artikel 3 Nummer 4 der Richtlinie (EU) 2016/681 und Anhang I derselben Richtlinie mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern das System zur allgemeinen Erhebung, Übermittlung und Verarbeitung von Passagierdaten, das mit diesen Bestimmungen eingeführt wird, auf jede Person abzielt, die das betreffende Beförderungsmittel benutzt, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von dieser Person eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

5. Ist Artikel 6 der Richtlinie (EU) 2016/681 in Verbindung mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das als Verarbeitungszweck der PNR-Daten die Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste zulässt und so diesen Zweck in die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität aufnimmt?

6. Ist Artikel 6 der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern die in ihm geregelte Vorabüberprüfung durch eine Korrelation mit Datenbanken und im Voraus festgelegten Kriterien systematisch und allgemein auf die Passagierdaten angewandt wird, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von diesen Fluggästen eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

7. Kann der in Artikel 12 Absatz 3 der Richtlinie (EU) 2016/681 erwähnte Ausdruck ' andere nationale Behörde, die [...] zuständig ist ' dahin ausgelegt werden, dass er sich auf die PNR-Zentralstelle bezieht, die durch das Gesetz vom 25. Dezember 2016 geschaffen wurde und die somit den Zugriff auf die PNR-Daten nach einer sechsmonatigen Frist im Rahmen von gezielten Recherchen gestatten dürfte?

8. Ist Artikel 12 der Richtlinie (EU) 2016/681 in Verbindung mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das eine allgemeine Aufbewahrungsdauer für die Daten von fünf Jahren vorsieht, ohne eine Unterscheidung danach vorzunehmen, ob sich im Rahmen der Vorabüberprüfung herausstellt, dass die betroffenen Fluggäste ein Risiko für die öffentliche Sicherheit darstellen können oder nicht?

9. *a)* Ist die Richtlinie 2004/82/EG mit Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 45 der Charta der Grundrechte der Europäischen Union vereinbar, insofern die Pflichten, die sie einführt, für Flüge innerhalb der Europäischen Union gelten?

b) Ist die Richtlinie 2004/82/EG in Verbindung mit Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 45 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass sie einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das zum Zwecke der Bekämpfung der illegalen Einwanderung und der Verbesserung der Grenzkontrollen ein System zur Erhebung und Verarbeitung der Daten ' zu den in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet ' beförderten Passagieren gestattet, was indirekt eine Wiedereinführung von Kontrollen an den Binnengrenzen bedeuten könnte?

10. Könnte der Verfassungsgerichtshof, falls er auf der Grundlage der Antworten auf die vorstehenden Vorabentscheidungsfragen zu dem Schluss gelangen sollte, dass das angefochtene Gesetz, mit dem insbesondere die Richtlinie (EU) 2016/681 umgesetzt wird, gegen eine oder mehrere der Verpflichtungen verstößt, die sich aus den in diesen Fragen genannten Bestimmungen ergeben, die Folgen des Gesetzes vom 25. Dezember 2016 ' über die Verarbeitung von Passagierdaten ' vorläufig aufrechterhalten, um eine Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch das Gesetz angestrebten Ziele benutzt werden können? ».

In seinem Urteil vom 21. Juni 2022 in der Rechtssache C-817/19 (ECLI:EU:C:2022:491) hat der Gerichtshof der Europäischen Union auf die Fragen geantwortet.

Durch Anordnung vom 13. Juli 2022 hat der Gerichtshof nach Anhörung der referierenden Richter T. Giet und W. Verrijdt beschlossen,

- die Verhandlung wiederzueröffnen,

- die Parteien aufzufordern, in einem spätestens am 30. September 2022 einzureichenden und innerhalb derselben Frist den jeweils anderen Parteien zu übermittelnden Ergänzungsschriftsatz ihren Standpunkt zu den Auswirkungen des vorerwähnten Urteils des Gerichtshofes der Europäischen Union auf die Nichtigkeitsklage zu äußern, und zwar insbesondere:

a) in Bezug darauf, wie es sich auf die Fortsetzung der Prüfung der Nichtigkeitsklage vor dem Gerichtshof auswirkt, insbesondere die Erwägungen:

- zur Verknüpfung der PNR-Richtlinie und der DSGVO;

- zum Anwendungsbereich der Erhebung und der Verarbeitung der PNR-Daten (erfasste Daten, Zielsetzungen und erwähnte Verstöße, betroffene Flüge);

- zu den Garantien im Zusammenhang mit der Verarbeitung der PNR-Daten (Vorabüberprüfung, automatisierte Verarbeitung, Zugriff auf die PNR-Daten, Begriff der « unabhängigen nationalen Behörde », Speicherfrist der PNR-Daten);

- zur fehlenden Möglichkeit einer Aufrechterhaltung der Folgen im Fall einer teilweisen Nichtigerklärung des Gesetzes vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten »;

b) in Bezug auf die konkret untermauerten Rechtfertigungen und Bedingungen für die auf das « absolut Notwendige » beschränkte Beschaffenheit und die Übereinstimmung von jedem einzelnen der oben genannten Elemente, wie sie im vorliegenden Fall im Gesetz vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten » vorgesehen sind, mit der Auslegung der PNR-Richtlinie;

- dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und

- dass vorbehaltlich eines solchen Antrags die Verhandlung am 5. Oktober 2022 geschlossen und die Rechtssache zur Beratung gestellt wird.

(...)

II. *Rechtliche Würdigung*

(...)

In Bezug auf das angefochtene Gesetz und dessen Kontext

B.1. Die durch die VoG « Ligue des Droits de l'Homme » (nunmehr « Ligue des droits humains ») eingereichte Nichtigkeitsklage richtet sich gegen das Gesetz vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten » (nachstehend: Gesetz vom 25. Dezember 2016), das eine Verpflichtung für die Beförderungsunternehmen und Reiseunternehmen festlegt, die Daten zu Passagieren, die sogenannten « PNR-Daten » (*Passenger Name Record*), zu übermitteln.

B.2.1. Nach Artikel 2 setzt das Gesetz vom 25. Dezember 2016 drei europäische Richtlinien um.

B.2.2. Zunächst wird mit dem Gesetz vom 25. Dezember 2016 die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 « über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität » (nachstehend: PNR-Richtlinie) umgesetzt.

Die PNR-Richtlinie sieht die Erhebung und Übermittlung der Fluggastdatensätze von Drittstaatsflügen durch die Fluggesellschaften zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität vor. Diese Richtlinie gilt für die Verarbeitung von PNR-Daten im Bereich des Luftverkehrs, gemäß ihrem Erwägungsgrund 33 schließt sie jedoch die Möglichkeit der Mitgliedstaaten nicht aus, den darin vorgesehenen PNR-Mechanismus nach ihrem jeweiligen nationalen Recht auf andere Beförderungsmittel oder auf andere Wirtschaftsteilnehmer als die Beförderungsunternehmen auszudehnen. Außerdem kann die PNR-Richtlinie gemäß ihrem Artikel 2 auch auf Flüge innerhalb der Europäischen Union angewandt werden.

B.2.3. Mit dem Gesetz vom 25. Dezember 2016 wird außerdem die Richtlinie 2004/82/EG des Rates vom 29. April 2004 « über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln » (nachstehend: API-Richtlinie) umgesetzt.

So regelt es die Verwendung von Passagierdaten für die in der Richtlinie 2004/82/EG vorgesehenen Zwecke, indem es den Inhalt des königlichen Erlasses vom 11. Dezember 2006 « über die Verpflichtung von Fluggesellschaften, Angaben über die beförderten Personen zu übermitteln » (nachstehend: königlicher Erlass vom 11. Dezember 2006) wiederaufnimmt.

B.2.4. Mit dem Gesetz vom 25. Dezember 2016 wird schließlich teilweise die Richtlinie 2010/65/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 « über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG » (nachstehend: Richtlinie 2010/65/EU) umgesetzt. Zweck dieser Richtlinie ist die Vereinfachung und Harmonisierung der Verwaltungsverfahren im Seeverkehr durch die allgemeine Nutzung elektronischer Systeme für die Datenübermittlung und durch die Rationalisierung der Meldeformalitäten (Artikel 1 Absatz 1).

B.3.1. Das Gesetz vom 25. Dezember 2016 zielt darauf ab, « einen rechtlichen Rahmen zu schaffen, um es verschiedenen Sektoren der internationalen Personenbeförderung (Flug-, Schienen-, internationaler Straßen- und Seeverkehr) und Reiseunternehmen aufzuerlegen, ihre Passagierdaten an eine vom FÖD Inneres verwaltete Datenbank zu übermitteln (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 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) » (ebenda, SS. 5-6).

B.3.2. Das durch die PNR-Richtlinie eingeführte System zur Erhebung der Daten vervollständigt das durch die API-Richtlinie geschaffene System, da die PNR-Daten umfassender sind als die API-Daten:

« 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 » (ebenda, SS. 6-7).

B.3.3. Die Verpflichtung zur Übermittlung der Passagierdaten gilt « sowohl für internationale Flüge, für internationale Hochgeschwindigkeitszüge, für den internationalen Charterverkehr mit Reisebussen und den Seeverkehr aus und in die Europäische Union als auch für Beförderungen in und aus der Europäischen Union » (ebenda, S. 7) gemäß der in Artikel 2 der PNR-Richtlinie vorgesehenen Möglichkeit.

Außerdem ist die gesetzliche Verpflichtung zur Übermittlung der Passagierdaten im Einklang mit der von der PNR-Richtlinie gebotenen Möglichkeit, diese Verpflichtung auch anderen Wirtschaftsteilnehmern als Beförderungsunternehmen aufzuerlegen, nicht nur auf die in der PNR-Richtlinie genannten Beförderungsunternehmen, sondern auch auf Reiseunternehmen anwendbar (ebenda, S. 8).

B.4.1. Artikel 4 Nr. 9 des Gesetzes vom 25. Dezember 2016 definiert « PNR » als « den Datensatz mit den zu jedem einzelnen Passagier notwendigen Reisedaten, der die in Artikel 9 erwähnten Informationen enthält, die die Bearbeitung und Überprüfung der von einer Person oder in ihrem Namen getätigten Reservierungen für jede Reise durch die buchenden und beteiligten Beförderungsunternehmen und Reiseunternehmen ermöglichen, unabhängig davon, ob dieser Datensatz in Buchungssystemen, Abfertigungssystemen (zur Überprüfung der Passagiere beim Anbordgehen) oder gleichwertigen Systemen, die die gleichen Funktionen bieten, enthalten ist ».

Was die Daten des Einscheckstatus und des Anbordgehens betrifft, so sind die unter Artikel 9 § 1 Nr. 18 erwähnten erweiterten Passagierdaten (API-Daten –*Advanced Passenger Information*) erschöpfend in den 16 Nummern von Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 aufgezählt.

Was die Buchungsdaten betrifft, so enthalten die Passagierdaten (PNR-Daten –*Passenger Name Record*) höchstens die neunzehn Bestandteile, die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 erschöpfend aufgezählt sind, darunter die in Artikel 9 § 1 Nr. 18 erwähnten API-Daten.

B.4.2. Nach Artikel 5 des Gesetzes vom 25. Dezember 2016 werden die PNR-Daten von den Beförderungsunternehmen und Reiseunternehmen erhoben und übermittelt, damit sie in der in Artikel 15 erwähnten Passagierdatenbank, die von der im Föderalen Öffentlichen Dienst Inneres geschaffenen PNR-Zentralstelle verwaltet wird, gespeichert werden (Artikel 12 ff.). Die Passagiere werden darüber informiert, dass ihre Daten der PNR-Zentralstelle übermittelt werden und später zu den in Artikel 8 erwähnten Zwecken verarbeitet werden können (Artikel 6).

Die Zwecke der Verarbeitung der PNR-Daten sind in Artikel 8 des Gesetzes vom 25. Dezember 2016 aufgelistet: Es handelt sich einerseits um die Ermittlung und Verfolgung von Straftaten (Artikel 8 § 1) und andererseits unter den in Kapitel 11 erwähnten Bedingungen um die Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung (Artikel 8 § 2).

Im Rahmen der in Artikel 8 § 1 erwähnten Zwecke sieht Artikel 16 des Gesetzes vom 25. Dezember 2016 vor, dass die Passagierdatenbank der PNR-Zentralstelle für die in den Artikeln 24 bis 27 erwähnten Verarbeitungen gemäß den Bestimmungen in Kapitel 9 direkt zugänglich ist.

Im Rahmen der in Artikel 8 § 2 erwähnten Zwecke werden nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten (API-Daten) in Bezug auf die in Artikel 29 § 2 des Gesetzes vom 25. Dezember 2016 erwähnten Kategorien von Passagieren übermittelt.

Die Aufbewahrungsdauer der Daten ist in den Artikeln 18 ff. des Gesetzes vom 25. Dezember 2016 geregelt.

In Bezug auf den Umfang der Klage

B.5.1. Der Gerichtshof muss die Tragweite der Nichtigkeitsklage auf der Grundlage des Inhalts der Klageschrift bestimmen.

Der Gerichtshof kann nur ausdrücklich angefochtene Gesetzesbestimmungen für nichtig erklären, gegen die Klagegründe angeführt werden, sowie gegebenenfalls Bestimmungen, die nicht angefochten werden, jedoch untrennbar mit den für nichtig zu erklärenden Bestimmungen verbunden sind.

B.5.2. Die klagende Partei beantragt zwar mit ihrem ersten Klagegrund die Nichtigerklärung des gesamten Gesetzes vom 25. Dezember 2016, aber aus der Begründung des Klagegrunds geht hervor, dass sich die Beschwerdegründe nur gegen Artikel 3 § 2, Artikel 4 Nr. 9 und 10, Artikel 7 bis 9, Artikel 12 bis 16, Artikel 18, Artikel 24 bis 27, Artikel 50 und Artikel 51 des Gesetzes vom 25. Dezember 2016 richten. Folglich ist die Nichtigkeitsklage nur in diesem Maße zulässig.

Der zweite, hilfsweise vorgebrachte Klagegrund richtet sich gegen Artikel 3 § 1, Artikel 8 § 2 und Kapitel 11 des Gesetzes vom 25. Dezember 2016, das die Artikel 28 bis 31 umfasst.

B.5.3. Sollte sich bei der genaueren Prüfung der Klagegründe herausstellen, dass nur bestimmte Teile der angefochtenen Bestimmungen bemängelt werden, wird die Prüfung gegebenenfalls auf diese Teile beschränkt.

B.6. Die angefochtenen Artikel bestimmen:

« KAPITEL 2. - *Anwendungsbereich*

Art. 3. § 1. Vorliegendes Gesetz bestimmt die Verpflichtungen der Beförderungsunternehmen und Reiseunternehmen in Bezug auf die Übermittlung von Daten zu Passagieren, die in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet befördert werden.

§ 2. Der König bestimmt durch einen im Ministerrat beratenen Erlass für jeden Beförderungssektor und für die Reiseunternehmen die zu übermittelnden Passagierdaten sowie die Übermittlungsmodalitäten nach Stellungnahme des Ausschusses für den Schutz des Privatlebens.

KAPITEL 3. - *Begriffsbestimmungen*

Art. 4. Für die Anwendung des vorliegenden Gesetzes und seiner Ausführungserlasse versteht man unter:

[...]

9. ' PNR ': den Datensatz mit den zu jedem einzelnen Passagier notwendigen Reisedaten, der die in Artikel 9 erwähnten Informationen enthält, die die Bearbeitung und Überprüfung der von einer Person oder in ihrem Namen getätigten Reservierungen für jede Reise durch die buchenden und beteiligten Beförderungsunternehmen und Reiseunternehmen ermöglichen, unabhängig davon, ob dieser Datensatz in Buchungssystemen, Abfertigungssystemen (zur Überprüfung der Passagiere beim Anbordgehen) oder gleichwertigen Systemen, die die gleichen Funktionen bieten, enthalten ist,

10. ' Passagier ': jede Person, einschließlich der Personen im Transfer- oder Transitverkehr, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung des Beförderungsunternehmens von ihm befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung dieser Person in die Passagierliste belegt wird,

[...]

KAPITEL 4 - *Verpflichtungen der Beförderungsunternehmen und Reiseunternehmen*

[...]

Art. 7. § 1. Beförderungsunternehmen übermitteln die in Artikel 9 § 1 erwähnten Passagierdaten, über die sie verfügen, und vergewissern sich, dass die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, über die sie verfügen, vollständig, exakt und aktuell sind. Zu diesem Zweck überprüfen sie die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers.

§ 2. Reiseunternehmen übermitteln die in Artikel 9 § 1 erwähnten Passagierdaten, über die sie verfügen, und vergewissern sich, dass die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, über die sie verfügen, vollständig, exakt und aktuell sind. Zu diesem Zweck treffen sie alle notwendigen Maßnahmen, um die Übereinstimmung zwischen den Reisedokumenten und der Identität des betreffenden Passagiers zu überprüfen.

§ 3. Der König bestimmt durch einen im Ministerrat beratenen Erlass pro Beförderungssektor und für die Reiseunternehmen die Modalitäten in Bezug auf die in den Paragraphen 1 und 2 erwähnte Verpflichtung.

KAPITEL 5. - *Zwecke der Datenverarbeitung*

Art. 8. § 1. Die Passagierdaten werden zu folgenden Zwecken verarbeitet:

1. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 90*ter* § 2 Nr. 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 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten,

2. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 196, was die Fälschung authentischer und öffentlicher Urkunden betrifft, 198, 199, 199*bis*, 207, 213, 375 und 505 des Strafgesetzbuches erwähnten Straftaten,

3. Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung durch Beobachtung der Phänomene und Gruppierungen gemäß Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 über das Polizeiamt,

4. Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Aktivitäten,

5. Ermittlung und Verfolgung der in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten.

§ 2. Die Passagierdaten werden unter den in Kapitel 11 erwähnten Bedingungen ebenfalls verarbeitet, um die Personenkontrolle an den Außengrenzen zu verbessern und die illegale Einwanderung zu bekämpfen.

KAPITEL 6. - *Passagierdaten*

Art. 9. § 1. In Bezug auf die Buchungsdaten enthalten die Passagierdaten höchstens:

1. PNR-Buchungscode (Record Locator),

2. Datum der Buchung und der Fahr- beziehungsweise Flugscheinausstellung,

3. planmäßige Reisedaten,

4. Namen, Vornamen und Geburtsdatum,

5. Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse),

6. Zahlungsinformationen einschließlich Rechnungsanschrift,

7. den gesamten Reiseverlauf für den betreffenden Passagier,

8. Informationen zu den ' registrierten Reisenden ', d. h. zu den ' Vielreisenden ',

9. Reisebüro oder Sachbearbeiter,

10. Reisestatus des Reisenden mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Reisen (No show) oder Passagier mit Fahr- beziehungsweise Flugschein, aber ohne Reservierung (Go show),

11. Angaben über gesplittete oder geteilte PNR-Daten,

12. allgemeine Hinweise, einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktangaben der Begleitperson bei der Abreise und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktangaben der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Mitarbeiter bei der Abreise und der Ankunft,

13. Fahr- beziehungsweise Flugscheindaten einschließlich Fahr- beziehungsweise Flugscheinnummer, Ausstellungsdatum, einfache Fahrten beziehungsweise Flüge, informatisierte tarifbezogene Felder der Fahr- beziehungsweise Flugscheine,

14. Sitzplatznummer und sonstige Sitzplatzinformationen,

15. Code-Sharing,

16. vollständige Gepäckangaben,

17. Zahl und Namen von Mitreisenden im Rahmen der PNR-Daten,

18. etwaige erhobene erweiterte Passagierdaten (API-Daten), die in § 2 aufgezählt sind,

19. alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten Daten.

§ 2. In Bezug auf die Daten des Eincheckstatus und des Anbordgehens umfassen die in § 1 Nr. 18 erwähnten erweiterten Daten Folgendes:

1. Art des Reisedokuments,

2. Nummer des Reisedokuments,

3. Staatsangehörigkeit,

4. Land, das das Dokument ausgestellt hat,

5. Ablaufdatum des Dokuments,

6. Familienname, Vorname, Geschlecht, Geburtsdatum,

7. Beförderungsunternehmen/Reiseunternehmen,

8. Beförderungsnummer,

9. Abreisedatum, Ankunftsdatum,

10. Abreiseort, Ankunftsort,

11. Abreisezeit, Ankunftszeit,

12. Gesamtzahl der mit der betreffenden Beförderung beförderten Personen,

13. Sitzplatznummer,

14. PNR-Buchungscode (Record Locator)

15. Anzahl, Gewicht und Identifizierung der Gepäckstücke,

16. Grenzübergangsstelle für die Einreise in das nationale Hoheitsgebiet.

[...]

KAPITEL 7. - *PNR-Zentralstelle*

Art. 12. Innerhalb des Föderalen Öffentlichen Dienstes Inneres wird eine PNR-Zentralstelle geschaffen.

Art. 13. § 1. Die PNR-Zentralstelle ist verantwortlich für:

1. die Erhebung, Aufbewahrung und Verarbeitung der Passagierdaten, die von den Beförderungsunternehmen und Reiseunternehmen übermittelt werden, sowie die Verwaltung der Passagierdatenbank,

2. den Austausch sowohl der Passagierdaten als auch der Ergebnisse der Verarbeitung dieser Daten mit den PNR-Zentralstellen anderer Mitgliedstaaten der Europäischen Union, mit Europol und mit Drittstaaten gemäß Kapitel 12.

§ 2. Unbeschadet anderer gesetzlicher Bestimmungen darf die PNR-Zentralstelle die aufgrund von Kapitel 9 aufbewahrten Daten nicht zu anderen als den in Artikel 8 erwähnten Zwecken benutzen.

Art. 14. § 1. Die PNR-Zentralstelle setzt sich zusammen aus:

1. einem leitenden Beamten, dem ein Unterstützungsdienst beisteht und der verantwortlich ist für:

a) Organisation und Arbeitsweise der PNR-Zentralstelle,

b) Überprüfung der Einhaltung der in Kapitel 4 vorgesehenen Verpflichtungen durch die Beförderungsunternehmen und Reiseunternehmen,

c) Verwaltung und Betrieb der Passagierdatenbank,

d) Verarbeitung der Passagierdaten,

e) Einhaltung der Recht- und Ordnungsmäßigkeit der in Kapitel 10 erwähnten Verarbeitungen,

f) Unterstützung der zuständigen Dienste bei der Ausübung ihrer Befugnisse innerhalb der PNR-Zentralstelle,

2. entsandten Mitgliedern, die aus folgenden zuständigen Diensten stammen:

a) den im Gesetz vom 7. Dezember 1998 zur Organisation eines auf zwei Ebenen strukturierten integrierten Polizeidienstes erwähnten Polizeidiensten,

b) der im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Staatssicherheit,

c) dem im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Allgemeinen Nachrichten- und Sicherheitsdienst,

d) der Verwaltung Ermittlung und Fahndung und der Verwaltung Aufsicht, Kontrolle und Feststellung der im Erlass des Präsidenten des Direktionsausschusses vom 16. Oktober 2014 zur Schaffung neuer Dienste der Generalverwaltung Zoll und Akzisen erwähnten Generalverwaltung Zoll und Akzisen.

Während der Entsendung unterliegen die Mitglieder der zuständigen Dienste der funktionellen und hierarchischen Amtsgewalt des leitenden Beamten der PNR-Zentralstelle. Sie behalten jedoch das Statut ihres ursprünglichen Dienstes.

§ 2. Nach Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens schließen der leitende Beamte der PNR-Zentralstelle und die zuständigen Dienste das in Artikel 17 erwähnte Vereinbarungsprotokoll ab, um die Modalitäten der Datenübermittlung zu bestimmen. Das Protokoll sieht mindestens folgende Sicherheitsvorkehrungen vor:

- Modalitäten des Datenaustauschs,

- durch das Gesetz für die Datenverarbeitung festgelegte Höchstfristen,

- Benachrichtigung der PNR-Zentralstelle durch die zuständigen Dienste über die Folgemaßnahmen zu validierten Treffern.

§ 3. Gemäß den gesetzlichen Verpflichtungen jeden zuständigen Dienstes homologiert die Nationale Sicherheitsbehörde ein abgesichertes und verschlüsseltes Kommunikations- und Informationssystem im Hinblick auf den automatisierten Versand von Treffern.

§ 4. Der König bestimmt durch einen im Ministerrat beratenen Erlass und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens die Modalitäten der Zusammensetzung und Organisation der PNR-Zentralstelle, das Statut des leitenden Beamten und der Mitglieder der PNR-Zentralstelle sowie die Direktionen oder Abteilungen, die innerhalb der zuständigen Dienste mit der Verarbeitung der Passagierdaten beauftragt sind

KAPITEL 8. - *Passagierdatenbank*

Art. 15. § 1. Eine vom Föderalen Öffentlichen Dienst Inneres verwaltete Passagierdatenbank wird geschaffen, in der die Passagierdaten gespeichert werden.

§ 2. Der leitende Beamte der PNR-Zentralstelle ist der für die Verarbeitung Verantwortliche der Passagierdatenbank im Sinne von Artikel 1 § 4 des Gesetzes über den Schutz des Privatlebens.

§ 3. Die in Artikel 10 beziehungsweise 12 des Gesetzes über den Schutz des Privatlebens vorgesehenen Zugriffs- und Berichtigungsrechte in Bezug auf die Passagierdaten werden unmittelbar bei dem Datenschutzbeauftragten ausgeübt.

In Abweichung von Absatz 1 werden diese Rechte beim Ausschuss für den Schutz des Privatlebens ausgeübt, was die in den Artikeln 24 bis 27 erwähnten Treffer und Ergebnisse gezielter Recherchen betrifft.

§ 4. Die aufgrund des vorliegenden Gesetzes vorgenommenen Verarbeitungen der Passagierdaten unterliegen dem Gesetz über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten. Der Ausschuss für den Schutz des Privatlebens übt die im Gesetz über den Schutz des Privatlebens vorgesehenen Befugnisse aus.

Art. 16. Im Rahmen der in Artikel 8 § 1 erwähnten Zwecke ist die Passagierdatenbank der PNR-Zentralstelle direkt zugänglich für die in den Artikeln 24 bis 27 erwähnten Verarbeitungen gemäß den Bestimmungen von Kapitel 9.

[...]

KAPITEL 9. - *Aufbewahrungsfristen*

Art. 18. Passagierdaten werden höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt. Am Ende dieser Frist werden sie vernichtet.

[...]

KAPITEL 10. - *Datenverarbeitung*

Abschnitt 1. Verarbeitung von Passagierdaten im Rahmen der Vorabüberprüfung der Passagiere

Art. 24. § 1. Die Passagierdaten werden im Hinblick auf die Durchführung einer Vorabüberprüfung der Passagiere vor ihrer Ankunft im nationalen Hoheitsgebiet, ihrer Abreise aus dem nationalen Hoheitsgebiet oder ihrer Durchreise durch das nationale Hoheitsgebiet verarbeitet, um diejenigen Personen zu ermitteln, die genauer überprüft werden müssen.

§ 2. Im Rahmen der Zwecke, die in Artikel 8 § 1 Nr. 1, 4 und 5 erwähnt sind oder sich auf Bedrohungen beziehen, die in den Artikeln 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und:

1. den Datenbanken, die von den zuständigen Diensten verwaltet werden oder die ihnen im Rahmen ihrer Aufträge unmittelbar zur Verfügung stehen oder zugänglich sind, oder Personenlisten, die von den zuständigen Diensten im Rahmen ihrer Aufträge erstellt werden,

2. den Überprüfungskriterien, die von der PNR-Zentralstelle im Voraus festgelegt sind und in Artikel 25 erwähnt sind.

§ 3. Im Rahmen der in Artikel 8 § 1 Nr. 3 erwähnten Zwecke beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und den in § 2 Nr. 1 erwähnten Datenbanken.

§ 4. Der Treffer wird innerhalb von vierundzwanzig Stunden nach Eingang der automatisierten Mitteilung des Treffers von der PNR-Zentralstelle validiert.

§ 5. Ab dieser Validierung sorgt der zuständige Dienst, von dem der Treffer herkommt, schnellstmöglich für die weitere Bearbeitung.

Art. 25. § 1. Die Passagierdaten können von der PNR-Zentralstelle zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien benutzt werden, die dazu bestimmt sind, bei den in Artikel 24 § 2 Nr. 2 erwähnten Vorabüberprüfungen der Passagiere Einzelpersonen ins Visier zu nehmen.

§ 2. Die Überprüfung der Passagiere vor ihrer Ankunft, ihrer Durchreise oder ihrer Abreise anhand im Voraus festgelegter Kriterien erfolgt in nichtdiskrimierender Weise. Diese Kriterien dürfen nicht darauf abzielen, eine Person zu identifizieren, und müssen zielgerichtet, verhältnismäßig und bestimmt sein.

§ 3. Die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaftsorganisation, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person dürfen nicht als Grundlage für diese Kriterien dienen.

Art. 26. § 1. Für den in Artikel 8 § 1 Nr. 3 erwähnten Zweck sind nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, die sich auf die Person(en) beziehen, für die sich ein Treffer ergeben hat, zugänglich.

§ 2. Für den Zweck, der in Artikel 8 § 1 Nr. 1, 4 und 5 erwähnt ist oder sich auf die Bedrohungen bezieht, die in Artikel 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, sind alle in Artikel 9 erwähnten Passagierdaten zugänglich.

Abschnitt 2. Datenverarbeitung im Rahmen gezielter Recherchen

Art. 27. Die Passagierdaten werden benutzt, um gezielte Recherchen zu den in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnten Zwecken und unter den in Artikel 46*septies* des Strafprozessgesetzbuches oder in Artikel 16/3 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste vorgesehenen Bedingungen durchzuführen.

KAPITEL 11. *Verarbeitung der Passagierdaten im Hinblick auf eine Verbesserung der Grenzkontrolle und die Bekämpfung der illegalen Einwanderung*

Art. 28. § 1. Vorliegendes Kapitel findet Anwendung auf die Verarbeitung der Passagierdaten durch die Polizeidienste, die mit der Grenzkontrolle beauftragt sind, und durch das Ausländeramt im Hinblick auf eine Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung.

§ 2. Es findet Anwendung unbeschadet der Verpflichtungen, die den mit der Grenzkontrolle beauftragten Polizeidiensten und dem Ausländeramt obliegen, personenbezogene Daten oder Informationen aufgrund von Gesetzes- oder Verordnungsbestimmungen zu übermitteln.

Art. 29. § 1. Die Passagierdaten werden den mit der Grenzkontrolle beauftragten Polizeidiensten und dem Ausländeramt innerhalb der im vorliegenden Artikel vorgesehenen Grenzen zu den in Artikel 28 § 1 erwähnten Zwecken übermittelt, damit sie ihre gesetzlichen Aufträge ausführen können.

§ 2. Nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten in Bezug auf folgende Kategorien von Passagieren werden übermittelt:

1. Passagiere, die beabsichtigen, über die Außengrenzen Belgiens ins Hoheitsgebiet zu kommen, oder bereits über die Außengrenzen Belgiens ins Hoheitsgebiet gekommen sind,

2. Passagiere, die beabsichtigen, das Hoheitsgebiet über die Außengrenzen Belgiens zu verlassen, oder die das Hoheitsgebiet bereits über die Außengrenzen Belgiens verlassen haben,

3. Passagiere, die beabsichtigen, sich in einer in Belgien gelegenen internationalen Transitzone aufzuhalten, sich dort aufhalten oder sich dort aufgehalten haben.

§ 3. Die in § 2 erwähnten Passagierdaten werden den Polizeidiensten, die mit der Kontrolle an den Außengrenzen Belgiens beauftragt sind, unmittelbar nach ihrer Speicherung in der Passagierdatenbank übermittelt. Diese Polizeidienste bewahren diese Daten in einer temporären Datei auf und vernichten sie innerhalb von vierundzwanzig Stunden nach ihrer Übermittlung.

§ 4. Wenn das Ausländeramt die in § 2 erwähnten Passagierdaten für die Ausführung seiner gesetzlichen Aufträge benötigt, werden sie ihm unmittelbar nach ihrer Speicherung in der Passagierdatenbank übermittelt. Das Ausländeramt bewahrt diese Daten in einer temporären Datei auf und vernichtet sie innerhalb von vierundzwanzig Stunden nach ihrer Übermittlung.

Wenn der Zugriff auf die in § 2 erwähnten Passagierdaten nach Ablauf dieser Frist noch notwendig ist, damit das Ausländeramt seine gesetzlichen Aufträge ausführen kann, richtet das Ausländeramt eine gebührend mit Gründen versehene Anfrage an die PNR-Zentralstelle.

Das Ausländeramt übermittelt dem Ausschuss für den Schutz des Privatlebens monatlich einen Bericht über die Anwendung von Absatz 2.

Der König bestimmt durch einen im Ministerrat beratenen Erlass nach Stellungnahme des Ausschusses für den Schutz des Privatlebens die in Absatz 2 erwähnten Zugriffsbedingungen.

Art. 30. § 1. Die technischen Sicherungs- und Zugriffsmodalitäten sowie die Modalitäten der Übermittlung der Passagierdaten an die mit der Grenzkontrolle beauftragten Polizeidienste und an das Ausländeramt werden in einem Protokoll dargelegt, das in Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens zwischen dem leitenden Beamten der PNR-Zentralstelle einerseits und dem Generalkommissar der föderalen Polizei und dem leitenden Beamten des Ausländeramtes andererseits für ihren jeweiligen Bereich abgeschlossen wird.

§ 2. Diese Modalitäten beziehen sich mindestens auf:

1. den Bedarf des Ausländeramtes, die Daten zu kennen,

2. die Kategorien von Personalmitgliedern, die auf der Grundlage der Ausführung ihrer Aufträge unmittelbaren Zugriff auf die übermittelten Daten haben,

3. die Pflicht zur Wahrung des Berufsgeheimnisses durch alle Personen, die die Passagierdaten unmittelbar oder mittelbar zur Kenntnis nehmen,

4. die Sicherheitsmaßnahmen in Zusammenhang mit ihrer Übermittlung.

Art. 31. Binnen vierundzwanzig Stunden nach dem Ende der in Artikel 4 Nr. 3 bis 6 erwähnten Beförderung löschen die Beförderungsunternehmen und Reiseunternehmen alle in Artikel 9 § 2 erwähnten Passagierdaten, die sie gemäß Artikel 7 übermitteln.

[...]

KAPITEL 15. - *Abänderungsbestimmungen*

Abschnitt 1. - Abänderung des Strafprozessgesetzbuches

Art. 50. In das Strafprozessgesetzbuch wird ein Artikel 46*septies* mit folgendem Wortlaut eingefügt:

‘ Art. 46*septies*. Bei der Ermittlung von Verbrechen und Vergehen, die in Artikel 8 § 1 Nr. 1, 2 und 5 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten erwähnt sind, kann der Prokurator des Königs durch einen mit Gründen versehenen schriftlichen Beschluss den Gerichtspolizeioffizier damit beauftragen, die PNR-Zentralstelle aufzufordern, die Passagierdaten gemäß Artikel 27 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten mitzuteilen.

Die Begründung spiegelt die Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und die Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe wider.

Die Maßnahme kann eine Gesamtheit von Daten in Bezug auf eine spezifische Ermittlung betreffen. In diesem Fall bestimmt der Prokurator des Königs die Dauer der Maßnahme, die einen Monat ab dem Beschluss nicht überschreiten darf, unbeschadet einer Erneuerung.

In Fällen äußerster Dringlichkeit kann jeder Gerichtspolizeioffizier mit der mündlichen und vorherigen Zustimmung des Prokurators des Königs durch einen mit Gründen versehenen schriftlichen Beschluss den leitenden Beamten der PNR-Zentralstelle auffordern, die Passagierdaten mitzuteilen. Der Gerichtspolizeioffizier teilt dem Prokurator des Königs diesen mit Gründen versehenen schriftlichen Beschluss sowie die erhaltenen Informationen binnen vierundzwanzig Stunden mit und begründet außerdem die äußerste Dringlichkeit ’.

Abschnitt 2. - Abänderung des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste

Art. 51. In Kapitel III Abschnitt 1 Unterabschnitt 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste wird ein Artikel 16/3 mit folgendem Wortlaut eingefügt:

' Art. 16/3. § 1. Die Nachrichten- und Sicherheitsdienste können im Interesse der Ausübung ihrer Aufträge und ordnungsgemäß begründet beschließen, auf die in Artikel 27 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten erwähnten Passagierdaten zuzugreifen.

§ 2. Der in § 1 erwähnte Beschluss wird von einem Dienstleiter gefasst und der in Kapitel 7 des vorerwähnten Gesetzes erwähnten PNR-Zentralstelle schriftlich übermittelt. Der Beschluss wird zusammen mit seiner Begründung dem Ständigen Ausschuss N notifiziert.

Der Ständige Ausschuss N verbietet den Nachrichten- und Sicherheitsdiensten, die gesammelten Daten unter Bedingungen zu benutzen, die die gesetzlichen Bedingungen nicht einhalten.

Der Beschluss kann eine Gesamtheit von Daten in Bezug auf eine spezifische nachrichtendienstliche Untersuchung betreffen. In diesem Fall wird dem Ständigen Ausschuss N einmal pro Monat die Liste der Abfragen der Passagierdaten übermittelt. ' ».

In Bezug auf das Inkrafttreten und den Anwendungsbereich des Gesetzes vom 25. *Dezember* 2016

B.7. Nach Artikel 54 des Gesetzes vom 25. Dezember 2016 bestimmt der König durch einen im Ministerrat beratenen Erlass pro Beförderungssektor und für die Reiseunternehmen das Datum des Inkrafttretens dieses Gesetzes.

B.8. In Bezug auf die Fluggesellschaften ist das Gesetz vom 25. Dezember 2016 am 7. August 2017, gemäß Artikel 12 des königlichen Erlasses vom 18. Juli 2017 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung der Pflichten der Fluggesellschaften » (nachstehend: königlicher Erlass vom 18. Juli 2017) in Kraft getreten.

Seit dem 22. Februar 2019 gilt das Gesetz vom 25. Dezember 2016 ebenfalls in Bezug auf die HST-Beförderungsunternehmen (Hochgeschwindigkeitszug - grenzüberschreitender Personenverkehrsdienst auf der Schiene) und die HST-Fahrkartenverkäufer, gemäß dem königlichen Erlass vom 3. Februar 2019 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung der Pflichten der HST-Beförderungsunternehmen und der HST-Fahrkartenverkäufer », sowie in Bezug auf die Busunternehmen, gemäß dem königlichen Erlass vom 3. Februar 2019 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung der Pflichten der Busunternehmen ».

In Bezug auf die Änderungen des Gesetzes vom 25. *Dezember* 2016

B.9. Das Gesetz vom 25. Dezember 2016 wurde abgeändert durch das Gesetz vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » (nachstehend: Gesetz vom 30. Juli 2018), durch das Gesetz vom 15. Juli 2018 « zur Festlegung verschiedener Bestimmungen im Bereich Inneres » (nachstehend: Gesetz vom 15. Juli 2018) und durch das Gesetz vom 2. Mai 2019 « zur Abänderung verschiedener Bestimmungen über die Verarbeitung von Passagierdaten » (nachstehend: Gesetz vom 2. Mai 2019).

B.10.1. Artikel 15 § 3 des Gesetzes vom 25. Dezember 2016 wurde durch Artikel 280 Absatz 4 des Gesetzes vom 30. Juli 2018 mit Wirkung vom 5. September 2018 aufgehoben.

Da gegen Artikel 280 Absatz 4 des Gesetzes vom 30. Juli 2018 keinerlei Klage auf Nichtigerklärung erhoben worden ist, ist die vorliegende Nichtigkeitsklage endgültig gegenstandslos geworden, insofern sie sich auf Artikel 15 § 3 des Gesetzes vom 25. Dezember 2016 bezieht.

B.10.2. Das Gesetz vom 30. Juli 2018 legt außerdem den Rahmen für die Verarbeitung von personenbezogenen Daten, insbesondere im Rahmen der in Artikel 8 des Gesetzes vom 25. Dezember 2016 aufgezählten Zwecke, fest.

In den Vorarbeiten zu dem Gesetz vom 30. Juli 2018 wurde diesbezüglich ausgeführt:

« 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 » (ebenda, SS. 188-189).

Daraus ergibt sich, dass der Gerichtshof zur Beurteilung der Tragweite des angefochtenen Artikels 8 des Gesetzes vom 25. Dezember 2016 das Gesetz vom 30. Juli 2018 berücksichtigen muss.

B.11.1. Durch die Artikel 62 bis 70 des Gesetzes vom 15. Juli 2018 « zur Festlegung verschiedener Bestimmungen im Bereich Inneres » (nachstehend: Gesetz vom 15. Juli 2018), veröffentlicht im *Belgischen Staatsblatt* vom 25. September 2018, wurde das Gesetz vom 25. Dezember 2016 ebenfalls abgeändert.

Die Artikel 62 bis 68 ändern mehrere der angefochtenen Artikel des Gesetzes vom 25. Dezember 2016 wie folgt ab:

« Art. 62. Artikel 8 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten wird wie folgt abgeändert:

1. Paragraph 1 Nr. 1 wird wie folgt ersetzt:

' 1. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 90*ter* § 2 Nr. 2, 3, 7, 8, 11, 14, 17 bis 20, 22, 24 bis 28, 30, 32, 33, 34, 36 bis 39, 43 bis 45 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten, '.

2. Paragraph 1 Nr. 5 wird wie folgt ersetzt:

‘ 5. Ermittlung und Verfolgung der Straftaten, erwähnt in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen, in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung, in Artikel 5 des Gesetzes vom 15. Mai 2007 über die Ahndung der Nachahmung und der Piraterie von geistigen Eigentumsrechten, in Artikel 26 des Dekretes der Deutschsprachigen Gemeinschaft vom 20. Februar 2017 zum Schutz des beweglichen Kulturgutes von außerordentlicher Bedeutung sowie in Artikel 24 des Dekretes der Flämischen Gemeinschaft vom 24. Januar 2003 ‘ houdende bescherming van het roerend cultureel erfgoed van uitzonderlijk belang ’ (Schutz des beweglichen Kulturerbes von außerordentlicher Bedeutung), im Ministeriellen Erlass vom 7. Februar 2012 zur Einführung einer Lizenzpflicht für die Einfuhr von Waren, deren Ursprung oder Herkunft Syrien ist, abgeändert durch den Ministeriellen Erlass vom 1. Juli 2014, im Ministeriellen Erlass vom 23. März 2004 zur Aufhebung des Ministeriellen Erlasses vom 17. Januar 2003 zur Einführung der Pflicht, für die Ein-, Aus- und Durchfuhr von Waren, deren Ursprung, Herkunft oder Bestimmung der Irak ist, über eine vorherige Ermächtigung zu verfügen und für die Ein-, Aus- und Durchfuhr bestimmter Waren, deren Ursprung, Herkunft oder Bestimmung der Irak ist, über eine Lizenz zu verfügen, sowie Ermittlung der Verstöße, erwähnt in Artikel 5 des Gesetzes vom 28. Juli 1981 zur Billigung des Übereinkommens über den internationalen Handel mit gefährdeten Arten freilebender Tiere und Pflanzen und der Anlagen, abgeschlossen in Washington am 3. März 1973, und der Änderung des Übereinkommens, angenommen in Bonn am 22. Juni 1979 ’.

Art. 63. Artikel 14 desselben Gesetzes wird wie folgt abgeändert:

1. In Paragraph 1 Nr. 2 wird Buchstabe *d)* wie folgt ersetzt:

‘ *d)* den Enquetendiensten, Ermittlungsdiensten und Diensten der Generalverwaltung Zoll und Akzisen, die mit der Aufsicht, Kontrolle und Feststellung beauftragt sind. ’

2. Paragraph 4 wird wie folgt ersetzt:

‘ § 4. Der König bestimmt durch einen im Ministerrat beratenen Erlass und nach Stellungnahme der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde die Modalitäten der Zusammensetzung und Organisation der PNR-Zentralstelle sowie das Statut des leitenden Beamten und der Mitglieder der PNR-Zentralstelle. ’

Art. 64. In Artikel 15 § 2 desselben Gesetzes wird das Wort ‘ Passagierdatenbank ’ durch das Wort ‘ Passagierdaten ’ ersetzt.

Art. 65. Artikel 17 desselben Gesetzes wird wie folgt ersetzt:

‘ Art. 17. Nach Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde schließen der leitende Beamte der PNR-Zentralstelle und die zuständigen Dienste ein Vereinbarungsprotokoll ab, das der Umsetzung der technischen Sicherungs- und Zugriffsmodalitäten dient.

Mit diesem Protokoll:

1. wird gewährleistet, dass die verarbeiteten Daten denselben Sicherheits- und Schutzanforderungen unterliegen,

2. wird sichergestellt, dass die notwendigen Schutzmaßnahmen getroffen werden, damit:

- alle Verpflichtungen erfüllt werden, die sich aus den Regeln in Bezug auf die im vorliegenden Gesetz festgelegten Fristen, die Aufbewahrung und Vernichtung der in der Passagierdatenbank aufbewahrten Daten ergeben,

- die Daten für alle Personen, die nicht zum Zugriff darauf befugt sind, gesperrt werden,

- gewährleistet wird, dass die von den Mitgliedern der PNR-Zentralstelle vorgenommenen Verarbeitungen mit dem Gesetz vom 11. Dezember 1998 über die Klassifizierung und die Sicherheitsermächtigungen, -bescheinigungen und -stellungnahmen in Übereinstimmung stehen,

3. wird vorgesehen, dass den Personen, die auf die Passagierdaten zugreifen können, Berechtigungen zum Zugriff auf die Passagierdaten erteilt und gemeinsame und spezifische Benutzerprofile zugewiesen werden,

4. wird gewährleistet, dass die Daten im Hoheitsgebiet der Europäischen Union aufbewahrt werden. ’.

Art. 66. In Artikel 24 § 2 desselben Gesetzes wird der einleitende Satz von Absatz 1 wie folgt ersetzt:

‘ Im Rahmen der Zwecke, die in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnt sind oder sich auf Bedrohungen beziehen, die in den Artikeln 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und: ’.

Art. 67. In Artikel 26 desselben Gesetzes wird § 2 wie folgt ersetzt:

‘ § 2. Für den Zweck, der in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnt ist oder sich auf die Bedrohungen bezieht, die in Artikel 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, sind alle in Artikel 9 erwähnten Passagierdaten zugänglich. ’.

Art. 68. In Artikel 31 desselben Gesetzes werden die Wörter ‘ Artikel 9 § 2 ’ durch die Wörter ‘ Artikel 9 § 1 Nr. 18 ’ ersetzt. ’ ».

Diese Abänderungen sind am 5. Oktober 2018 in Kraft getreten.

B.11.2. Die Artikel 62, 63, 65, 66 und 67 des Gesetzes vom 15. Juli 2018 ersetzten jeweils die Artikel 8 § 1 Nrn. 1 und 5, 14 § 1, Nr. 2, Buchstabe *d)* und § 4, 17, 24 § 2 Absatz 1 einleitender Satz und 26 § 2 des Gesetzes vom 25. Dezember 2016.

Da keine Nichtigkeitsklage gegen die vorerwähnten Artikel des Gesetzes vom 15. Juli 2018 eingereicht wurde, ist die vorliegende Nichtigkeitsklage im Prinzip gegenstandslos geworden, insoweit sie gegen die ersetzten Artikel des Gesetzes vom 25. Dezember 2016 gerichtet ist.

Die vorliegende Klage richtet sich gegen die ursprüngliche Fassung des Gesetzes vom 25. Dezember 2016. Auch wenn Artikel 8 § 1 Nrn. 1 und 5, Artikel 14 § 1 Nr. 2 Buchstabe *d)* und § 4, Artikel 17, Artikel 24 § 2 Absatz 1 einleitender Satz und Artikel 26 § 2 des Gesetzes vom 25. Dezember 2016 durch die vorerwähnten Artikel des Gesetzes vom 15. Juli 2018 ersetzt wurden, hat die Nichtigkeitsklage, insofern sie gegen Artikel 8 § 1 Nrn. 1 und 5, Artikel 14 § 1 Nr. 2 Buchstabe *d)* und § 4, Artikel 17, Artikel 24 § 2 Absatz 1 einleitender Satz und Artikel 26 § 2 des Gesetzes vom 25. Dezember 2016 gerichtet ist, weiterhin einen Gegenstand, sofern das Gesetz vom 15. Juli 2018 diese angefochtenen Artikel des Gesetzes vom 25. Dezember 2016 nicht wesentlich abändert.

Der Gerichtshof prüft folglich für jede dieser Bestimmungen und in Bezug auf jeden Beschwerdegrund, in welchem Maße die Nichtigkeitsklage weiterhin einen Gegenstand hat.

B.11.3. Artikel 64 des Gesetzes vom 15. Juli 2018 ersetzt in Artikel 15 § 2 des Gesetzes vom 25. Dezember 2016 das Wort « Passagierdatenbank » durch das Wort « Passagierdaten ».

Artikel 68 des Gesetzes vom 15. Juli 2018 ersetzt in Artikel 31 des Gesetzes vom 25. Dezember 2016 die Wörter « Artikel 9 § 2 » durch die Wörter « Artikel 9 § 1 Nr. 18 ».

Diese Abänderungen betreffen nur technische Korrekturen der Artikel 15 § 2 und 31 des Gesetzes vom 25. Dezember 2016, ohne diese Bestimmungen zu ersetzen, sodass sie nicht als Abänderungen angesehen werden können, die sich auf den Gegenstand der vorliegenden Klage auswirken.

B.11.4. Im Übrigen berücksichtigt der Gerichtshof die vorerwähnten Abänderungen, insbesondere um die Tragweite der angefochtenen Bestimmungen zu bestimmen.

B.12.1. Durch die Artikel 2 bis 11 des Gesetzes vom 2. Mai 2019, veröffentlicht im *Belgischen Staatsblatt* vom 24. Mai 2019, wurde das Gesetz vom 25. Dezember 2016 ebenfalls abgeändert.

Die Artikel 2 und 4 bis 7 des Gesetzes vom 2. Mai 2019 ändern mehrere der angefochtenen Artikel des Gesetzes vom 25. Dezember 2016 wie folgt ab:

« 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. À 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. À 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)* '».

Diese Abänderungen sind am 3. Juni 2019 in Kraft getreten.

B.12.2. Da die Artikel 2, 4 und 7 des Gesetzes vom 2. Mai 2019 nur technische Korrekturen der Artikel 3 § 2, 14 § 2, 15 § 4, 29 und 30 § 1 des Gesetzes vom 25. Dezember 2016 betreffen, wirken sich diese Abänderungen nicht auf den Klagegegenstand aus.

Im Übrigen hat die Nichtigkeitsklage – obgleich durch Artikel 6 des Gesetzes vom 2. Mai 2019 der angefochtene Artikel 27 des Gesetzes vom 25. Dezember 2016 ersetzt wird –, insofern sie gegen diese Bestimmung gerichtet ist, weiterhin einen Gegenstand, sofern der Inhalt von Artikel 6 des Gesetzes vom 2. Mai 2019 mit der ursprünglichen Fassung dieses Artikels 27 identisch ist.

Des Weiteren berücksichtigt der Gerichtshof die Abänderung, die durch Artikel 5 des Gesetzes vom 2. Mai 2019 an Artikel 24 § 2 des Gesetzes vom 25. Dezember 2016 vorgenommen wurde, insbesondere um die Tragweite der angefochtenen Bestimmung zu bestimmen.

In Bezug auf das Ersuchen um Vorabentscheidung durch den Gerichtshof der Europäischen Union

B.13.1. Mit seinem Zwischenentscheid Nr. 135/2019 vom 17. Oktober 2019 (ECLI:BE:GHCC:2019:ARR.135) hat der Verfassungsgerichtshof den Gerichtshof der Europäischen Union zur Auslegung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG » (Datenschutz-Grundverordnung – nachstehend: DSGVO) sowie zur Auslegung und Gültigkeit der PNR-Richtlinie und der API-Richtlinie befragt. Der Verfassungsgerichtshof hat den Gerichtshof der Europäischen Union ebenfalls gefragt, ob er im Fall der Nichtigerklärung des angefochtenen Gesetzes wegen Verstoßes gegen das europäische Recht die Folgen dieses Gesetzes vorläufig aufrechterhalten könnte.

B.13.2. Der Gerichtshof hat dem Gerichtshof der Europäischen Union somit die folgenden zehn Vorabentscheidungsfragen gestellt:

« 1. Ist Artikel 23 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 ' zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG ' (Datenschutz-Grundverordnung - DSGVO) in Verbindung mit Artikel 2 Absatz 2 Buchstabe d dieser Verordnung so auszulegen, dass er auf einzelstaatliche Rechtsvorschriften wie das Gesetz vom 25. Dezember 2016 ' über die Verarbeitung von Passagierdaten ', mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 ' über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität ', sowie die Richtlinie 2004/82/EG des Rates vom 29. April 2004 « über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln » und die Richtlinie 2010/65/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 ' über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG ' umgesetzt wird, anwendbar ist?

2. Ist Anhang I der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union in dem Sinne vereinbar, dass die darin aufgeführten Daten sehr weitgehend sind – insbesondere die in Nummer 18 von Anhang I der Richtlinie (EU) 2016/681 erwähnten Daten, die über die in Artikel 3 Absatz 2 der Richtlinie 2004/82/EG erwähnten Daten hinausgehen – insofern sie zusammen genommen sensible Daten offenlegen könnten und so über das ' absolut Notwendige ' hinausgehen könnten?

3. Sind die Nummern 12 und 18 von Anhang I der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern unter Berücksichtigung des Wortes ' einschließlich ' die dort aufgeführten Daten in beispielhafter und nicht erschöpfender Weise genannt werden, was somit gegen die Anforderung der Präzision und Klarheit der Regeln, die einen Eingriff in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten nach sich ziehen, verstoßen könnte?

4. Sind Artikel 3 Nummer 4 der Richtlinie (EU) 2016/681 und Anhang I derselben Richtlinie mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern das System zur allgemeinen Erhebung, Übermittlung und Verarbeitung von Passagierdaten, das mit diesen Bestimmungen eingeführt wird, auf jede Person abzielt, die das betreffende Beförderungsmittel benutzt, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von dieser Person eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

5. Ist Artikel 6 der Richtlinie (EU) 2016/681 in Verbindung mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das als Verarbeitungszweck der PNR-Daten die Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste zulässt und so diesen Zweck in die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität aufnimmt?

6. Ist Artikel 6 der Richtlinie (EU) 2016/681 mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union vereinbar, insofern die in ihm geregelte Vorabüberprüfung durch eine Korrelation mit Datenbanken und im Voraus festgelegten Kriterien systematisch und allgemein auf die Passagierdaten angewandt wird, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von diesen Fluggästen eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

7. Kann der in Artikel 12 Absatz 3 der Richtlinie (EU) 2016/681 erwähnte Ausdruck ' andere nationale Behörde, die [...] zuständig ist ' dahin ausgelegt werden, dass er sich auf die PNR-Zentralstelle bezieht, die durch das Gesetz vom 25. Dezember 2016 geschaffen wurde und die somit den Zugriff auf die PNR-Daten nach einer sechsmonatigen Frist im Rahmen von gezielten Recherchen gestatten dürfte?

8. Ist Artikel 12 der Richtlinie (EU) 2016/681 in Verbindung mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das eine allgemeine Aufbewahrungsdauer für die Daten von fünf Jahren vorsieht, ohne eine Unterscheidung danach vorzunehmen, ob sich im Rahmen der Vorabüberprüfung herausstellt, dass die betroffenen Fluggäste ein Risiko für die öffentliche Sicherheit darstellen können oder nicht?

9. *a)* Ist die Richtlinie 2004/82/EG mit Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 45 der Charta der Grundrechte der Europäischen Union vereinbar, insofern die Pflichten, die sie einführt, für Flüge innerhalb der Europäischen Union gelten?

b) Ist die Richtlinie 2004/82/EG in Verbindung mit Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 45 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass sie einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das zum Zwecke der Bekämpfung der illegalen Einwanderung und der Verbesserung der Grenzkontrollen ein System zur Erhebung und Verarbeitung der Daten ' zu den in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet ' beförderten Passagieren gestattet, was indirekt eine Wiedereinführung von Kontrollen an den Binnengrenzen bedeuten könnte?

10. Könnte der Verfassungsgerichtshof, falls er auf der Grundlage der Antworten auf die vorstehenden Vorabentscheidungsfragen zu dem Schluss gelangen sollte, dass das angefochtene Gesetz, mit dem insbesondere die Richtlinie (EU) 2016/681 umgesetzt wird, gegen eine oder mehrere der Verpflichtungen verstößt, die sich aus den in diesen Fragen genannten Bestimmungen ergeben, die Folgen des Gesetzes vom 25. Dezember 2016 ' über die Verarbeitung von Passagierdaten ' vorläufig aufrechterhalten, um eine Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch das Gesetz angestrebten Ziele benutzt werden können? ».

B.14. In seinem Urteil vom 21. Juni 2022 in Sachen *Ligue des droits humains gegen Ministerrat* (C-817/19, ECLI:EU:C:2022:491) hat der Gerichtshof der Europäischen Union, Große Kammer, auf die vorerwähnten Vorabentscheidungsfragen geantwortet.

Im vorerwähnten Urteil hat der Gerichtshof der Europäischen Union nacheinander geprüft:

- die erste Vorabentscheidungsfrage bezüglich der Verknüpfung der DSGVO mit der PNR-Richtlinie (Randnrn. 63 bis 84);

- die zweite bis vierte und sechste Vorabentscheidungsfrage über die Gültigkeit der PNR-Richtlinie und/oder ihre Anhänge, was das System der Datenerhebung und die betroffenen Daten betrifft (Randnrn. 85 bis 228);

- die fünfte Vorabentscheidungsfrage über die Auslegung der PNR-Richtlinie, was die Zwecke in Bezug auf den Nachrichten- und Sicherheitsdienst betrifft (Randnrn. 229 bis 237);

- die siebte Vorabentscheidungsfrage über die Auslegung des in der PNR-Richtlinie erwähnten Begriffs der unabhängigen nationalen Behörde (Randnrn. 238 bis 247);

- die achte Vorabentscheidungsfrage über die Auslegung der in der PNR-Richtlinie erwähnten Speicherfrist der Daten (Randnrn. 248 bis 262);

- Buchstabe a der neunten Vorabentscheidungsfrage über die Gültigkeit der API-Richtlinie, ob diese Richtlinie für EU-Flüge gilt (Randnrn. 263 bis 269);

- Buchstabe b der neunten Vorabentscheidungsfrage über die Auslegung der API-Richtlinie, insofern sie es ermöglichen würde, die illegale Einwanderung zu bekämpfen und eine Form der Kontrolle an den Grenzen wieder einzuführen (Randnrn. 270 bis 291);

- die zehnte Vorabentscheidungsfrage bezüglich einer möglichen Aufrechterhaltung der Folgen des Gesetzes, das eventuell mit dem Unionsrecht unvereinbar wäre (Randnrn. 292 bis 298).

In Bezug auf den ersten Klagegrund

B.15. Der erste, hauptsächlich vorgebrachte Klagegrund ist abgeleitet aus einem Verstoß gegen Artikel 22 der Verfassung, an sich oder in Verbindung mit Artikel 23 der DSGVO, mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union und mit Artikel 8 der Europäischen Menschenrechtskonvention.

Nach Auffassung der klagenden Partei verletzt das Gesetz vom 25. Dezember 2016 das Recht auf Achtung des Privatlebens und das Recht auf den Schutz personenbezogener Daten, die durch diese Bestimmungen gewährleistet werden. Das Gesetz vom 25. Dezember 2016 verstoße gegen das Legalitätsprinzip. Die systematische und unterschiedslose Erhebung, Übermittlung und Verarbeitung von PNR-Daten mit einem « Pre-Screening »-Verfahren seien weder notwendig noch durch ein dem Gemeinwohl dienendes Ziel gerechtfertigt und mehrere eingeführte Maßnahmen seien unverhältnismäßig.

Was die Bezugsnormen betrifft

B.16.1. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

B.16.2. Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer ».

B.16.3. Der Verfassungsgeber hat eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorgenannten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gewährleisteten Garantien eine untrennbare Einheit bilden.

B.17.1. Das Recht auf Achtung des Privat- und Familienlebens, so wie es durch die vorerwähnten Verfassungs- und Vertragsbestimmungen gewährleistet wird, bezweckt im Wesentlichen, die Personen gegen Einmischungen in ihr Privatleben und Familienleben zu schützen.

Dieses Recht hat eine weitreichende Tragweite und umfasst unter anderem das Recht auf körperliche Unversehrtheit der Person (EuGHMR, Große Kammer, 8. April 2021, *Vavřička u.a. gegen Tschechische Republik*, ECLI:CE:ECHR:2021:0408JUD004762113, § 261) und den Schutz personenbezogener Daten und persönlicher Informationen in Bezug auf die Gesundheit (EuGHMR, 25. Februar 1997, *Z. gegen Finnland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; 10. Oktober 2006, *L.L. gegen Frankreich*, ECLI:CE:ECHR:2006:1010JUD000750802, § 32; 27. Februar 2018, *Mockuté gegen Litauen*, ECLI:CE:ECHR:2018:0227JUD006649009, § 93). Aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ergibt sich, dass unter anderem die folgenden Daten und Informationen über die Person von diesem Recht geschützt sind: Name, Adresse, berufliche Aktivitäten, persönliche Beziehungen, digitale Fingerabdrücke, Kamerabilder, Fotos, Kommunikationsdaten, DNA-Daten, gerichtliche Daten (Verurteilung oder Verdacht), Finanzdaten, Informationen über Vermögenswerte und medizinische Daten (siehe u.a. EuGHMR, 26. März 1987, *Leander gegen Schweden*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47-48; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66-68; 17. Dezember 2009, *B.B. gegen Frankreich*, ECLI:CE:ECHR:2009:1217JUD000533506, § 57; 10. Februar 2011, *Dimitrov-Kazakov gegen Bulgarien*, ECLI:CE:ECHR:2011:0210JUD001137903, §§ 29-31; 18. Oktober 2011, *Khelili gegen Schweiz*, ECLI:CE:ECHR:2011:1018JUD001618807, §§ 55-57; 9. Oktober 2012, *Alkaya gegen Türkei*, ECLI:CE:ECHR:2012:1009JUD004281106, § 29; 18. April 2013, *M.K. gegen Frankreich*, ECLI:CE:ECHR:2013:0418JUD001952209, § 26; 18. September 2014, *Brunet gegen Frankreich*, ECLI:CE:ECHR:2014:0918JUD002101010, § 31; 13. Oktober 2020, *Frâncu gegen Rumänien*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

B.17.2. Die durch Artikel 22 der Verfassung und durch Artikel 8 der Europäischen Menschenrechtskonvention gewährleisteten Rechte sind jedoch nicht absolut.

Sie schließen eine behördliche Einmischung in das Recht auf Achtung des Privatlebens nicht aus, verlangen jedoch, dass diese durch eine ausreichend präzise Gesetzesbestimmung erlaubt wird, einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht und im Verhältnis zu der damit verfolgten gesetzmäßigen Zielsetzung steht. Diese Bestimmungen beinhalten außerdem die positive Verpflichtung für die Behörden, Maßnahmen zu ergreifen, die eine tatsächliche Achtung des Privatlebens gewährleisten, selbst in der Sphäre der gegenseitigen Beziehungen zwischen Einzelpersonen (EuGHMR, 27. Oktober 1994, *Kroon und andere gegen Niederlande*, ECLI:CE:ECHR:1994:1027JUD001853591, § 31; Große Kammer, 12. November 2013, *Söderman gegen Schweden*, ECLI:CE:ECHR:2013:1112JUD000578608, § 78).

Wenn sie die Abwägung zwischen dem Interesse des Staates an der Verarbeitung personenbezogener Daten und das Interesse des Einzelnen am Schutz der Vertraulichkeit dieser Daten vornehmen, verfügen die nationalen Behörden über einen gewissen Beurteilungsspielraum (ebenda, § 99). In Anbetracht der grundlegenden Bedeutung des Schutzes personenbezogener Daten ist dieser Spielraum jedoch recht begrenzt (EuGHMR, 26. Januar 2017, *Surikov gegen Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 73). Damit eine Norm mit dem Recht auf Achtung des Privatlebens vereinbar ist, ist es erforderlich, dass ein faires Gleichgewicht zwischen allen betroffenen Rechten und Interessen hergestellt wird. Bei der Beurteilung dieses Gleichgewichts sind unter anderem die Bestimmungen des Übereinkommens des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (nachstehend: Übereinkommen Nr. 108) zu berücksichtigen (EuGHMR, 25. Februar 1997, *Z gegen Finnland*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, § 103; 26. Januar 2017, *Surikov gegen Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

Das Übereinkommen Nr. 108 beinhaltet u.a. die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Verhältnismäßigkeit, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht.

Dasselbe Übereinkommen wird durch ein Änderungsprotokoll aktualisiert, das am 10. Oktober 2018 zur Unterzeichnung aufgelegt wurde.

Aus dem Übereinkommen Nr. 108 ergibt sich, dass das innerstaatliche Recht insbesondere gewährleisten muss, dass die personenbezogenen Daten unter Berücksichtigung der Zwecke, für die sie erhoben oder gespeichert werden, erheblich sind und nicht darüber hinausgehen, dass sie so aufbewahrt werden, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke erfordern, und dass die gespeicherten Daten wirksam gegen unangemessene und missbräuchliche Nutzungen geschützt werden. Es hat auch vorgegeben, dass es von großer Bedeutung ist, dass im innerstaatlichen Recht klare und detaillierte Regeln zur Tragweite und Anwendung der betreffenden Maßnahmen sowie Mindestgarantien vorgesehen sind, die unter anderem die Dauer, die Speicherung, die Nutzung, den Zugriff von Dritten, die Verfahren zur Wahrung der Integrität und Vertraulichkeit von Daten und die Verfahren zu deren Vernichtung betreffen, sodass ausreichende Garantien gegen die Gefahr von Missbrauch und Willkür in jeder Phase der Datenverarbeitung existieren (EuGHMR, 26. Januar 2017, *Surikov gegen Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

B.18.1. Artikel 7 der Charta der Grundrechte der Europäischen Union bestimmt:

« Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation ».

B.18.2. Artikel 8 derselben Charta bestimmt:

« 1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht ».

B.18.3. Innerhalb des Geltungsbereichs des Rechts der Europäischen Union gewährleisten Artikel 22 der Verfassung, Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 der Charta analoge Grundrechte (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke GbR u.a.*, ECLI:EU:C:2010:662), während Artikel 8 der Charta einen spezifischen Rechtsschutz für personenbezogene Daten bietet (EuGH, Große Kammer, 21. Dezember 2016, C-203/15 und C-698/15, *Tele*2 *Sverige AB*, ECLI:EU:C:2016:970, Randnr. 129; 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, ECLI:EU:C:2020:791, Randnr. 114).

Der Gerichtshof weist diesbezüglich darauf hin, dass « Artikel 7 der Charta, der das Recht auf Achtung des Privat- und Familienlebens betrifft, Rechte enthält, die den in Artikel 8 Absatz 1 der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (nachstehend: EMRK) gewährleisteten Rechten entsprechen, und dass diesem Artikel 7 gemäß Artikel 52 Absatz 3 der Charta somit die gleiche Bedeutung und Tragweite beizumessen ist wie Artikel 8 Absatz 1 EMRK in seiner Auslegung durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte » (EuGH, 17. Dezember 2015, C-419/14, *WebMindLicenses Kft.*, ECLI:EU:C:2015:832, Randnr. 70; 14. Februar 2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122, Randnr. 65).

B.18.4. Der Gerichtshof der Europäischen Union ist der Auffassung, dass sich die Achtung des Rechts auf Privatleben hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke GbR u.a.*, ECLI:EU:C:2010:662, Randnr. 52; 16. Januar 2019, C-496/17, *Deutsche Post AG*, ECLI:EU:C:2019:26, Randnr. 54).

B.18.5. Auch die in den Artikeln 7 und 8 der Charta verankerten Grundrechte können keine uneingeschränkte Geltung beanspruchen (EuGH, Große Kammer, 16. Juli 2020, C-311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, Randnr. 172).

Nach Artikel 52 Absatz 1 Satz 1 der Charta müssen Einschränkungen der Ausübung der darin garantierten Rechte und Freiheiten, einschließlich insbesondere des durch deren Artikel 7 gewährleisteten Rechts auf Achtung des Privatlebens und des in Artikel 8 verankerten Rechts auf Schutz personenbezogener Daten, gesetzlich vorgesehen sein, den Wesensgehalt dieser Rechte achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sein sowie einer dem Gemeinwohl dienenden Zielsetzung oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (EuGH, Große Kammer, 6. Oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, Randnr. 64).

B.18.6. In seinem Gutachten 1/15 vom 26. Juli 2017 über den Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen stellt der Gerichtshof fest, dass die PNR-Daten Informationen über bestimmte oder bestimmbare natürliche Personen enthalten und ihre Erhebung und Verarbeitung und der Zugang zu diesen Daten somit das in Artikel 7 der Charta garantierte Recht auf Achtung des Privatlebens und das durch Artikel 8 der Charta garantierte Recht auf den Schutz personenbezogener Daten berühren können (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, PNR-Abkommen EU-Kanada, ECLI:EU:C:2017:592, Randnrn. 122-126).

Hinsichtlich der Einschränkungen, denen Artikel 7 und 8 der Charta unterliegen können, ist der Gerichtshof folgender Auffassung: « Die in den Art. 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden » (ebenda, Randnr. 136):

« 137. Insoweit ist auch darauf hinzuweisen, dass nach Artikel 8 Absatz 2 der Charta personenbezogene Daten nur ' für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage ' verarbeitet werden dürfen.

138. Überdies muss nach Artikel 52 Absatz 1 der Charta jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten (Satz 1); unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Satz 2) » (ebenda).

B.19.1 Artikel 22 der Verfassung behält dem zuständigen Gesetzgeber die Befugnis vor, festzulegen, in welchen Fällen und unter welchen Bedingungen das Recht auf Achtung des Privatlebens beeinträchtigt werden kann. Somit garantiert er jedem Bürger, dass eine Einmischung in die Ausübung dieses Rechts nur aufgrund von Regeln erfolgen darf, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Ermächtigung einer anderen Gewalt steht jedoch nicht im Widerspruch zum Legalitätsprinzip, sofern die Ermächtigung ausreichend präzise beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

B.19.2. Neben dem formalen Erfordernis der Legalität wird durch Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention und mit den Artikeln 7, 8 und 52 der Charta der Grundrechte der Europäischen Union ebenfalls die Verpflichtung auferlegt, dass die Einmischung in das Recht auf Achtung des Privatlebens und das Recht auf den Schutz personenbezogener Daten deutlich und ausreichend präzise formuliert wird, damit es möglich ist, die Fälle vorherzusehen, in denen der Gesetzgeber eine solche Einmischung in das Recht auf Achtung des Privatlebens erlaubt.

Auf dem Gebiet des Schutzes personenbezogener Daten bedeutet dieses Erfordernis der Vorhersehbarkeit, dass ausreichend präzise vorgesehen werden muss, unter welchen Umständen Verarbeitungen von personenbezogenen Daten erlaubt sind (EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). Das Erfordernis, dass die Einschränkung gesetzlich vorgesehen sein muss, bedeutet insbesondere, dass die gesetzliche Grundlage für den Eingriff in diese Rechte den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen muss (EuGH, 6. Oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, Randnr. 65).

Deshalb muss es jeder Person möglich sein, sich ein ausreichend klares Bild von den verarbeiteten Daten, den an einer bestimmten Datenverarbeitung beteiligten Personen sowie den Bedingungen und den Zwecken der Verarbeitung zu machen.

B.20.1. Artikel 23 der DSGVO bestimmt:

« 1. Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.

2. Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) die Kategorien personenbezogener Daten,

c) den Umfang der vorgenommenen Beschränkungen,

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung,

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist ».

Gemäß dieser Bestimmung müssen Beschränkungen der darin genannten Verpflichtungen der Verantwortlichen und der Rechte der betroffenen Personen gesetzlich vorgesehen sein, den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zur Verwirklichung des verfolgten Ziels darstellen, sowie die in Absatz 2 formulierten spezifischen Anforderungen erfüllen (EuGH, Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, ECLI:EU:C:2020:791, Randnrn. 209-210; 10. Dezember 2020, C-620/19, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, Randnr. 46).

B.20.2. Artikel 2 der DSGVO bestimmt:

« 1. Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

2. Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten:

[...]

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

[...] ».

B.20.3. Der Erwägungsgrund 19 der DSGVO bestimmt:

« Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie der freie Verkehr dieser Daten sind in einem eigenen Unionsrechtsakt geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zu den vorstehenden Zwecken verwendet werden, einem spezifischeren Unionsrechtsakt, nämlich der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates unterliegen. Die Mitgliedstaaten können die zuständigen Behörden im Sinne der Richtlinie (EU) 2016/680 mit Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich dieser Verordnung fällt,

als sie in den Anwendungsbereich des Unionsrechts fällt. In Bezug auf die Verarbeitung personenbezogener Daten durch diese Behörden für Zwecke, die in den Anwendungsbereich dieser Verordnung fallen, sollten die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen können, um die Anwendung der Vorschriften dieser Verordnung anzupassen. In den betreffenden Bestimmungen können die Auflagen für die Verarbeitung personenbezogener Daten durch diese zuständigen Behörden für jene anderen Zwecke präziser festgelegt werden, wobei der verfassungsmäßigen, organisatorischen und administrativen Struktur des betreffenden Mitgliedstaats Rechnung zu tragen ist. Soweit diese Verordnung für die Verarbeitung personenbezogener Daten durch private Stellen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter wichtiger Interessen darstellt, wozu auch die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Dies ist beispielsweise im Rahmen der Bekämpfung der Geldwäsche oder der Arbeit kriminaltechnischer Labors von Bedeutung ».

Wie aus diesem Erwägungsgrund hervorgeht, fällt die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung grundsätzlich nicht unter die DSGVO, sondern unter die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates » (nachstehend: Polizeirichtlinie).

B.20.4. Die Polizeirichtlinie legt in den Bereichen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit spezifische Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit fest, wobei den Besonderheiten dieser Tätigkeiten Rechnung getragen wird.

Artikel 1 Absatz 1 der Polizeirichtlinie bestimmt:

« Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit ».

Artikel 9 Absätze 1 und 2 derselben Richtlinie bestimmt:

« 1. Personenbezogene Daten, die von zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke erhoben werden, dürfen nicht für andere als die in Artikel 1 Absatz 1 genannten Zwecke verarbeitet werden, es sei denn, eine derartige Verarbeitung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig. Wenn personenbezogene Daten für solche andere Zwecke verarbeitet werden, gilt die Verordnung (EU) 2016/679, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

2. Sind nach dem Recht der Mitgliedstaaten zuständige Behörden mit der Wahrnehmung von Aufgaben betraut, die sich nicht mit den für die in Artikel 1 Absatz 1 genannten Zwecke wahrgenommenen Aufgaben decken, gilt die Verordnung (EU) 2016/679 für die Verarbeitung zu diesen Zwecken — wozu auch im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke zählen —, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt ».

Im Erwägungsgrund 11 der Polizeirichtlinie ist diesbezüglich präzisiert, dass

« diesen Bereichen durch eine Richtlinie Rechnung getragen werden [sollte], die spezifische Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, enthält, wobei den Besonderheiten dieser Tätigkeiten Rechnung getragen wird. Diese zuständigen Behörden können nicht nur staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden einschließen, sondern auch alle anderen Stellen oder Einrichtungen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke dieser Richtlinie übertragen wurde. Wenn solche Stellen oder Einrichtungen jedoch personenbezogene Daten zu anderen Zwecken als denen dieser Richtlinie verarbeiten, gilt die Verordnung (EU) 2016/679. Daher gilt die Verordnung (EU) 2016/679 in Fällen, in denen eine Stelle oder Einrichtung personenbezogene Daten zu anderen Zwecken erhebt und diese personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der sie unterliegt, weiterverarbeitet. Zum Beispiel speichern Finanzinstitute zum Zwecke der Ermittlung, Aufdeckung oder Verfolgung von Straftaten bestimmte personenbezogene Daten, die sie verarbeiten, und stellen sie nur den zuständigen nationalen Behörden in bestimmten Fällen und in Einklang mit dem Recht der Mitgliedstaaten zur Verfügung. Eine Stelle oder Einrichtung, die personenbezogene Daten im Rahmen des Anwendungsbereichs dieser Richtlinie für solche Behörden verarbeitet, sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments und durch die für Auftragsverarbeiter nach dieser Richtlinie geltenden Bestimmungen gebunden sein, wobei die Anwendung der Verordnung (EU) 2016/679 in Bezug auf die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter außerhalb des Anwendungsbereichs dieser Richtlinie durchführt, unberührt bleibt ».

Im Erwägungsgrund 34 der Polizeirichtlinie ist weiter erläutert:

« [...] Wurden personenbezogene Daten ursprünglich von einer zuständigen Behörde für einen der Zwecke dieser Richtlinie erhoben, so sollte die Verordnung (EU) 2016/679 für die Verarbeitung dieser Daten für andere Zwecke als diejenigen dieser Richtlinie gelten, wenn eine solche Verarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist. Insbesondere sollte die Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten für Zwecke gelten, die außerhalb des Anwendungsbereichs dieser Richtlinie liegen. Für die Verarbeitung personenbezogener Daten durch einen Empfänger, der keine zuständige Behörde im Sinne dieser Richtlinie ist oder nicht als solche handelt und gegenüber dem personenbezogene Daten von einer zuständigen Behörde rechtmäßig offengelegt werden, sollte die Verordnung (EU) 2016/679 gelten. [...] ».

B.21.1. Der Ministerrat macht hauptsächlich eine Einrede der Unzulässigkeit des ersten Klagegrunds geltend, insofern er aus einem Verstoß gegen Artikel 23 der DSGVO abgeleitet ist, der nicht auf das Gesetz vom 25. Dezember 2016 anwendbar sei.

B.21.2. Das Gesetz vom 25. Dezember 2016 regelt die Erhebung und Übermittlung von PNR-Daten, die Schaffung einer Passagierdatenbank, die von der PNR-Zentralstelle verwaltet wird, die Verarbeitungszwecke dieser Datenbank und den Zugriff auf diese Datenbank.

Im Wesentlichen setzt das Gesetz vom 25. Dezember 2016 die PNR-Richtlinie um, aber es geht, wie in seinem Artikel 2 angegeben ist und wie in B.2 erwähnt wurde, inhaltlich auch über die Umsetzung dieser Richtlinie hinaus.

B.21.3. Auf die Frage des Verfassungsgerichtshofes, ob Artikel 23 in Verbindung mit Artikel 2 Absatz 2 Buchstabe *d)* der DSGVO dahin auszulegen ist, dass er für nationale Rechtsvorschriften wie das Gesetz vom 25. Dezember 2016 gilt, mit denen die Bestimmungen sowohl der PNR-Richtlinie als auch der API-Richtlinie und der Richtlinie 2010/65/EU umgesetzt werden, hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 geantwortet, dass aus dem Wortlaut von Artikel 2 Absatz 2 Buchstabe *d)* der DSGVO « klar hervor[geht], dass zwei Voraussetzungen erfüllt sein müssen, damit eine Datenverarbeitung unter die dort vorgesehene Ausnahme fällt » und dass « während die erste von ihnen die Zwecke der Verarbeitung - Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit - betrifft, [...] es in der zweiten Voraussetzung um den Urheber der Verarbeitung [geht], bei dem es sich um eine ‘ zuständige Behörde ’ im Sinne dieser Bestimmung handeln muss » (Randnr. 67), wobei die in Artikel 2 Absatz 2 Buchstabe *d)* der DSGVO erwähnte Ausnahme « wie die übrigen in Art. 2 Abs. 2 der DSGVO vorgesehenen Ausnahmen von ihrem Anwendungsbereich, eng auszulegen [ist] » (Randnr. 70):

« 71. Nach dem 19. Erwägungsgrund der DSGVO beruht die genannte Ausnahme darauf, dass Verarbeitungen personenbezogener Daten, die von den zuständigen Behörden u. a. zum Zweck der Verhütung und Aufdeckung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, vorgenommen werden, in einem spezifischeren Rechtsakt der Union geregelt sind, und zwar in der Richtlinie 2016/680, die am selben Tag wie die DSGVO erlassen wurde (Urteil vom 22. Juni 2021, *Latvijas Republikas Saeima* [Strafpunkte], C-439/19, EU:C:2021:504, Rn. 69).

72. Wie im Übrigen in den Erwägungsgründen 9 bis 11 der Richtlinie 2016/680 klargestellt wird, enthält sie spezifische Vorschriften zum Schutz natürlicher Personen bei diesen Verarbeitungen, wobei den Besonderheiten der Tätigkeiten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit Rechnung getragen wird, während in der DSGVO allgemeine Bestimmungen zum Schutz dieser Personen festgelegt werden, die auf die genannten Verarbeitungen Anwendung finden sollen, wenn die Richtlinie 2016/680 als der spezifischere Rechtsakt nicht anwendbar ist. Insbesondere gilt die DSGVO nach dem elften Erwägungsgrund dieser Richtlinie für die Verarbeitung personenbezogener Daten durch eine „zuständige Behörde" im Sinne ihres Art. 3 Nr. 7, die aber anderen als den von ihr vorgesehenen Zwecken dient (vgl. in diesem Sinne Urteil vom 22. Juni 2021, *Latvijas Republikas Saeima* [Strafpunkte], C-439/19, EU:C:2021:504, Rn. 70).

73. Zur ersten oben in Rn. 67 genannten Voraussetzung und insbesondere zu den Zwecken, die mit den in der PNR-Richtlinie vorgesehenen Verarbeitungen personenbezogener Daten verfolgt werden, ist darauf hinzuweisen, dass nach Art. 1 Abs. 2 dieser Richtlinie die PNR-Daten ausschließlich zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität verarbeitet werden dürfen. Diese Zwecke gehören zu den in Art. 2 Abs. 2 Buchst. d der DSGVO und in Art. 1 Abs. 1 der Richtlinie 2016/680 genannten, so dass solche Verarbeitungen unter die in Art. 2 Abs. 2 Buchst. d der DSGVO vorgesehene Ausnahme und folglich in den Anwendungsbereich dieser Richtlinie fallen können.

74. Bei den in der API-Richtlinie und der Richtlinie 2010/65 vorgesehenen Verarbeitungen, die zu anderen als den in Art. 2 Abs. 2 Buchst. d der DSGVO und in Art. 1 Abs. 1 der Richtlinie 2016/680 vorgesehenen Zwecken dienen, ist dies hingegen nicht der Fall.

75. Die API-Richtlinie bezweckt nämlich nach ihren Erwägungsgründen 1, 7 und 9 sowie ihrem Art. 1, die Grenzkontrollen zu verbessern und die illegale Einwanderung zu bekämpfen, indem die Beförderungsunternehmen Angaben über die beförderten Personen vorab an die zuständigen nationalen Behörden übermitteln. Überdies zeigen mehrere Erwägungsgründe und Bestimmungen dieser Richtlinie, dass die zu ihrer Durchführung vorgesehenen Verarbeitungen von Daten in den Anwendungsbereich der DSGVO fallen. So heißt es in ihrem zwölften Erwägungsgrund: ' Die Richtlinie [95/46] findet auf die Verarbeitung personenbezogener Daten durch die Behörden der Mitgliedstaaten Anwendung '. Außerdem können die Mitgliedstaaten die API-Daten nach Art. 6 Abs. 1 Unterabs. 5 der API-Richtlinie auch zu Strafverfolgungszwecken verwenden, sofern die ' Datenschutzbestimmungen der Richtlinie [95/46] ' gewahrt werden; diese Wendung findet sich ferner in Art. 6 Abs. 1 Unterabs. 3. Desgleichen wird u. a. im neunten Erwägungsgrund der API-Richtlinie die Wendung ' unbeschadet der Richtlinie [95/46] ' verwendet. Schließlich sieht Art. 6 Abs. 2 der API-Richtlinie vor, dass die beförderten Personen von den Beförderungsunternehmern ' gemäß der Richtlinie [95/46] ' zu unterrichten sind.

76. Was die Richtlinie 2010/65 betrifft, geht aus ihrem zweiten Erwägungsgrund und aus ihrem Art. 1 Abs. 1 hervor, dass ihr Zweck die Vereinfachung und Harmonisierung der Verwaltungsverfahren im Seeverkehr durch die allgemeine Nutzung elektronischer Systeme für die Datenübermittlung und durch die Rationalisierung der Meldeförmlichkeiten ist, um den Seeverkehr zu erleichtern und den Verwaltungsaufwand für Seeschifffahrtsunternehmen zu verringern. Art. 8 Abs. 2 dieser Richtlinie bestätigt, dass die zu ihrer Umsetzung vorgesehenen Datenverarbeitungen in den Anwendungsbereich der DSGVO fallen, da die Mitgliedstaaten durch diese Bestimmung verpflichtet werden, in Bezug auf personenbezogene Daten die Einhaltung der Richtlinie 95/46 sicherzustellen.

77. Daraus folgt, dass die in nationalen Rechtsvorschriften, mit denen die Bestimmungen der API-Richtlinie und der Richtlinie 2010/65 in innerstaatliches Recht umgesetzt werden, vorgesehenen Verarbeitungen von Daten in den Anwendungsbereich der DSGVO fallen. Dagegen können die in nationalen Rechtsvorschriften, mit denen die PNR-Richtlinie in innerstaatliches Recht umgesetzt wird, vorgesehenen Verarbeitungen von Daten nach der in Art. 2 Abs. 2 Buchst. d der DSGVO enthaltenen Ausnahme von ihrem Anwendungsbereich ausgenommen sein, sofern die zweite oben in Rn. 67 genannte Voraussetzung erfüllt ist, dass der Urheber der Verarbeitungen eine zuständige Behörde im Sinne der letztgenannten Bestimmung ist.

78. Zu dieser zweiten Voraussetzung hat der Gerichtshof entschieden, dass die in Art. 3 Abs. 7 der Richtlinie 2016/680 enthaltene Definition des Begriffs ' zuständige Behörde ' auf Art. 2 Abs. 2 Buchst. d der DSGVO entsprechend anzuwenden ist (vgl. in diesem Sinne Urteil vom 22. Juni 2021, *Latvijas Republikas Saeima* [Strafpunkte], C-439/19, EU:C:2021:504, Rn. 69).

79. Nach den Art. 4 und 7 der PNR-Richtlinie muss jeder Mitgliedstaat eine für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständige Behörde als seine PNR-Zentralstelle benennen und eine Liste der zuständigen Behörden erstellen, die berechtigt sind, PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von der PNR-Zentralstelle anzufordern oder entgegenzunehmen, wobei Letztere auch die in diesem Bereich zuständigen Behörden sind (Art. 7 Abs. 2 der PNR-Richtlinie).

80. Daraus ergibt sich, dass die Verarbeitungen von PNR-Daten durch die PNR-Zentralstelle und die erwähnten zuständigen Behörden zu solchen Zwecken die beiden oben in Rn. 67 genannten Voraussetzungen erfüllen, so dass für diese Verarbeitungen - neben den Bestimmungen der PNR-Richtlinie selbst - die Bestimmungen der Richtlinie 2016/680 und nicht der DSGVO gelten, was im Übrigen durch den 27. Erwägungsgrund der PNR-Richtlinie bestätigt wird.

81. Da Wirtschaftsteilnehmer wie die Fluggesellschaften, auch wenn sie gesetzlich zur Übermittlung von PNR-Daten verpflichtet sind, durch diese Richtlinie weder mit der Ausübung öffentlicher Gewalt betraut noch mit hoheitlichen Befugnissen ausgestattet werden, können sie hingegen nicht als zuständige Behörden im Sinne von Art. 3 Abs. 7 der Richtlinie 2016/680 und Art. 2 Abs. 2 Buchst. d der DSGVO angesehen werden, so dass die Erhebung dieser Daten und ihre Übermittlung an die PNR-Zentralstelle durch die Fluggesellschaften unter diese Verordnung fallen. Das Gleiche gilt in einer Situation wie der im Gesetz vom 25. Dezember 2016 vorgesehenen, wonach die Erfassung und Übermittlung der Daten von anderen Beförderungsunternehmen oder von den Reisebüros vorgenommen werden.

82. Schließlich wirft das vorlegende Gericht die Frage nach den etwaigen Auswirkungen des Erlasses nationaler Rechtsvorschriften zur Umsetzung der Bestimmungen sowohl der PNR-Richtlinie als auch der API-Richtlinie und der Richtlinie 2010/65 auf. Insoweit ist darauf hinzuweisen, dass die in den beiden letztgenannten Richtlinien vorgesehenen Datenverarbeitungen in den Anwendungsbereich der DSGVO fallen, die allgemeine Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten enthält (siehe oben, Rn. 72 und 75 bis 77).

83. Fällt eine auf der Grundlage dieser Rechtsvorschriften vorgenommene Datenverarbeitung unter die API-Richtlinie und/oder die Richtlinie 2010/65, ist die DSGVO somit darauf anwendbar. Das Gleiche gilt für eine auf dieser Grundlage vorgenommene Datenverarbeitung, die hinsichtlich ihres Zwecks nicht nur unter die PNR-Richtlinie fällt, sondern auch unter die API-Richtlinie und/oder die Richtlinie 2010/65. Schließlich ist, wenn eine auf dieser Grundlage vorgenommene Datenverarbeitung hinsichtlich ihres Zwecks nur unter die PNR-Richtlinie fällt, die DSGVO anwendbar, sofern es sich um die Erhebung von PNR-Daten und ihre Übermittlung an die PNR-Zentralstelle durch Fluggesellschaften handelt. Erfolgt eine solche Verarbeitung durch die PNR-Zentralstelle oder die zuständigen Behörden zu den in Art. 1 Abs. 2 der PNR-Richtlinie genannten Zwecken, fällt sie hingegen unter das nationale Recht sowie die Richtlinie 2016/680.

84. Nach alledem ist auf die erste Frage zu antworten, dass Art. 2 Abs. 2 Buchst. d und Art. 23 der DSGVO dahin auszulegen sind, dass diese Verordnung für die Verarbeitung personenbezogener Daten gilt, die in nationalen Rechtsvorschriften vorgesehen ist, mit denen die Bestimmungen sowohl der API-Richtlinie als auch der Richtlinie 2010/65 und der PNR-Richtlinie in Bezug auf die Verarbeitung von Daten durch private Wirtschaftsteilnehmer sowie in Bezug auf die nur oder auch unter die API-Richtlinie oder die Richtlinie 2010/65 fallende Verarbeitung von Daten durch Behörden in innerstaatliches Recht umgesetzt werden sollen. Die Verordnung gilt hingegen nicht für die in nationalen Rechtsvorschriften vorgesehene, nur unter die PNR-Richtlinie fallende Verarbeitung von Daten durch die PNR-Zentralstelle oder die zuständigen Behörden zu den in Art. 1 Abs. 2 dieser Richtlinie genannten Zwecken ».

B.21.4. Aus dem Vorstehenden ergibt sich, dass die DSGVO für Verarbeitungen personenbezogener Daten gilt, die in nationalen Rechtsvorschriften wie dem Gesetz vom 25. Dezember 2016 vorgesehen sind, mit denen die Bestimmungen sowohl der PNR-Richtlinie als auch der API-Richtlinie und der Richtlinie 2010/65/EU umgesetzt werden sollen, entweder (1) wenn eine auf der Grundlage dieser Rechtsvorschriften vorgenommene Datenverarbeitung unter die API-Richtlinie und/oder die Richtlinie 2010/65/EU fällt, oder (2) wenn eine auf dieser Grundlage vorgenommene Datenverarbeitung hinsichtlich ihres Zwecks nicht nur unter die PNR-Richtlinie fällt, sondern auch unter die API-Richtlinie und/oder die Richtlinie 2010/65/EU, oder (3) wenn eine auf dieser Grundlage vorgenommene Datenverarbeitung hinsichtlich ihres Zwecks nur unter die PNR-Richtlinie fällt, es sich aber um die Erhebung von PNR-Daten und ihre Übermittlung an die PNR-Zentralstelle durch Fluggesellschaften oder andere Beförderungsunternehmen oder Reisebüros handelt.

Wenn hingegen eine auf der Grundlage derselben Rechtsvorschriften vorgenommene Datenverarbeitung hinsichtlich ihres Zwecks nur unter die PNR-Richtlinie fällt und durch die PNR-Zentralstelle oder die zuständigen Behörden zu den in Artikel 1 Absatz 2 der PNR-Richtlinie genannten Zwecken vorgenommen wird, gilt die DSGVO nicht, sondern diese Verarbeitung fällt unter das nationale Recht und die Polizeirichtlinie.

B.21.5. Der Gerichtshof berücksichtigt daher bei der Prüfung des Klagegrunds Artikel 23 der DSGVO, es sei denn, die auf der Grundlage des Gesetzes vom 25. Dezember 2016 vorgenommene Datenverarbeitung fällt hinsichtlich ihres Zwecks nur unter die PNR-Richtlinie und wird durch die PNR-Zentralstelle oder die zuständigen Behörden zu den in Artikel 1 Absatz 2 der PNR-Richtlinie genannten Zwecken vorgenommen.

B.21.6. Im Übrigen stellt der Gerichtshof fest, dass die klagenden Parteien aus dieser Bestimmung keine anderen Argumente herleiten als den aus dem Verstoß gegen die Artikel 7 und 8 der Charta abgeleiteten Argumente.

B.21.7. Die Einrede des Ministerrates wird in diesem Maße abgewiesen.

In Bezug auf die Gültigkeit der PNR-Richtlinie

B.22.1. Auf die Frage des Verfassungsgerichtshofes nach der Gültigkeit der PNR-Richtlinie hat der Gerichtshof der Europäischen Union in dem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 geantwortet, « da eine Auslegung der PNR-Richtlinie im Licht der Art. 7, 8 und 21 sowie von Art. 52 Abs. 1 der Charta die Vereinbarkeit dieser Richtlinie mit den genannten Artikeln der Charta gewährleistet, [hat] die Prüfung der Fragen 2 bis 4 und 6 nichts ergeben, was die Gültigkeit der Richtlinie berühren könnte » (Randnr. 228).

B.22.2. Zunächst weist der Gerichtshof der Europäischen Union darauf hin, dass « ein Rechtsakt der Union nach einem allgemeinen Auslegungsgrundsatz so weit wie möglich in einer seine Gültigkeit nicht in Frage stellenden Weise und im Einklang mit dem gesamten Primärrecht und insbesondere mit den Bestimmungen der Charta auszulegen ist » (Randnr. 86) und dass die Mitgliedstaaten « bei der Durchführung dieser Maßnahmen nicht nur ihr nationales Recht in einer mit der fraglichen Richtlinie konformen Weise auslegen, sondern auch darauf achten [müssen], dass sie sich nicht auf eine Auslegung der Richtlinie stützen, die mit den durch die Rechtsordnung der Union geschützten Grundrechten oder mit anderen in dieser Rechtsordnung anerkannten allgemeinen Grundsätzen kollidiert » (Randnr. 87).

Was die PNR-Richtlinie anbelangt, stellt der Gerichtshof der Europäischen Union fest, dass « in ihren Erwägungsgründen 15, 20, 22, 25, 36 und 37 die Bedeutung hervorgehoben wird, die der Unionsgesetzgeber - unter Bezugnahme auf ein hohes Datenschutzniveau - der uneingeschränkten Achtung der in den Art. 7, 8 und 21 der Charta verankerten Grundrechte sowie dem Grundsatz der Verhältnismäßigkeit beimisst » (Randnr. 88) sowie dass « die Kommission bei der Überprüfung der PNR-Richtlinie nach deren Art. 19 Abs. 2 insbesondere ' die Einhaltung des einschlägigen Schutzstandards bezüglich personenbezogener Daten ', ' die Erforderlichkeit und Verhältnismäßigkeit der Erhebung und Verarbeitung von PNR-Daten für jeden der in dieser Richtlinie genannten Zwecke ' sowie ' die Datenspeicherungsfristen ' berücksichtigen [muss] » (Randnr. 90).

B.22.3. Zu den sich aus der PNR-Richtlinie ergebenden Eingriffen in die durch die Artikel 7 und 8 der Charta garantierten Grundrechte stellt der Gerichtshof der Europäischen Union fest, dass die PNR-Richtlinie « mit fraglos schwerwiegenden Eingriffen in die durch die Art. 7 und 8 der Charta garantierten Rechte verbunden ist, insbesondere soweit sie auf die Schaffung eines Systems kontinuierlicher, nicht zielgerichteter und systematischer Überwachung abzielt, das die automatisierte Überprüfung personenbezogener Daten sämtlicher Personen einschließt, die Luftverkehrsdienste in Anspruch nehmen » (Randnr. 111):

« 97. Somit stellen sowohl die in Art. 1 Abs. 1 Buchst. a der PNR-Richtlinie in Verbindung mit deren Art. 8 vorgesehene Übermittlung der PNR-Daten durch die Fluggesellschaften an die PNR-Zentralstelle des betreffenden Mitgliedstaats als auch die Festlegung der Bedingungen für die Speicherung dieser Daten, ihre Verwendung und ihre etwaige Weitergabe an die zuständigen Behörden dieses Mitgliedstaats, an die PNR-Zentralstellen und die zuständigen Behörden der übrigen Mitgliedstaaten, an Europol oder an die Behörden von Drittstaaten, wie es insbesondere die Art. 6, 7, 9 und 10 bis 12 dieser Richtlinie gestatten, Eingriffe in die durch die Art. 7 und 8 der Charta garantierten Rechte dar

98. Zur Schwere dieser Eingriffe ist erstens festzustellen, dass die PNR-Richtlinie nach ihrem Art. 1 Abs. 1 Buchst. a in Verbindung mit ihrem Art. 8 die systematische und kontinuierliche Übermittlung der PNR-Daten aller Fluggäste von Drittstaatsflügen im Sinne von Art. 3 Nr. 2 der Richtlinie, d. h. von Flügen zwischen Drittstaaten und der Union, an die PNR-Zentralstelle vorsieht. Wie der Generalanwalt in Nr. 73 seiner Schlussanträge ausgeführt hat, ist mit einer solchen Übermittlung ein allgemeiner Zugang der PNR-Zentralstellen zu allen übermittelten PNR-Daten sämtlicher Personen verbunden, die Luftverkehrsdienstleistungen nutzen, und zwar unabhängig von der späteren Verwendung dieser Daten..

99. Zweitens können die Mitgliedstaaten nach Art. 2 Abs. 1 der PNR-Richtlinie entscheiden, diese Richtlinie auf EU-Flüge im Sinne ihres Art. 3 Nr. 3 anzuwenden, und nach Art. 2 Abs. 2 gelten in diesem Fall alle Bestimmungen der Richtlinie ‘ für EU-Flüge so, als handele es sich um Drittstaatsflüge, und für PNR-Daten zu EU-Flügen so, als handele es sich um PNR-Daten zu Drittstaatsflügen ’.

100. Drittens können, auch wenn einige der in Anhang I der PNR-Richtlinie aufgezählten und oben in Rn. 93 zusammengefassten PNR-Daten für sich genommen nicht geeignet sein dürften, genaue Informationen über das Privatleben der betreffenden Personen zu liefern, diese Daten zusammen betrachtet u. a. einen gesamten Reiseverlauf, Reisegewohnheiten, Beziehungen zwischen zwei oder mehreren Personen sowie Informationen über die finanzielle Situation der Fluggäste, ihre Ernährungsgewohnheiten oder ihren Gesundheitszustand offenbaren, und sie könnten sogar sensible Daten über die Fluggäste liefern (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 128).

101. Viertens sollen nach Art. 6 Abs. 2 Buchst. a und b der PNR-Richtlinie die von den Fluggesellschaften übermittelten Daten nicht nur einer Vorabüberprüfung vor der planmäßigen Ankunft der Fluggäste oder ihrem geplanten Abflug unterzogen werden, sondern auch einer nachträglichen Überprüfung.

102. Zur Vorabüberprüfung ergibt sich aus Art. 6 Abs. 2 Buchst. a und Abs. 3 der PNR-Richtlinie, dass sie von den PNR-Zentralstellen der Mitgliedstaaten systematisch und automatisiert durchgeführt wird, d. h. kontinuierlich und unabhängig davon, ob es irgendeinen Anhaltspunkt dafür gibt, dass die betreffenden Personen an terroristischen Straftaten oder an schwerer Kriminalität beteiligt sein könnten. Zu diesem Zweck sehen die genannten Bestimmungen vor, dass die PNR-Daten mit ‘ maßgeblichen ’ Datenbanken und anhand ‘ im Voraus festgelegter Kriterien ’ abgeglichen werden können.

103. In diesem Zusammenhang hat der Gerichtshof bereits entschieden, dass der Umfang des mit automatisierten Analysen der PNR-Daten verbundenen Eingriffs in die in den Art. 7 und 8 der Charta verankerten Rechte im Wesentlichen von den im Voraus festgelegten Modellen und Kriterien sowie von den Datenbanken abhängt, auf denen diese Art der Datenverarbeitung beruht (Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 172).

104. Wie der Generalanwalt in Nr. 78 seiner Schlussanträge ausgeführt hat, kann die in Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie vorgesehene Verarbeitung in Form des Abgleichs der PNR-Daten mit ‘ maßgeblichen ’ Datenbanken zusätzliche Informationen über das Privatleben der Fluggäste liefern und insoweit sehr genaue Schlüsse ermöglichen.

105. Was die Verarbeitung der PNR-Daten anhand ‘ im Voraus festgelegter Kriterien ’ (Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie) betrifft, verlangt Art. 6 Abs. 4 der Richtlinie zwar, dass die Überprüfung von Fluggästen mittels dieser Kriterien in nicht diskriminierender Weise erfolgen muss und insbesondere nicht auf einer ganzen Reihe von Eigenschaften beruhen darf, die im letzten Satz von Art. 6 Abs. 4 aufgeführt sind. Außerdem müssen die herangezogenen Kriterien zielgerichtet, verhältnismäßig und bestimmt sein.

106. Der Gerichtshof hat allerdings bereits befunden, dass die automatisierten Analysen der PNR-Daten, da sie anhand von nicht überprüften personenbezogenen Daten durchgeführt werden und auf im Voraus festgelegten Modellen und Kriterien beruhen, zwangsläufig mit einer gewissen Fehlerquote behaftet sind (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 169). Insbesondere geht, wie der Generalanwalt in Nr. 78 seiner Schlussanträge im Wesentlichen ausgeführt hat, aus dem Arbeitspapier der Kommission (SWD[2020] 128 endg.), das ihrem Bericht vom 24. Juli 2020 über die Überprüfung der PNR-Richtlinie beigefügt ist, hervor, dass die Anzahl der aus der automatisierten Verarbeitung gemäß Art. 6 Abs. 3 Buchst. a und b dieser Richtlinie resultierenden Treffer, die sich nach der individuellen Überprüfung mit nicht automatisierten Mitteln als falsch erwiesen haben, erheblich war und sich in den Jahren 2018 und 2019 auf wenigstens fünf von sechs identifizierten Personen belief. Diese Verarbeitungen führen somit zu einer eingehenden Analyse der PNR-Daten für die genannten Personen.

107. Zu der in Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie vorgesehenen nachträglichen Überprüfung der PNR-Daten ergibt sich aus dieser Bestimmung, dass die PNR-Zentralstelle während des in Art. 12 Abs. 2 der Richtlinie genannten Zeitraums von sechs Monaten ab der Übermittlung der PNR-Daten verpflichtet ist, den zuständigen Behörden auf deren Anfrage die PNR-Daten zur Verfügung zu stellen und sie in besonderen Fällen zur Bekämpfung terroristischer Straftaten oder schwerer Kriminalität zu verarbeiten.

108. Außerdem kann die PNR-Zentralstelle, auch wenn die PNR-Daten nach Ablauf der Frist von sechs Monaten durch Unkenntlichmachung bestimmter Datenelemente depersonalisiert werden, gleichwohl nach Art. 12 Abs. 3 der PNR-Richtlinie verpflichtet sein, auf eine solche Anfrage hin die vollständigen PNR-Daten in einer die Identifizierung der betroffenen Person ermöglichenden Form zu übermitteln, sofern berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Art. 6 Abs. 2 Buchst. b der Richtlinie erforderlich ist; eine solche Übermittlung bedarf allerdings der Genehmigung durch eine Justizbehörde oder eine ‘ andere nationale Behörde ’.

109. Fünftens sieht die PNR-Richtlinie in ihrem Art. 12 Abs. 1 ohne nähere Angaben vor, dass die PNR-Daten für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen bzw. von dem er abgegangen ist, in einer Datenbank vorgehalten werden. Angesichts der Tatsache, dass die PNR-Daten, obwohl sie nach Ablauf der ursprünglichen Frist von sechs Monaten durch Unkenntlichmachung bestimmter Datenelemente depersonalisiert werden, in dem in der vorstehenden Randnummer genannten Fall weiterhin in vollständiger Form offengelegt werden können, macht die Richtlinie damit Informationen über das Privatleben der Fluggäste für einen Zeitraum verfügbar, den der Gerichtshof bereits in seinem Gutachten 1/15 (PNR-Abkommen EU–Kanada) vom 26. Juli 2017 (EU:C:2017:592, Rn. 132) als besonders lang bezeichnet hat.

110. In Anbetracht der Üblichkeit der Inanspruchnahme des Luftverkehrs führt eine solche Speicherfrist dazu, dass die PNR-Daten weiter Teile der Bevölkerung der Union im Rahmen des durch die PNR-Richtlinie geschaffenen Systems möglicherweise wiederholt gespeichert und damit während eines erheblichen Zeitraums oder - im Fall von Personen, die mehr als einmal in fünf Jahren mit dem Flugzeug reisen - sogar auf unbestimmte Zeit für Analysen im Rahmen von Vorabüberprüfungen und nachträglichen Überprüfungen der PNR-Zentralstelle und der zuständigen Behörden zur Verfügung stehen ».

B.22.4.1. Zur Rechtfertigung der mit der PNR-Richtlinie verbundenen Eingriffe weist der Gerichtshof der Europäischen Union insbesondere darauf hin, dass « die Möglichkeit für die Mitgliedstaaten, eine Einschränkung der durch die Art. 7 und 8 der Charta garantierten Rechte zu rechtfertigen, zu beurteilen [ist], indem die Schwere des mit einer solchen Einschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die mit ihr verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zu dessen Schwere steht » (Randnr. 116):

« 117. Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss die betreffende Regelung, die den Eingriff enthält, klare und präzise Regeln für die Tragweite und die Anwendung der vorgesehenen Maßnahmen sowie Mindesterfordernisse aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Die Notwendigkeit, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden. Diese Erwägungen gelten in besonderem Maß, wenn sich den PNR-Daten sensible Informationen über die beförderten Personen entnehmen lassen (Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 141, und Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 132 und die dort angeführte Rechtsprechung).

118. Eine Regelung, die eine Vorratsspeicherung personenbezogener Daten vorsieht, muss daher stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 191 und die dort angeführte Rechtsprechung, sowie Urteile vom 3. Oktober 2019, *A u. a.*, C-70/18, EU:C:2019:823, Rn. 63, und vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 133).

a) Zur Achtung des Grundsatzes der Gesetzmäßigkeit und des Wesensgehalts der fraglichen Grundrechte

119. Die Einschränkung der Ausübung der durch die Art. 7 und 8 der Charta garantierten Grundrechte, die sich aus dem durch die PNR-Richtlinie geschaffenen System ergibt, ist in einem Gesetzgebungsakt der Union vorgesehen. Zur Frage, ob im Einklang mit der oben in Rn. 114 angeführten Rechtsprechung die Richtlinie als Unionsrechtsakt, der den Eingriff in diese Rechte ermöglicht, den Umfang der Einschränkung ihrer Ausübung selbst festlegt, ist festzustellen, dass die Bestimmungen der PNR-Richtlinie sowie ihre Anhänge I und II zum einen eine Aufzählung der PNR-Daten enthalten und zum anderen ihre Verarbeitungen regeln, indem sie insbesondere deren Zwecke und Modalitäten festlegen. Im Übrigen deckt sich diese Frage weitgehend mit der oben in Rn. 117 angesprochenen Frage der Wahrung des Erfordernisses der Verhältnismäßigkeit (vgl. in diesem Sinne Urteil vom 16. Juli 2020, *Facebook Ireland und Schrems*, C-311/18, EU:C:2020:559, Rn. 180) und wird in den Rn. 125 ff. des vorliegenden Urteils geprüft.

120. Was die Achtung des Wesensgehalts der in den Art. 7 und 8 der Charta verankerten Grundrechte anbelangt, können die PNR-Daten zwar unter Umständen sehr genaue Informationen über das Privatleben einer Person offenbaren. Da sich diese Informationen aber ihrer Art nach auf bestimmte, insbesondere die Flugreisen dieser Person betreffende Aspekte des Privatlebens beschränken und da die PNR-Richtlinie in ihrem Art. 13 Abs. 4 die Verarbeitung sensibler Daten im Sinne von Art. 9 Abs. 1 der DSGVO ausdrücklich verbietet, ermöglichen die von der Richtlinie erfassten Daten für sich genommen keinen umfassenden Einblick in das Privatleben einer Person. Außerdem werden in Art. 1 Abs. 2 in Verbindung mit Art. 3 Nrn. 8 und 9 sowie in Anhang II der Richtlinie die Zwecke der Verarbeitung dieser Daten abgegrenzt. Schließlich enthält die Richtlinie in ihren Art. 4 bis 15 Regeln für die Übermittlung, die Verarbeitungen und die Speicherung der Daten sowie Regeln, die insbesondere die Sicherheit, die Vertraulichkeit und die Unversehrtheit der Daten gewährleisten und sie vor rechtswidrigen Zugriffen und Verarbeitungen schützen sollen. Unter diesen Umständen berühren die mit der PNR-Richtlinie verbundenen Eingriffe nicht den Wesensgehalt der in den Art. 7 und 8 der Charta verankerten Grundrechte.

b) Zu der dem Gemeinwohl dienenden Zielsetzung und zur Eignung der Verarbeitungen der PNR-Daten in Anbetracht dieser Zielsetzung

121. Zur Frage, ob mit dem durch die PNR-Richtlinie geschaffenen System eine dem Gemeinwohl dienende Zielsetzung verfolgt wird, geht aus ihren Erwägungsgründen 5, 6 und 15 hervor, dass die Richtlinie die innere Sicherheit in der Union gewährleisten und damit das Leben und die Sicherheit von Personen schützen soll und zugleich einen Rechtsrahmen schaffen soll, der ein hohes Schutzniveau der Grundrechte der Fluggäste garantiert, insbesondere der Rechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten bei der Verarbeitung von PNR-Daten durch die zuständigen Behörden.

122. Insoweit bestimmt Art. 1 Abs. 2 der PNR-Richtlinie, dass die nach Maßgabe dieser Richtlinie erhobenen PNR-Daten ausschließlich zum Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gemäß ihrem Art. 6 Abs. 2 Buchst. a bis c verarbeitet werden dürfen. Dabei handelt es sich unzweifelhaft um dem Gemeinwohl dienende Zielsetzungen, die auch schwere Eingriffe in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte rechtfertigen können (vgl. in diesem Sinne Urteil vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU:C:2014:238, Rn. 42, sowie Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 148 und 149)..

123. Was die Eignung des durch die PNR-Richtlinie geschaffenen Systems zur Erreichung der verfolgten Ziele betrifft, vermag zwar die Möglichkeit ‘ falsch negativer ’ Ergebnisse und die erhebliche Zahl ‘ falsch positiver ’ Ergebnisse, die, wie oben in Rn. 106 ausgeführt, in den Jahren 2018 und 2019 bei den in der Richtlinie vorgesehenen automatisierten Verarbeitungen auftraten, die Eignung dieses Systems zu begrenzen. Das bedeutet aber nicht, dass dieses System ungeeignet ist, einen Beitrag zur Verwirklichung des Ziels der Bekämpfung terroristischer Straftaten und schwerer Kriminalität zu leisten. Wie nämlich aus dem oben in Rn. 106 erwähnten Arbeitspapier der Kommission hervorgeht, haben die automatisierten Verarbeitungen nach dieser Richtlinie tatsächlich bereits die Identifizierung von Fluggästen ermöglicht, die im Rahmen der Bekämpfung terroristischer Straftaten und schwerer Kriminalität eine Bedrohung darstellten.

124. Außerdem hängt die Eignung des durch die PNR-Richtlinie geschaffenen Systems - angesichts der einer automatisierten Verarbeitung der PNR-Daten innewohnenden Fehlerquote und insbesondere der erheblichen Zahl ‘ falsch positiver ’ Ergebnisse - im Wesentlichen vom ordnungsgemäßen Ablauf der anschließenden Überprüfung der im Rahmen dieser Verarbeitungen erzielten Ergebnisse mit nicht automatisierten Mitteln ab, was nach der PNR-Richtlinie Aufgabe der PNR-Zentralstelle ist. Die dafür in der Richtlinie vorgesehenen Bestimmungen tragen somit zur Verwirklichung dieser Ziele bei ».

B.22.4.2. Bezüglich der notwendigen Beschaffenheit der Eingriffe, die sich aus der PNR-Richtlinie ergeben, weist der Gerichtshof der Europäischen Union darauf hin, dass « zu prüfen [ist], ob die Eingriffe, die sich aus der PNR-Richtlinie ergeben, auf das absolut Notwendige beschränkt sind, und insbesondere, ob diese Richtlinie klare und präzise Regeln für den Umfang und die Anwendung der von ihr vorgesehenen Maßnahmen enthält und ob das durch sie geschaffene System stets objektiven Kriterien entspricht, die einen Zusammenhang zwischen den eng mit der Buchung und Durchführung von Flugreisen verbundenen PNR-Daten und den mit der Richtlinie verfolgten Zielen – Bekämpfung terroristischer Straftaten und schwerer Kriminalität – herstellen » (Randnr. 125).

Der Gerichtshof der Europäischen Union gelangt zu dem Schluss, dass die Prüfung nichts ergeben hat, was die Gültigkeit der PNR-Richtlinie berühren könnte, « da eine Auslegung der PNR-Richtlinie im Licht der Art. 7, 8 und 21 sowie von Art. 52 Abs. 1 der Charta die Vereinbarkeit dieser Richtlinie mit den genannten Artikeln der Charta gewährleistet » (Randnr. 228) und somit die Grenzen des absolut Notwendigen eingehalten werden, wobei er mehrere Klarstellungen vornimmt bezüglich (1) der von der PNR-Richtlinie erfassten Fluggastdaten (Randnrn. 126-140), (2) der Zwecke der Verarbeitung der PNR-Daten (Randnrn. 141-152), (3) des Zusammenhangs zwischen den PNR-Daten und den Verarbeitungszwecken dieser Daten (Randnrn. 153-157), (4) der Fluggäste und der betroffenen Flüge (Randnrn. 158-175), (5) der Vorabüberprüfung der PNR-Daten mittels automatisierter Verarbeitungen (Randnrn. 176-213) und (6) der nachträglichen Zurverfügungstellung und Überprüfung der PNR-Daten (Randnrn. 214-227).

B.22.5. Bei der Prüfung des Klagegrunds berücksichtigt der Verfassungsgerichtshof diese Klarstellungen des Gerichtshofs der Europäischen Union in Bezug auf die Auslegung der PNR-Richtlinie.

In Bezug auf die Reihenfolge der Prüfung der Beschwerdegründe

B.23.1. Aus der Prüfung des ersten Klagegrunds und der angefochtenen Bestimmungen geht hervor, dass die klagende Partei mehrere Aspekte des Gesetzes vom 25. Dezember 2016 bemängelt.

B.23.2. In seinem Entscheid Nr. 135/2019 vom 17. Oktober 2019 hat der Gerichtshof geurteilt, dass der Klagegrund unbegründet ist, insofern er gegen die Ausführungsmodalitäten des Gesetzes vom 25. Dezember 2016 (Artikel 3 § 2 und Artikel 7 § 3 – B.21 bis B.29) und gegen die Begriffe « Identitätsdokumente » und « Reisedokumente » (Artikel 7 §§ 1 und 2 – B.30 bis B.33) gerichtet ist.

B.23.3. Die Beschwerdegründe, die unter Berücksichtigung der Antwort des Gerichtshofs der Europäischen Union in seinem Urteil vom 21. Juni 2022 noch zu prüfen sind, sind gegen folgende Aspekte gerichtet:

1. die fraglichen Daten (Artikel 4 Nr. 9 und Artikel 9) (B.24 bis B.34);

2. den Begriff des « Passagiers » (Artikel 4 Nr. 10) (B.35 bis B.41);

3. die Verarbeitungszwecke der PNR-Daten (Artikel 8) (B.42 bis B.56);

4. die Verwaltung der Passagierdatenbank und die Verarbeitung der Daten im Rahmen der Vorabüberprüfung und der gezielten Recherchen (Artikel 12 bis 16 und 24 bis 27 und Artikel 50 und 51) (B.57 bis B.70);

5. die Aufbewahrungsdauer der PNR-Daten (Artikel 18) (B.71 bis B.75).

1. *Die fraglichen Daten (Artikel 4 Nr. 9 und Artikel 9)*

B.24. Die klagende Partei vertritt zunächst die Meinung, dass der sehr weit gefasste Anwendungsbereich der in Artikel 4 Nr. 9 und Artikel 9 des Gesetzes vom 25. Dezember 2016 erwähnten Passagierdaten offenkundig in keinem Verhältnis zur verfolgten Zielsetzung steht. Die klagende Partei führt an, dass es zumindest angebracht wäre, die Kategorie der unter Artikel 9 § 1 Nr. 12 des angefochtenen Gesetzes fallenden Daten zu beschränken.

Zudem könnten aus den fraglichen Daten nach Ansicht der klagenden Partei sensible Daten wie die Zugehörigkeit zu einer Gewerkschaftsorganisation, persönliche Neigungen und persönliche oder berufliche Beziehungen hervorgehen.

B.25.1. Gemäß den in B.17 und B18 in Erinnerung gerufenen Grundsätzen muss ein Eingriff in das Recht auf Achtung des Privatlebens durch Verarbeitung von personenbezogenen Daten, hier durch Zugang seitens öffentlicher Behörden zu bestimmten personenbezogenen Daten und deren Nutzung mithilfe besonderer Techniken (EuGHMR, 26. März 1987, *Leander gegen Schweden*, ECLI:CE:ECHR:1987:0326JUD000924881, § 48; Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, ECLI:CE:ECHR:2000:0504JUD002834195, § 46; EuGH, Große Kammer, 8. April 2014, C-293/12 und C-594/12, *Digital Rights Ireland Ltd u.a.*, ECLI:EU:C:2014:238), deshalb eine angemessene Rechtfertigungsgrundlage haben und den vom Gesetzgeber verfolgten Zielen entsprechen.

B.25.2. In Rahmen der Verhältnismäßigkeit berücksichtigen der Europäische Gerichtshof für Menschenrechte und der Gerichtshof der Europäischen Union das etwaige Vorhandensein der in B.19 erwähnten materiellen und prozessualen Garantien in der einschlägigen Regelung.

Bei der Beurteilung der Verhältnismäßigkeit von Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten sind mithin u. a. deren automatischer Charakter, die verwendeten Techniken, der Genauigkeitsgrad, die Relevanz, der gegebenenfalls außergewöhnliche Charakter der zu verarbeitenden Daten, das etwaige Vorhandensein von Maßnahmen zur Begrenzung der Datenspeicherfrist, das etwaige Vorhandensein eines unabhängigen Überwachungssystems, mit dem geprüft werden kann, ob eine Datenspeicherung weiterhin erforderlich ist, das etwaige Vorhandensein von ausreichenden Kontrollrechten und Rechtsbehelfen für die betroffenen Personen, das etwaige Vorhandensein von Garantien zur Vermeidung einer Stigmatisierung der Personen, deren Daten verarbeitet werden, der unterscheidende Charakter der Regelung und das etwaige Vorhandensein von Garantien zur Vermeidung einer falschen Nutzung und von Missbrauch der verarbeiteten personenbezogenen Daten durch öffentliche Behörden zu berücksichtigen (vgl. EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, ECLI:CE:ECHR:2000:0504JUD002834195, § 59; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 101-103, 119, 122 und 124; 18. April 2013, *M.K. gegen Frankreich*, ECLI:CE:ECHR:2013:0418JUD001952209, §§ 37 und 42-44; 18. September 2014, *Brunet gegen Frankreich*, ECLI:CE:ECHR:2014:0918JUD002101010, §§ 35-37; 12. Januar 2016, *Szabó und Vissy gegen Ungarn*, ECLI:CE:ECHR:2016:0112JUD003713814, § 68; EuGH, Große Kammer, 8. April 2014, C-293/12 und C-594/12, *Digital Rights Ireland Ltd u.a.*, ECLI:EU:C:2014:238, §§ 56-66).

B.25.3. In seinem Gutachten 1/15 vom 26. Juli 2017 hat der Gerichtshof ebenfalls darauf hingewiesen, dass eine Einmischung in das Recht auf Schutz personenbezogener Daten auf das « absolut Notwendige » beschränkt sein muss:

« 140. Zum Grundsatz der Verhältnismäßigkeit ist festzustellen, dass der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken (Urteil vom 16. Dezember 2008, *Satakunnan Markkinapörssi und Satamedia*, C-73/07, EU:C:2008:727, Rn. 56, vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU:C:2014:238, Rn. 51 und 52, vom 6. Oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, Rn. 92, und vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 96 und 103).

141. Um diesem Erfordernis zu genügen, muss die betreffende Regelung, die den Eingriff enthält, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden. Dies gilt insbesondere, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 und 55, sowie vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 109 und 117; vgl. in diesem Sinne EGMR, 4. Dezember 2008, *S. und Marper/Vereinigtes Königreich*, CE:ECHR:2008:1204JUD003056204, § 103) ».

B.26.1. In Artikel 4 Nr. 9 des Gesetzes vom 25. Dezember 2016 ist PNR als « der Datensatz mit den zu jedem einzelnen Passagier notwendigen Reisedaten, der die in Artikel 9 erwähnten Informationen enthält, » definiert. Wie in B.4.1. erwähnt, werden in Artikel 9 des Gesetzes vom 25. Dezember 2016 einerseits die in Artikel 9 § 1 Nr. 18 erwähnten erweiterten Daten des Eincheckstatus und des Anbordgehens (API-Daten), die in Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 erschöpfend aufgelistet sind, und andererseits die Buchungsdaten (PNR-Daten) unterschieden, die höchstens die 19 Elemente umfassen, die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 erschöpfend aufgezählt sind, darunter die in Artikel 9 § 1 Nr. 18 erwähnten API-Daten.

Die Unterscheidung zwischen den API-Daten und den PNR-Daten ist in den in B.3 zitierten Vorarbeiten ausdrücklich angegeben.

B.26.2.1. In den Vorarbeiten zu Artikel 9 des Gesetzes vom 25. Dezember 2016 wurde ausgeführt:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 20-21).

Diese Unterscheidung entspricht der Unterscheidung zwischen den Daten, auf die sich die API-Richtlinie bezieht, und den Daten, auf die sich die PNR-Richtlinie bezieht.

B.26.2.2. Die Übermittlung von Passagierdaten, die im Gesetz vom 25. Dezember 2016 geregelt wird, schreibt es den Beförderungs- und Reiseunternehmen jedoch nicht vor, weitere Daten als diejenigen, über die sie bereits verfügen, zu erheben:

« 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 voyages 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 » (ebenda, SS. 15-16).

In den Erwägungsgründen 8 und 9 der PNR-Richtlinie ist diesbezüglich ebenfalls angegeben:

« (8) Die Fluggesellschaften erheben und verarbeiten bereits PNR-Daten ihrer Fluggäste für ihre eigenen geschäftlichen Zwecke. Durch diese Richtlinie sollten weder Fluggesellschaften dazu verpflichtet werden, weitere Fluggastdaten zu erheben oder vorzuhalten, noch sollte von den Fluggästen verlangt werden, dass sie neben den Daten, die die Fluggesellschaften bereits von ihnen erhalten, noch zusätzliche Daten bereitstellen.

(9) Einige Fluggesellschaften halten API-Daten, die sie erheben, als Teil der PNR-Daten vor, während andere dies nicht tun. Die Verwendung von PNR-Daten zusammen mit API-Daten bietet einen Mehrwert, indem sie den Mitgliedstaaten die Feststellung der Identität einer Person erleichtert, mithin den Nutzen dieses Ergebnisses für die Verhütung, Aufdeckung und Ermittlung von Straftaten erhöht und die Gefahr minimiert, dass Überprüfungen und Ermittlungen zu unschuldigen Personen durchgeführt werden. Es muss daher sichergestellt werden, dass Fluggesellschaften, die API-Daten erheben, diese übermitteln, unabhängig davon, ob sie API-Daten auf andere technische Weise als PNR-Daten vorhalten ».

B.27.1. In Bezug auf die API-Daten sieht Artikel 3 Absatz 2 der API-Richtlinie vor, dass zu den Angaben über die Personen, die sie zu einer zugelassenen Grenzübergangsstelle befördern werden, über die diese Personen in das Hoheitsgebiet eines Mitgliedstaats einreisen werden, die folgenden Angaben zählen:

« - die Nummer und die Art des mitgeführten Reisedokuments,

- die Staatsangehörigkeit,

- der vollständige Name,

- das Geburtsdatum,

- die Grenzübergangsstelle für die Einreise in das Hoheitsgebiet der Mitgliedstaaten,

- die Beförderungs-Codenummer,

- die Abreise- und Ankunftszeit,

- die Gesamtzahl der mit der betreffenden Beförderung beförderten Personen,

- der ursprüngliche Abreiseort ».

B.27.2.1. Vorher waren die Fluggesellschaften bereits verpflichtet, die API-Daten gemäß dem königlichen Erlass vom 11. Dezember 2006, aufgehoben durch Artikel 10 des königlichen Erlasses vom 18. Juli 2017, zu übermitteln.

In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wurde nämlich bestätigt:

« 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 » (ebenda, S. 11).

B.27.2.2. Vor seiner Aufhebung durch den königlichen Erlass vom 18. Juli 2017 waren in Artikel 3 § 2 des königlichen Erlasses vom 11. Dezember 2006 als Angaben, die von den Fluggesellschaften zu übermitteln sind, genannt:

« 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 ».

Diese Liste der Angaben übernahm also die in Artikel 3 Absatz 2 der API-Richtlinie vorgesehene Mindestliste.

B.28.1. In Bezug auf die PNR-Daten heißt es im Erwägungsgrund 15 der PNR-Richtlinie:

« Eine Liste mit den PNR-Daten, die für eine PNR-Zentralstelle bestimmt sind, sollte erstellt und inhaltlich so zusammengesetzt sein, dass sie sowohl den legitimen Bedürfnissen der Behörden im Zusammenhang mit der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gerecht werden und damit einen Beitrag zur inneren Sicherheit in der Union leisten als auch dem Grundrechtsschutz und insbesondere dem Schutz der Privatsphäre des Einzelnen und seiner personenbezogenen Daten Genüge tun. Zu diesem Zweck sollten hohe Standards zur Anwendung kommen, die mit der Charta der Grundrechte der Europäischen Union (im Folgenden ' Charta '), dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) im Einklang stehen. Eine solche Liste sollte nicht auf der Rasse oder ethnischen Herkunft, der Religion oder der Weltanschauung, der politischen oder sonstigen Meinungen, der Mitgliedschaft in einer Gewerkschaft, dem Gesundheitszustand, dem Sexualleben oder der sexuellen Orientierung einer Person beruhen. Die PNR-Daten sollten nur jene Details über den Buchungsvorgang und die Reiseroute von Fluggästen beinhalten, mit deren Hilfe die zuständigen Stellen diejenigen Fluggäste ermitteln können, die eine Bedrohung für die innere Sicherheit darstellen ».

B.28.2. Artikel 3 Nummer 5 der PNR-Richtlinie definiert den « Fluggastdatensatz » oder PNR als « einen Datensatz mit den für die Reise notwendigen Angaben zu jedem einzelnen Fluggast, die die Bearbeitung und Überprüfung der von einer Person oder in ihrem Namen getätigten Reservierungen für jede Reise durch die buchenden und beteiligten Fluggesellschaften ermöglichen, unabhängig davon, ob er in Buchungssystemen, Abfertigungssystemen (Departure Control Systems) zum Einchecken von Passagieren auf Flüge, oder gleichwertigen Systemen, die die gleichen Funktionen bieten, enthalten ist ».

Diese Definition des PNR-Datensatzes wurde in fast identischer Weise in Artikel 4 Nr. 9 des Gesetzes vom 25. Dezember 2016 übernommen.

B.28.3.1. Anhang I der PNR-Richtlinie mit der Überschrift « Von Fluggesellschaften erhobene PNR-Daten » bestimmt:

« 1. PNR-Buchungscode (Record Locator)

2. Datum der Buchung/Flugscheinausstellung

3. Planmäßiges Abflugdatum bzw. planmäßige Abflugdaten

4. Name(n)

5. Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse)

6. Alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift

7. Gesamter Reiseverlauf für bestimmte PNR-Daten

8. ' Vielflieger-Eintrag '

9. Reisebüro/Sachbearbeiter

10. Reisestatus des Fluggasts mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge (No show) und Fluggäste mit Flugschein, aber ohne Reservierung (Go show)

11. Angaben über gesplittete/geteilte PNR-Daten

12. Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft)

13. Flugscheindaten einschließlich Flugscheinnummer, Ausstellungsdatum, einfacher Flug (One-way), automatische Tarifanzeige (Automated Ticket Fare Quote fields)

14. Sitzplatznummer und sonstige Sitzplatzinformationen

15. Code-Sharing

16. Vollständige Gepäckangaben

17. Zahl und Namen von Mitreisenden im Rahmen der PNR-Daten

18. Etwaige erhobene erweiterte Fluggastdaten (API-Daten) (einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten, Staatsangehörigkeit, Familienname, Vorname, Geschlecht, Geburtsdatum, Fluggesellschaft, Flugnummer, Tag des Abflugs, Tag der Ankunft, Flughafen des Abflugs, Flughafen der Ankunft, Uhrzeit des Abflugs und Uhrzeit der Ankunft)

19. Alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten PNR-Daten ».

B.28.3.2. Durch Rubrik 18 von Anhang I der PNR-Richtlinie wird also der Begriff der API-Daten, auf den sich Artikel 3 Absatz 2 der API-Richtlinie bezog, erweitert.

B.29.1.1. In Bezug auf die Buchungsdaten bezeichnet Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 als PNR-Daten höchstens:

« In Bezug auf die Buchungsdaten enthalten die Passagierdaten höchstens:

1. PNR-Buchungscode (Record Locator),

2. Datum der Buchung und der Fahr- beziehungsweise Flugscheinausstellung,

3. planmäßige Reisedaten,

4. Namen, Vornamen und Geburtsdatum,

5. Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse),

6. Zahlungsinformationen einschließlich Rechnungsanschrift,

7. den gesamten Reiseverlauf für den betreffenden Passagier,

8. Informationen zu den ' registrierten Reisenden ', d. h. zu den ' Vielreisenden ',

9. Reisebüro oder Sachbearbeiter,

10. Reisestatus des Reisenden mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Reisen (No show) oder Passagier mit Fahr- beziehungsweise Flugschein, aber ohne Reservierung (Go show),

11. Angaben über gesplittete oder geteilte PNR-Daten,

12. allgemeine Hinweise, einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktangaben der Begleitperson bei der Abreise und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktangaben der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Mitarbeiter bei der Abreise und der Ankunft,

13. Fahr- beziehungsweise Flugscheindaten einschließlich Fahr- beziehungsweise Flugscheinnummer, Ausstellungsdatum, einfache Fahrten beziehungsweise Flüge, informatisierte tarifbezogene Felder der Fahr- beziehungsweise Flugscheine,

14. Sitzplatznummer und sonstige Sitzplatzinformationen,

15. Code-Sharing,

16. vollständige Gepäckangaben,

17. Zahl und Namen von Mitreisenden im Rahmen der PNR-Daten,

18. etwaige erhobene erweiterte Passagierdaten (API-Daten), die in § 2 aufgezählt sind,

19. alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten Daten ».

B.29.1.2. Die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 erwähnten PNR-Daten übernehmen somit die in Anhang I der PNR-Richtlinie erwähnten Daten.

B.29.2.1. In Bezug auf die erweiterten Daten des Eincheckstatus und des Anbordgehens bezeichnet Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 als API-Daten:

« In Bezug auf die Daten des Eincheckstatus und des Anbordgehens umfassen die in § 1 Nr. 18 erwähnten erweiterten Daten Folgendes:

1. Art des Reisedokuments,

2. Nummer des Reisedokuments,

3. Staatsangehörigkeit,

4. Land, das das Dokument ausgestellt hat,

5. Ablaufdatum des Dokuments,

6. Familienname, Vorname, Geschlecht, Geburtsdatum,

7. Beförderungsunternehmen/Reiseunternehmen,

8. Beförderungsnummer,

9. Abreisedatum, Ankunftsdatum,

10. Abreiseort, Ankunftsort,

11. Abreisezeit, Ankunftszeit,

12. Gesamtzahl der mit der betreffenden Beförderung beförderten Personen,

13. Sitzplatznummer,

14. PNR-Buchungscode (Record Locator)

15. Anzahl, Gewicht und Identifizierung der Gepäckstücke,

16. Grenzübergangsstelle für die Einreise in das nationale Hoheitsgebiet ».

B.29.2.2. Mit den in Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten werden im Wesentlichen die in Rubrik 18 von Anhang I der PNR-Richtlinie erwähnten Daten übernommen und diese sind somit umfassender als die Daten, die unter Artikel 3 Absatz 2 der API-Richtlinie fielen.

B.30.1. In seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 hat der Gerichtshof der Europäischen Union in Beantwortung der vom Verfassungsgerichtshof zur Gültigkeit der PNR-Richtlinie gestellten Vorabentscheidungsfragen in Bezug auf die von der PNR-Richtlinie erfassten Fluggastdaten [...] zunächst auf den 15. Erwägungsgrund der PNR-Richtlinie und den Umstand hingewiesen, dass Artikel 13 Absatz 4 Satz 1 der PNR-Richtlinie « die Verarbeitung von PNR-Daten, die die rassische oder ethnische Herkunft einer Person, ihre politischen Meinungen, ihre religiösen oder weltanschaulichen Überzeugungen, ihre Mitgliedschaft in einer Gewerkschaft, ihren Gesundheitszustand oder ihr Sexualleben oder ihre sexuelle Orientierung erkennen lassen » verbietet, um zu der Auffassung zu gelangen, dass « die im Einklang mit Anhang I der PNR-Richtlinie erhobenen und übermittelten PNR-Daten in unmittelbarem Zusammenhang mit dem durchgeführten Flug und dem betreffenden Fluggast stehen [müssen] und in der Weise begrenzt sein [müssen], dass sie zum einen nur den legitimen Bedürfnissen der Behörden im Zusammenhang mit der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gerecht werden und zum anderen sensible Daten ausnehmen » (Randnr. 128).

Der Gerichtshof der Europäischen Union urteilt, dass die Rubriken 1 bis 4, 7, 9, 11, 15, 17 und 19 des Anhangs I der PNR-Richtlinie diesen Anforderungen sowie den Anforderungen an Klarheit und Genauigkeit genügen, da es sich bei ihnen um klar identifizierbare und umschriebene Informationen in unmittelbarem Zusammenhang mit dem durchgeführten Flug und dem betreffenden Fluggast handelt. Wie der Generalanwalt in Nr. 165 seiner Schlussanträge ausgeführt hat, und dass dies trotz ihres offenen Wortlauts auch für die Rubriken 10, 13, 14 und 16 gilt (Randnr. 129).

B.30.2. Für die Auslegung der Rubriken 5, 6, 8, 12 und 18 hält der Gerichtshof der Europäischen Union hingegen die folgenden Klarstellungen für notwendig:

« 131. In Rubrik 5 - ‘ Anschrift und Kontaktdaten (Telefonnummer, E-Mail-Adresse) ’ - wird nicht ausdrücklich klargestellt, ob sich die Anschrift und die Kontaktdaten nur auf den Fluggast beziehen oder auch auf Dritte, die den Flug für den Fluggast gebucht haben, auf Dritte, über die ein Fluggast erreicht werden kann, oder auf Dritte, die in Notfällen zu verständigen sind. Wie der Generalanwalt in Nr. 162 seiner Schlussanträge im Wesentlichen ausgeführt hat, kann diese Rubrik in Anbetracht der Erfordernisse der Klarheit und Genauigkeit jedoch nicht dahin ausgelegt werden, dass sie implizit auch die Erhebung und Übermittlung von personenbezogenen Daten solcher Dritter erlaubt. Sie ist folglich dahin auszulegen, dass sie sich nur auf die Postanschrift und die Kontaktdaten, d. h. Telefonnummer und E-Mail-Adresse, des Fluggasts bezieht, in dessen Namen die Buchung getätigt wird.

132. Rubrik 6 - ‘ Alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift ’ - ist, um den Anforderungen an Klarheit und Genauigkeit zu genügen, dahin auszulegen, dass sie lediglich Informationen über die Modalitäten der Zahlung und die Abrechnung des Flugscheins betrifft, nicht aber andere Informationen, die keinen direkten Bezug zum Flug aufweisen (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 159).

133. Rubrik 8 - ‘ Vielflieger-Eintrag ’ - ist, wie der Generalanwalt in Nr. 164 seiner Schlussanträge ausgeführt hat, dahin auszulegen, dass sie sich ausschließlich auf Angaben zum Status des betreffenden Fluggasts im Kontext des Vielfliegerprogramms einer bestimmten Fluggesellschaft oder einer bestimmten Gruppe von Fluggesellschaften sowie auf die Nummer bezieht, die dieser Fluggast als ‘ Vielflieger ’ trägt. Rubrik 8 ermöglicht es daher nicht, Informationen zu den Transaktionen zu erheben, mit denen dieser Status erworben wurde.

134. Rubrik 12 betrifft ‘ Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft) ’.

135. Insoweit ist zunächst festzustellen, dass zwar die Worte ‘ Allgemeine Hinweise ’ nicht den Anforderungen an Klarheit und Genauigkeit genügen, da sie als solche Art und Umfang der gemäß Rubrik 12 zu erhebenden und einer PNR-Zentralstelle zu übermittelnden Informationen nicht begrenzen (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 160); dagegen genügt die Aufzählung in Klammern diesen Anforderungen.

136. Infolgedessen ist, um Rubrik 12, in Anwendung der oben in Rn. 86 angeführten Rechtsprechung, eine Auslegung zu geben, die mit den Anforderungen an Klarheit und Genauigkeit und, allgemeiner, mit den Art. 7 und 8 sowie mit Art. 52 Abs. 1 der Charta im Einklang steht, davon auszugehen, dass sich die Erhebung und die Übermittlung nur auf die in dieser Rubrik ausdrücklich aufgezählten Angaben erstrecken dürfen, nämlich Name und Geschlecht des minderjährigen Fluggasts, sein Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft.

137. Schließlich betrifft Rubrik 18 ‘ Etwaige erhobene erweiterte Fluggastdaten (API-Daten) (einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten, Staatsangehörigkeit, Familienname, Vorname, Geschlecht, Geburtsdatum, Fluggesellschaft, Flugnummer, Tag des Abflugs, Tag der Ankunft, Flughafen des Abflugs, Flughafen der Ankunft, Uhrzeit des Abflugs und Uhrzeit der Ankunft) ’.

138. Wie der Generalanwalt in den Nrn. 156 bis 160 seiner Schlussanträge im Wesentlichen ausgeführt hat, ergibt sich aus Rubrik 18 im Licht der Erwägungsgründe 4 und 9 der PNR-Richtlinie, dass die Angaben, auf die sie sich bezieht, allein die in dieser Rubrik und in Art. 3 Abs. 2 der API-Richtlinie genannten API-Daten sind.

139. Somit kann, sofern Rubrik 18 dahin ausgelegt wird, dass sie nur die in dieser Rubrik und in Art. 3 Abs. 2 der API-Richtlinie ausdrücklich genannten Angaben erfasst, davon ausgegangen werden, dass sie den Anforderungen an Klarheit und Genauigkeit genügt (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 161).

140. Daher ist festzustellen, dass Anhang I der PNR-Richtlinie unter der Voraussetzung, dass er im Einklang mit den insbesondere oben in den Rn. 130 bis 139 dargelegten Erwägungen ausgelegt wird, insgesamt hinreichend klar und präzise ist und damit die Tragweite des Eingriffs in die Grundrechte abgrenzt, die in den Art. 7 und 8 der Charta verankert sind ».

B.31.1. Wie in B.3 erwähnt, hat das Gesetz vom 25. Dezember 2016 die Zielsetzung, die öffentliche Sicherheit zu gewährleisten, indem eine Übermittlung von Passagierdaten und deren Verwendung im Rahmen der Bekämpfung terroristischer Straftaten und grenzübergreifender schwerer Kriminalität eingeführt wird.

Diese Ziele stellen eine dem Gemeinwohl dienende Zielsetzung dar, die Eingriffe in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten rechtfertigen können (EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238, Randnr. 42). Der Gerichtshof hat außerdem bestätigt, dass diese dem Gemeinwohl dienende Zielsetzung die Übermittlung und Verarbeitung von Fluggastdatensätzen rechtfertigen kann (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, ECLI:EU:C:2017:592, Randnrn. 148 und 149; EuGH, Große Kammer, 21. Juni 2022, C-817/19, *Ligue des droits humains gegen Ministerrat*, ECLI:EU:C:2022:491, Randnr. 122)).

B.31.2. Die Erhebung der unter das Gesetz vom 25. Dezember 2016 fallenden Passagierdaten ist in Bezug auf den Inhalt dieser Daten mit Garantien versehen.

B.31.3. Wie in B.4.1 erwähnt, sind diese Daten zunächst in erschöpfender Weise in Artikel 9 des Gesetzes vom 25. Dezember 2016 bestimmt.

Diese Daten sind Informationen, die direkt mit der Reise zusammenhängen, die zu der in den Anwendungsbereich des Gesetzes vom 25. Dezember 2016 fallenden Beförderung Anlass gibt. Wie in B.26.2.2 erwähnt, handelt es sich um Daten, über die die Beförderungs- und Reiseunternehmen grundsätzlich bereits verfügen. Außerdem entsprechen diese Daten dem Anhang I der Leitlinien der International Civil Aviation Organization (ICAO) (EuGH, Große Kammer, 26. Juli 2017, Gutachten 1/15, ECLI:EU:C:2017:592, Randnr. 156). Diese Daten sind somit sachdienlich in Bezug auf die Zielsetzung des Gesetzes vom 25. Dezember 2016.

B.31.4.1. Im Übrigen bestimmen die nicht angefochtenen Artikel 10 und 11 des Gesetzes vom 25. Dezember 2016:

« Art. 10. Die Passagierdaten dürfen nicht die rassische oder ethnische Herkunft einer Person, ihre religiösen oder weltanschaulichen Überzeugungen, ihre politischen Meinungen, ihre Mitgliedschaft in einer Gewerkschaftsorganisation, ihren Gesundheitszustand, ihr Sexualleben oder ihre sexuelle Orientierung betreffen.

Art. 11. Wenn die von den Beförderungsunternehmen und Reiseunternehmen übermittelten Passagierdaten andere als die in Artikel 9 aufgeführten Daten beinhalten oder wenn sie Daten, wie in Artikel 10 aufgeführt, beinhalten, werden diese zusätzlichen Daten von der PNR-Zentralstelle unmittelbar nach ihrem Eingang dauerhaft gelöscht ».

B.31.4.2. In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wird diesbezüglich bestätigt:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 21).

B.31.5. Diese Bestimmungen gewährleisten daher, dass sensible Daten im Rahmen der Passagierdaten, die unter das Gesetz vom 25. Dezember 2016 fallen, nicht erhoben oder gespeichert werden dürfen (Artikel 10). Die Daten, die über die in Artikel 9 abschließend aufgeführten Daten hinausgehen, oder die Daten, die sensible Daten beinhalten, werden von der PNR-Zentralstelle gelöscht (Artikel 11).

Diese Garantie in Bezug auf sensible Daten kommt daher zu derjenigen hinzu, die der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 bezüglich des 15. Erwägungsgrundes und Artikel 13 Absatz 4 Satz 1 der PNR-Richtlinie betont hat (Randnr. 128), wie er es bereits in seinem vorerwähnten Gutachten 1/15 vom 26. Juli 2017 hervorgehoben hat (Randnr. 167).

Der Umstand, dass solche Daten, wenn sie zusammengeführt werden, sensible Informationen offenlegen könnten, führt nicht zu einer anderen Schlussfolgerung, da ein solcher Vorgang eine Weiterverarbeitung der in Artikel 9 des Gesetzes vom 25. Dezember 2016 aufgezählten Daten voraussetzen würde, die nicht den vom Gesetz vom 25. Dezember 2016 verfolgten Zielen und Zwecken entsprechen würde.

B.32.1. Wie in B.29 erwähnt, entsprechen die in Artikel 9 § 1 des Gesetzes vom 25. Dezember 2016 erwähnten PNR-Daten den Daten, die in Anhang I der PNR-Richtlinie aufgeführt sind, und mit den in Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten werden im Wesentlichen die in der Rubrik 18 von Anhang I der PNR-Richtlinie erwähnten Daten übernommen.

B.32.2. Es ist nun unter Berücksichtigung des vorerwähnten Urteils des Gerichtshofes der Europäischen Union in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022, auf das in B.30 hingewiesen wurde, zu prüfen, ob diese Eingriffe ausreichend präzise, verhältnismäßig und auf das « absolut Notwendige » beschränkt sind, um die vom Gesetz vom 25. Dezember 2016 verfolgten Ziele zu erreichen.

B.33.1. Aus dem vorerwähnten Urteil des Gerichtshofs der Europäischen Union geht hervor, dass die PNR-Daten « in unmittelbarem Zusammenhang mit dem durchgeführten Flug und dem betreffenden Fluggast stehen [müssen] und in der Weise begrenzt sein [müssen], dass sie zum einen nur den legitimen Bedürfnissen der Behörden im Zusammenhang mit der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gerecht werden und zum anderen sensible Daten ausnehmen » (Randnr. 128). Diese Erwägungen sind auf andere Beförderungsmittel übertragbar, auf die sich das PNR-System bezieht.

Analog zu dem, was der Gerichtshof der Europäischen Union bezüglich der PNR-Richtlinie geurteilt hat (Randnr. 129), stellt der Verfassungsgerichtshof fest, dass die in Artikel 9 § 1 Nr. 1 bis 4, 7, 9, 11, 15, 17 und 19 des Gesetzes vom 25. Dezember 2016 erwähnten Daten die Rubriken 1 bis 4, 7, 9, 11, 15, 17 und 19 des Anhangs I der PNR-Richtlinie diesen Anforderungen sowie den Anforderungen an Klarheit und Genauigkeit genügen, da es sich bei ihnen um klar identifizierbare und umschriebene Informationen in unmittelbarem Zusammenhang mit dem durchgeführten Flug und dem betreffenden Fluggast handelt, und das Gleiche gilt trotz ihres weit gefassten Wortlauts für die in Artikel 9 § 1 Nr. 10, 13, 14 und 16 desselben Gesetzes erwähnten Daten.

B.33.2. Was Artikel 9 § 1 Nr. 5 des Gesetzes vom 25. Dezember 2016 betrifft, der sich auf die « Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse) » bezieht, sind diese Begriffe analog zu dem, was der Gerichtshof der Europäischen Union bezüglich der Rubrik 5 der PNR-Richtlinie geurteilt hat (Randnr. 131), dahin auszulegen, dass sie sich nur auf die Postanschrift und die Kontaktdaten, d. h. Telefonnummer und E-Mail-Adresse, des Passagiers beziehen, in dessen Namen die Buchung getätigt wird. Sodass diese Begriffe nicht dahin ausgelegt werden können, dass sie implizit auch die Erhebung und Übermittlung von personenbezogenen Daten Dritter erlauben.

B.33.3. Was Artikel 9 § 1 Nr. 6 des Gesetzes vom 25. Dezember 2016 betrifft, der sich auf die « Zahlungsinformationen einschließlich Rechnungsanschrift » bezieht, sind, um den Anforderungen an Klarheit und Genauigkeit zu genügen, diese Begriffe analog zu dem, was der Gerichtshof der Europäischen Union bezüglich der Rubrik 6 der PNR-Richtlinie geurteilt hat (Randnr. 132), dahin auszulegen, dass sie lediglich Informationen über die Modalitäten der Zahlung und die Abrechnung des Flugscheins oder des Fahrscheins betreffen, nicht aber andere Informationen, die keinen direkten Bezug zum Flug oder zur Fahrstrecke aufweisen.

B.33.4. Was Artikel 9 § 1 Nr. 8 des Gesetzes vom 25. Dezember 2016 betrifft, der sich auf die « Informationen zu den ‘ registrierten Reisenden ’, d. h. zu den Vielreisenden » bezieht, sind diese Begriffe analog zu dem, was der Gerichtshof der Europäischen Union bezüglich der Rubrik 8 der PNR-Richtlinie geurteilt hat (Randnr. 133), dahin auszulegen, dass sie sich ausschließlich auf Angaben zum Status des betreffenden Fluggasts im Kontext eines Vielfliegerprogramms einer bestimmten Fluggesellschaft oder einer bestimmten Gruppe von Fluggesellschaften oder in einem anderen Kundenbindungsprogramm für Vielreisende sowie auf die Nummer beziehen, die dieser Passagier als « Vielreisender » oder Begünstigter eines anderen Kundenbindungsprogramms trägt. In dieser Weise ausgelegt, ermöglichen es diese Begriffe daher nicht, Informationen zu den Transaktionen zu erheben, mit denen dieser Status erworben wurde.

B.33.5. Was Artikel 9 § 1 Nr. 12 des Gesetzes vom 25. Dezember 2016 betrifft, der sich auf « allgemeine Hinweise, einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktangaben der Begleitperson bei der Abreise und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktangaben der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Mitarbeiter bei der Abreise und der Ankunft » bezieht, sind diese Begriffe analog zu dem, was der Gerichtshof der Europäischen Union bezüglich der Rubrik 12 der PNR-Richtlinie geurteilt hat (Randnrn. 134 bis 136), dahin auszulegen, dass nur die Erhebung und Übermittlung der ausdrücklich in dieser Bestimmung aufgezählten Angaben zulässig sind, nämlich Name und Geschlecht des minderjährigen Fluggasts oder Reisenden, sein Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft.

Dahin ausgelegt, dass er eine abschließende Datenliste festlegt, genügt Artikel 9 § 1 Nr. 12 des Gesetzes vom 25. Dezember 2016 den Anforderungen an Klarheit und Genauigkeit.

B.33.6.1. Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 bezieht sich auf « etwaige erhobene erweiterte Passagierdaten (API-Daten), die in § 2 aufgezählt sind », nämlich: Art des Reisedokuments (Nr. 1), Nummer des Reisedokuments (Nr. 2), Staatsangehörigkeit (Nr. 3), Land, das das Dokument ausgestellt hat (Nr. 4), Ablaufdatum des Dokuments (Nr. 5), Familienname, Vorname, Geschlecht, Geburtsdatum (Nr. 6), Beförderungsunternehmen/Reiseunternehmen (Nr. 7), Beförderungsnummer (Nr. 8), Abreisedatum, Ankunftsdatum (Nr. 9), Abreiseort, Ankunftsort (Nr. 10), Abreisezeit, Ankunftszeit (Nr. 11), Gesamtzahl der mit der betreffenden Beförderung beförderten Personen (Nr. 12), Sitzplatznummer (Nr. 13), PNR-Buchungscode (Record Locator) (Nr. 14), Anzahl, Gewicht und Identifizierung der Gepäckstücke (Nr. 15), Grenzübergangsstelle für die Einreise in das nationale Hoheitsgebiet (Nr. 16).

Bezüglich der Rubrik 18 hat der Gerichtshof der Europäischen Union geurteilt, dass bei dieser Rubrik, sofern sie dahin ausgelegt wird, dass sie nur die in dieser Rubrik und in Artikel 3 Absatz 2 der API-Richtlinie ausdrücklich genannten Angaben erfasst, davon ausgegangen werden kann, dass sie den Anforderungen an Klarheit und Genauigkeit genügt (Randnrn. 137 bis 139).

B.33.6.2. Der Verfassungsgerichtshof stellt diesbezüglich fest, dass sich Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 anders als die Rubrik 18 der PNR-Richtlinie auf eine in Artikel 9 § 2 desselben Gesetzes abschließend aufgezählte Datenliste bezieht, sodass diese Bestimmungen den Anforderungen an Klarheit und Genauigkeit genügen.

B.33.6.3. Was den Umfang der « API-Daten » betrifft, die in Artikel 9 § 2 des Gesetzes vom 25. Dezember 2016 erwähnt sind, werden – wie in B.29 erwähnt – mit diesen Daten im Wesentlichen die in Rubrik 18 des Anhangs I der PNR-Richtlinie erwähnten Daten übernommen.

So entsprechen die in Artikel 9 § 2 Nr. 1 bis 11 des Gesetzes vom 25. Dezember 2016 erwähnten Daten exakt den Daten, die in der vorerwähnten Rubrik 18 ausdrücklich aufgezählt sind.

Außerdem entsprechen die in Artikel 9 § 2 Nr. 12, 14 und 16 des Gesetzes vom 25. Dezember 2016 erwähnten Daten exakt den Daten, die in Artikel 3 Absatz 2 der API-Richtlinie ausdrücklich aufgezählt sind.

B.33.6.4. Daraus folgt, dass nur die in Artikel 9 § 2 Nr. 13 und 15 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten, nämlich Sitzplatznummer (Nr. 13) und Anzahl, Gewicht und Identifizierung der Gepäckstücke (Nr. 15), nicht ausdrücklich den in der Rubrik 18 des Anhangs I der PNR-Richtlinie sowie in Artikel 3 Absatz 2 der API-Richtlinie erwähnten Angaben entsprechen.

Die vorstehende Feststellung kann jedoch weder zu der Auffassung führen, dass es diesen Daten an Klarheit und Genauigkeit fehlen würden, noch dass sie die Grenze des « absolut Notwendigen » überschreiten würden., um die vom Gesetz vom 25. Dezember 2016 verfolgten Ziele zu erreichen.

Wie in B.3.2 angegeben, sind die API-Daten nämlich die Daten, die im Rahmen des Check-in und des Anbordgehens übermittelt werden und weniger schnell verfügbar sind als die PNR-Daten. Solche Daten sind, wie der Generalanwalt Pitruzzella in seinen Schlussanträgen vom 27. Januar 2022 in der Rechtssache C-817/19 hervorgehoben hat, « von den Fluggesellschaften im Rahmen ihrer normalen Geschäftstätigkeit erhoben worden » (ECLI:EU:C:2022:65, Randnr. 160), und gegebenenfalls sind sie von anderen Beförderungsunternehmen erhoben worden. Nur wenn die Daten von den Beförderungsunternehmen im Rahmen ihrer normalen Geschäftstätigkeit erhoben worden sind, fallen sie unter die in Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten, da das vorerwähnte Gesetz, wie in B.26.2.2 erwähnt, keine zusätzliche Pflicht zur Datenerhebung einführt.

Die in Artikel 9 § 1 Nr. 14 und 16 erwähnten PNR-Daten betreffen bereits - wie die Rubriken 14 und 16 der PNR-Richtlinie - jeweils « Sitzplatznummer » und « sonstige Sitzplatzinformationen und vollständige Gepäckangaben » und bei solchen Daten wird, wie in B.33.1 erwähnt, davon ausgegangen, dass sie den Anforderungen an Klarheit und Genauigkeit genügen und einen direkten Bezug zum Flug oder zur Fahrstrecke und mit den im vorliegenden Fall verfolgten Zielen aufweisen. Artikel 9 § 1 Nr. 19 betrifft bei den PNR-Daten ebenfalls « alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten Daten », einschließlich etwaiger Änderungen bezüglich des Sitzes oder Gepäcks. Die in Artikel 9 § 2 Nr. 13 und 15 erwähnten Informationen zum Sitz oder Gepäck sind somit bereits in den in Artikel 9 § 1 Nr. 14 und 16 erwähnten Daten enthalten.

Indem er sich bei den API-Daten, das heißt den beim Check-in und Anbordgehen erhobenen Daten, ausdrücklich auf die Informationen zum Sitz und Gepäck bezieht, schafft Artikel 9 § 2 Nr. 13 und 15 des Gesetzes vom 25. Dezember 2016 daher keine weiteren Daten gegenüber der Liste der nach Artikel 9 § 1 Nr. 14 und 16 zu erhebenden Daten und genügt daher den Anforderungen an Klarheit und Genauigkeit und Verhältnismäßigkeit.

B.34. Vorbehaltlich der in B.33.2 bis B.33.5 erwähnten Auslegungen ist der Klagegrund insofern, als er gegen die Artikel 4 Nr. 9 und 9 des Gesetzes vom 25. Dezember 2016 gerichtet ist, unbegründet.

2. *Der Begriff des « Passagiers » (Artikel* 4 *Nr.* 10*)*

B.35. Die klagende Partei bemängelt den weit gefassten Begriff « Passagier », der zu einer nicht gezielten systematischen und automatisierten Verarbeitung von Daten aller Passagiere führe.

B.36.1. Artikel 4 Nr. 10 des angefochtenen Gesetzes definiert den « Passagier » als « jede Person, einschließlich der Personen im Transfer- oder Transitverkehr, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung des Beförderungsunternehmens von ihm befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung dieser Person in die Passagierliste belegt wird ».

In diesem Artikel wird der Inhalt von Artikel 3 Nummer 4 der PNR-Richtlinie übernommen, der den « Fluggast » ebenfalls als « jede Person, einschließlich Transfer- oder Transitfluggästen, mit Ausnahme der Besatzungsmitglieder, die mit Zustimmung der Fluggesellschaft in einem Luftfahrzeug befördert wird oder befördert werden soll, wobei diese Zustimmung durch die Eintragung der Person in die Fluggastliste belegt wird » definiert.

B.36.2. Die Definition des « Passagiers » hat zur Folge, dass die Erhebung, Übermittlung und Verarbeitung der PNR-Daten dieser « Passagiere » allgemeine und unterschiedslose Verpflichtungen darstellen, die für alle Personen gelten, die befördert werden oder befördert werden sollen und auf der Passagierliste eingetragen sind.

Die Verpflichtungen, die das Gesetz vom 25. Dezember 2016 vorschreibt, gelten somit unabhängig davon, ob schwerwiegende Gründe zu der Annahme vorliegen, dass die betroffenen Personen eine Straftat begangen haben oder eine Straftat begehen werden, oder wegen einer Straftat verurteilt wurden.

Das Gesetz vom 25. Dezember 2016 führt die allgemeine und unterschiedslose Erhebung, Übermittlung und Verwendung von PNR Daten für sämtliche Passagiere ein, die per Luftverkehr reisen, unabhängig davon, ob sie eine Außengrenze der Union überschreiten, und diese Datenerhebung wurde durch die in B.8 zitierten königlichen Erlasse vom 3. Februar 2019 auf den Schienen- und Busverkehr ausgedehnt.

B.36.3. In seiner Stellungnahme vom 19. August 2016 « über die datenschutzrechtlichen Auswirkungen der Verarbeitung von Passagierdaten » hat der Beratende Ausschuss für das Übereinkommen des Europarates Nr. 108 « zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten » diesbezüglich angemerkt:

« 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 » (Stellungnahme vom 19. August 2016, T-PD(2016)18rev, S. 5).

Der Ausschuss hat auch die Notwendigkeit einer regelmäßigen Bewertung eines solchen PNR-Systems betont, um festzustellen, ob es noch gerechtfertigt ist:

« 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 » (ebenda, S. 6).

B.36.4.1. Artikel 19 der PNR-Richtlinie mit der Überschrift « Überprüfung » sieht vor, dass die Kommission anhand von Informationen der Mitgliedstaaten, einschließlich der statistischen Daten, bis zum 25. Mai 2020 eine Überprüfung aller Elemente dieser Richtlinie vornimmt und dem Europäischen Parlament und dem Rat einen Bericht vorlegt und diesen erläutert.

Artikel 19 Absatz 3 der PNR-Richtlinie sieht vor, dass « die Kommission [...] dabei die Erfahrungen der Mitgliedstaaten, insbesondere jener Mitgliedstaaten, die gemäß Absatz 2 diese Richtlinie auf EU-Flüge anwenden, » berücksichtigt und « auch [prüft], ob es erforderlich ist, Wirtschaftsteilnehmer, die keine Beförderungsunternehmen sind, wie etwa Reisebüros oder Reiseveranstalter, die Dienstleistungen im Zusammenhang mit Reisen – einschließlich Flugbuchungen – erbringen, in den Anwendungsbereich dieser Richtlinie aufzunehmen ».

Gemäß dieser Bestimmung hat die Kommission dem Europäischen Parlament und dem Rat am 24. Juli 2020 ihren Bericht « über die Überprüfung der Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität » (COM(2020) 305 final) zugeleitet.

Dieser Bericht kommt zu dem Schluss:

« Die von der Kommission durchgeführte Überprüfung der Anwendung der Richtlinie in den ersten zwei Jahren fällt insgesamt positiv aus. Die wichtigste Schlussfolgerung der Überprüfung ist, dass die Richtlinie einen positiven Beitrag zu ihrem Hauptziel leistet, das darin besteht, die Einrichtung wirksamer PNR-Systeme in den Mitgliedstaaten als Instrument zur Bekämpfung von Terrorismus und schwerer Kriminalität zu gewährleisten » (S. 13).

Bezüglich des Anwendungsbereichs der Erhebung von PNR-Daten hat die Kommission betont:

« Alle Mitgliedstaaten außer einem haben die Erhebung von PNR-Daten auf Flüge innerhalb der EU ausgeweitet. Die nationalen Behörden sehen in der Erhebung von PNR-Daten zu Flügen innerhalb der EU (und insbesondere innerhalb des Schengen-Raums) ein wichtiges Instrument der Strafverfolgung, das dazu eingesetzt werden kann, die Bewegungen bekannter verdächtiger Personen zu verfolgen und verdächtige Reisemuster unbekannter Personen zu ermitteln, die an kriminellen oder terroristischen Aktivitäten innerhalb des Schengen-Raums beteiligt sein könnten. Da die Mitgliedstaaten bereits effektiv PNR-Daten zu EU-Flügen erheben, hält es die Kommission zum gegenwärtigen Zeitpunkt nicht für wesentlich, die Erhebung von PNR-Daten zu EU-Flügen verbindlich vorzuschreiben » (S. 11).

B.36.4.2. Artikel 52 § 1 des Gesetzes vom 25. Dezember 2016 sieht vor, dass « vorliegendes Gesetz [...] drei Jahre nach seinem Inkrafttreten einer Bewertung unterzogen » wird.

B.37. Auf die Frage des Verfassungsgerichtshofes in Bezug auf ein System der allgemeinen und unterschiedslosen Erhebung, Übermittlung und Verwendung von PNR-Daten für sämtliche « Fluggäste », unabhängig davon, ob sie eine Außengrenze der Union überschreiten, hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 geantwortet:

« 158. Das durch die PNR-Richtlinie geschaffene System erstreckt sich auf die PNR-Daten sämtlicher Personen, die unter den Begriff ‘ Fluggast ’ im Sinne von Art. 3 Nr. 4 der Richtlinie fallen und auf Flügen befördert werden, die in den Anwendungsbereich der Richtlinie fallen.

159. Nach Art. 8 Abs. 1 der PNR-Richtlinie werden diese Daten an die PNR-Zentralstelle des Mitgliedstaats übermittelt, in dessen Hoheitsgebiet der betreffende Flug ankommt oder von dem er abgeht, unabhängig davon, ob es irgendwelche objektiven Anhaltspunkte dafür gibt, dass die betreffenden Fluggäste in terroristische Straftaten oder schwere Kriminalität verwickelt sein könnten. Die übermittelten Daten werden u. a. automatisierten Verarbeitungen im Rahmen der Vorabüberprüfung gemäß Art. 6 Abs. 2 Buchst. a und Abs. 3 der PNR-Richtlinie unterzogen; anhand dieser Überprüfung sollen, wie sich aus dem siebten Erwägungsgrund der Richtlinie ergibt, Personen ermittelt werden, die zuvor nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die von den zuständigen Behörden genauer überprüft werden sollten.

160. Insbesondere ergibt sich aus Art. 1 Abs. 1 Buchst. a und Art. 2 der PNR-Richtlinie, dass diese zwischen Fluggästen von Drittstaatsflügen zwischen der Union und Drittstaaten und Fluggästen von EU-Flügen zwischen verschiedenen Mitgliedstaaten unterscheidet.

161. Was die Fluggäste von Drittstaatsflügen betrifft, hat der Gerichtshof in Bezug auf Fluggäste von Flügen zwischen der Union und Kanada bereits entschieden, dass die automatisierte Verarbeitung ihrer PNR-Daten vor ihrer Ankunft in Kanada die Sicherheitskontrollen, insbesondere an den Grenzen, erleichtert und beschleunigt. Der Ausschluss bestimmter Kategorien von Personen oder bestimmter Herkunftsländer könnte dem Ziel der automatisierten Verarbeitung der PNR-Daten zuwiderlaufen, das darin besteht, unter sämtlichen Fluggästen mittels einer Überprüfung dieser Daten die Personen zu ermitteln, von denen eine Gefahr für die öffentliche Sicherheit ausgehen kann. Außerdem könnte diese Überprüfung umgangen werden (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 187).

162. Diese Erwägungen lassen sich *mutatis mutandis* auf die Situation der Fluggäste von Flügen zwischen der Union und sämtlichen Drittstaaten übertragen, die die Mitgliedstaaten gemäß Art. 1 Abs. 1 Buchst. a in Verbindung mit Art. 3 Nrn. 2 und 4 der PNR-Richtlinie dem durch diese geschaffenen System unterwerfen müssen. Die Übermittlung und Vorabüberprüfung der PNR-Daten von Fluggästen, die in die Union ein- oder aus der Union ausreisen, können nämlich angesichts der Art der Bedrohungen für die öffentliche Sicherheit, die sich aus terroristischen Straftaten und schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen zwischen der Union und Drittstaaten ergeben können, nicht auf einen bestimmten Kreis von Fluggästen beschränkt werden. Somit ist davon auszugehen, dass es den erforderlichen Zusammenhang zwischen diesen Daten und dem Ziel der Bekämpfung solcher strafbarer Handlungen gibt, so dass die PNR-Richtlinie nicht allein deshalb über das absolut Notwendige hinausgeht, weil sie den Mitgliedstaaten vorschreibt, die PNR-Daten aller dieser Fluggäste systematisch zu übermitteln und vorab zu überprüfen.

163. Für die Fluggäste von Flügen zwischen verschiedenen Mitgliedstaaten der Union sieht Art. 2 Abs. 1 der PNR-Richtlinie in Verbindung mit ihrem zehnten Erwägungsgrund lediglich vor, dass die Mitgliedstaaten die Anwendung des durch diese Richtlinie geschaffenen Systems auf EU-Flüge ausdehnen können.

164. Somit hatte der Unionsgesetzgeber nicht die Absicht, den Mitgliedstaaten die Verpflichtung aufzuerlegen, die Anwendung des durch die PNR-Richtlinie geschaffenen Systems auf EU-Flüge auszudehnen, sondern er hat, wie sich aus Art. 19 Abs. 3 der Richtlinie ergibt, seine Entscheidung über eine solche Ausweitung zurückgestellt, in der Annahme, dass ihr eine eingehende Prüfung ihrer rechtlichen Auswirkungen, insbesondere auf die Grundrechte der Betroffenen, vorausgehen sollte.

165. Insoweit ist darauf hinzuweisen, dass nach Art. 19 Abs. 3 der PNR-Richtlinie der in Art. 19 Abs. 1 genannte Bericht der Kommission ‘ zudem eine Überprüfung der Erforderlichkeit, Verhältnismäßigkeit und Wirksamkeit der Aufnahme der obligatorischen Erhebung und Übermittlung von PNR-Daten in Bezug auf sämtliche oder ausgewählte EU-Flüge in den Anwendungsbereich dieser Richtlinie [enthält] ’ und dass die Kommission dabei ‘ die Erfahrungen der Mitgliedstaaten, insbesondere jener Mitgliedstaaten, die gemäß [Artikel] 2 diese Richtlinie auf EU-Flüge anwenden ’, berücksichtigen muss; damit zeigt diese Vorschrift, dass für den Unionsgesetzgeber das durch die PNR-Richtlinie geschaffene System nicht zwangsläufig auf alle EU-Flüge ausgedehnt werden muss.

166. Im gleichen Sinne bestimmt Art. 2 Abs. 3 der PNR-Richtlinie, dass die Mitgliedstaaten beschließen können, diese Richtlinie nur auf ausgewählte EU-Flüge anzuwenden, wenn sie dies für die Verfolgung der Ziele der Richtlinie für erforderlich halten, und dass sie die Auswahl der Flüge jederzeit ändern können.

167. Die Befugnis der Mitgliedstaaten, die Anwendung des durch die PNR-Richtlinie geschaffenen Systems auf EU-Flüge auszudehnen, muss jedenfalls, wie sich aus ihrem 22. Erwägungsgrund ergibt, so ausgeübt werden, dass die durch die Art. 7 und 8 der Charta garantierten Grundrechte in vollem Umfang geachtet werden. Insoweit ist es zwar nach dem 19. Erwägungsgrund der Richtlinie Sache der Mitgliedstaaten, eine Einschätzung der Bedrohung durch terroristische Straftaten und schwere Kriminalität vorzunehmen, doch setzt die Ausübung dieser Befugnis voraus, dass die Mitgliedstaaten bei ihrer Einschätzung zu dem Ergebnis gelangen, dass eine Bedrohung durch solche strafbaren Handlungen vorliegt, die geeignet ist, die Anwendung der Richtlinie auch auf EU-Flüge zu rechtfertigen.

168. Unter diesen Umständen ist ein Mitgliedstaat, der von der in Art. 2 der PNR-Richtlinie vorgesehenen Befugnis – sei es für alle EU-Flüge (Art. 2 Abs. 2) oder nur für einige von ihnen (Art. 2 Abs. 3) – Gebrauch machen möchte, nicht von der Prüfung befreit, ob die Ausdehnung der Anwendung dieser Richtlinie auf alle oder einen Teil der EU-Flüge tatsächlich zur Verwirklichung des in Art. 1 Abs. 2 der Richtlinie genannten Ziels erforderlich ist und in angemessenem Verhältnis steht.

169. Unter Berücksichtigung der Erwägungsgründe 5 bis 7, 10 und 22 der PNR-Richtlinie muss ein solcher Mitgliedstaat daher prüfen, ob die in dieser Richtlinie vorgesehenen Verarbeitungen der PNR-Daten der Fluggäste aller oder einiger EU-Flüge in Anbetracht der Schwere des Eingriffs in die durch die Art. 7 und 8 der Charta garantierten Grundrechte zur Gewährleistung der inneren Sicherheit der Union oder zumindest des betreffenden Mitgliedstaats und damit zum Schutz des Lebens und der Sicherheit von Personen absolut notwendig ist.

170. Speziell zu den Bedrohungen durch terroristische Straftaten ergibt sich aus der Rechtsprechung des Gerichtshofs, dass terroristische Aktivitäten geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, und dass es ein zentrales Anliegen jedes Mitgliedstaats ist, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft durch die Verhütung und Repression solcher Tätigkeiten zu schützen, um die nationale Sicherheit zu wahren. Derartige Bedrohungen unterscheiden sich somit in ihrer Art, in ihrer besonderen Schwere und im spezifischen Charakter der sie begründenden Umstände von der allgemeinen und permanenten Gefahr des Auftretens schwerer Straftaten (vgl. in diesem Sinne Urteile vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 135 und 136, sowie vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 61 und 62).

171. In einer Situation, in der es nach der Einschätzung eines Mitgliedstaats hinreichend konkrete Umstände für die Annahme gibt, dass er mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist, werden die Grenzen des absolut Notwendigen nicht überschritten, wenn dieser Mitgliedstaat vorsieht, dass die PNR-Richtlinie gemäß ihrem Art. 2 Abs. 1 für begrenzte Zeit Anwendung auf alle EU-Flüge aus oder nach diesem Mitgliedstaat findet. Das Vorliegen einer derartigen Bedrohung ist nämlich als solches geeignet, einen Zusammenhang zwischen der Übermittlung und Verarbeitung der betreffenden Daten und der Bekämpfung des Terrorismus herzustellen (vgl. entsprechend Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 137).

172. Die Anordnung dieser Anwendung muss Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein können, deren Entscheidung bindend ist. Ferner muss der Zeitraum der Anwendung auf das absolut Notwendige begrenzt, aber im Fall des Fortbestands der Bedrohung verlängerbar sein (vgl. entsprechend Urteile vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 168, und vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 58).

173. In Ermangelung einer realen und aktuellen oder vorhersehbaren terroristischen Bedrohung des betreffenden Mitgliedstaats kann dagegen nicht von einer Beschränkung auf das absolut Notwendige ausgegangen werden, wenn das durch die PNR-Richtlinie geschaffene System unterschiedslos nicht nur auf Drittstaatsflüge, sondern auch auf alle EU-Flüge angewandt wird.

174. Die Anwendung des durch die PNR-Richtlinie geschaffenen Systems auf bestimmte EU-Flüge muss sich in einem solchen Fall auf die Übermittlung und Verarbeitung der PNR-Daten von Flügen beschränken, die etwa bestimmte Flugverbindungen, bestimmte Reisemuster oder bestimmte Flughäfen betreffen, für die es Anhaltspunkte gibt, die eine solche Anwendung rechtfertigen können. Es ist Sache des betreffenden Mitgliedstaats, in einem solchen Fall die EU-Flüge anhand der Ergebnisse der Einschätzung auszuwählen, die er auf der Grundlage der oben in den Rn. 163 bis 169 dargelegten Anforderungen vorzunehmen hat, und sie nach Maßgabe der Entwicklung der Bedingungen, die ihre Auswahl gerechtfertigt haben, regelmäßig zu überprüfen, um sicherzustellen, dass sich die Anwendung des durch die PNR-Richtlinie geschaffenen Systems auf EU-Flüge stets auf das absolut Notwendige beschränkt.

175. Aus den vorstehenden Erwägungen folgt, dass diese Auslegung von Art. 2 und Art. 3 Nr. 4 der PNR-Richtlinie im Licht der Art. 7 und 8 sowie von Art. 52 Abs. 1 der Charta zu gewährleisten vermag, dass diese Bestimmungen die Grenzen des absolut Notwendigen einhalten ».

B.38.1. Was den in der PNR-Richtlinie erwähnten Begriff « Fluggast » betrifft, hat der Gerichtshof der Europäischen Union geurteilt, dass, wenn die Daten der « Fluggäste » an die PNR-Zentralstelle des Mitgliedstaats übermittelt werden, unabhängig davon, ob es irgendwelche objektiven Anhaltspunkte dafür gibt, dass die betreffenden Fluggäste in terroristische Straftaten oder schwere Kriminalität verwickelt sein könnten, diese Daten automatisierten Verarbeitungen unterzogen werden, die, wie aus dem Erwägungsgrund 7 dieser Richtlinie hervorgeht, den Zweck haben, Personen zu ermitteln, die vor einer solchen Überprüfung nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die von den zuständigen Behörden genauer überprüft werden sollten (Randnr. 161).

Angesichts der Art der Bedrohungen für die öffentliche Sicherheit, die sich aus terroristischen Straftaten und schwerer Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Fluggästen ergeben können, ist der Gerichtshof der Europäischen Union der Auffassung, dass « die Übermittlung und Vorabüberprüfung der PNR-Daten von Fluggästen, die in die Union ein- oder aus der Union ausreisen, nicht auf einen bestimmten Kreis von Fluggästen beschränkt werden » können: Es « ist davon auszugehen, dass es den erforderlichen Zusammenhang zwischen diesen Daten und dem Ziel der Bekämpfung solcher strafbarer Handlungen gibt, so dass die PNR-Richtlinie nicht allein deshalb über das absolut Notwendige hinausgeht, weil sie den Mitgliedstaaten vorschreibt, die PNR-Daten aller dieser Fluggäste systematisch zu übermitteln und vorab zu überprüfen » (Randnr. 162).

B.38.2. Wie der Gerichtshof der Europäischen Union in dem vorerwähnten Urteil hervorhebt, unterliegt die Erhebung von Daten aller in Artikel 4 Nr. 10 des Gesetzes vom 25. Dezember 2016 erwähnten Fluggäste einer automatisierten Weiterverarbeitung, mit der unter diesen Fluggästen diejenigen ermittelt werden sollen, die von den zuständigen Behörden im Rahmen des Ziels der Bekämpfung terroristischer Straftaten und schwerer Kriminalität genauer überprüft werden müssen.

B.46.1. Ein solches System unterschiedet sich somit von einem System der allgemeinen und unterschiedslosen Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel sowie der Pflicht der Betreiber elektronischer Kommunikationsdienste, diese Daten systematisch und kontinuierlich ohne jede Ausnahme zu speichern (vgl. EuGH, Große Kammer, 21. Dezember 2016, C-203/15 und C-698/15, *Tele*2 *Sverige AB*, ECLI:EU:C:2016:970, Randnrn. 103-112).

B.39.1. In Bezug auf die betroffenen Flüge hat der Gerichtshof der Europäischen Union geurteilt, dass die Mitgliedstaaten, die entscheiden, die Anwendung des durch diese Richtlinie geschaffenen Systems auf EU-Flüge auszudehnen, nur eine von Artikel 2 Absatz 1 der PNR-Richtlinie eingeräumte Befugnis nutzen.

Der Bericht der Kommission « über die Überprüfung der Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität », der in B.36.4.1 zitierte wurde, stellt außerdem fest, dass alle Mitgliedstaaten mit Ausnahme eines einzigen das System der Erhebung von PNR-Daten auf EU-Flüge ausgedehnt haben.

B.39.2. Aus dem in B.37 zitierten Urteil des Gerichtshofs der Europäischen Union geht zudem hervor, dass die etwaige Ausdehnung des Systems zur Erhebung von PNR-Daten auf alle EU-Flüge, die ein Mitgliedstaat beschließen kann, indem er von der von dieser Richtlinie vorgesehenen Befugnis Gebrauch macht, an die Bedingung geknüpft ist, dass nach der Einschätzung eines Mitgliedstaats festgestellt wird, dass es hinreichend konkrete Umstände für die Annahme gibt, dass der betreffende Mitgliedstaat mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist, wobei das Vorliegen einer derartigen Bedrohung als solches geeignet ist, einen Zusammenhang zwischen der Übermittlung und Verarbeitung der betreffenden Daten und der Bekämpfung des Terrorismus herzustellen (Randnr. 171).

Die Anordnung dieser Anwendung muss außerdem Gegenstand einer wirksamen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein können, deren Entscheidung bindend ist, und der Zeitraum der Anwendung muss auf das absolut Notwendige begrenzt, aber im Fall des Fortbestands der Bedrohung verlängerbar sein (Randnr. 172).

Schließlich ist, wenn das Vorliegen dieser Bedrohung nicht erwiesen ist, das System zur Erhebung von PNR-Daten auf Flüge zu beschränken, die etwa bestimmte Flugverbindungen, bestimmte Reisemuster oder bestimmte Flughäfen betreffen, für die es nach Einschätzung des betreffenden Mitgliedstaates Anhaltspunkte gibt, die eine solche Anwendung rechtfertigen können, und dass diese Anwendung auf die so ausgewählten EU-Flüge auf das absolut Notwendige beschränkt ist, muss nach Maßgabe der Entwicklung der Bedingungen, die ihre Auswahl gerechtfertigt haben, regelmäßig überprüft werden (Randnr. 174).

B.40.1. Wie in den Vorarbeiten angegeben, soll mit dem Gesetz vom 25. Dezember 2016 durch die Umsetzung der PNR-Richtlinie die terroristische Bedrohung bekämpft werden:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 5).

B.40.2.1. Da Belgien der Ort von zwei terroristischen Attentaten war, die in den vorerwähnten Vorarbeiten angesprochen werden (Jüdisches Museum im Mai 2014 und Metrostation Maelbeek und Flughafen Zaventem im März 2016) konnte der Gesetzgeber bei der Annahme des Gesetzes vom 25. Dezember 2016 den Standpunkt vertreten, dass die terroristische Bedrohung real und aktuell ist.

Zudem ist erkennbar, dass diese terroristische Bedrohung nach wie vor real und aktuell ist. So berichtet das « Koordinierungsorgan für die Bedrohungsanalyse » (KOBA), das durch Artikel 5 des Gesetzes vom 10. Juli 2006 « über die Bedrohungsanalyse » (nachstehend: Gesetz vom 10. Juli 2006) eingerichtet wurde, 2022 über 215 Ausschreibungen im Zusammenhang mit Terrorismus und Extremismus und das allgemeine Bedrohungsniveau in Belgien liegt aktuell bei 2 von 4, das heißt einer mittleren Bedrohung.

B.40.2.2. Um die tatsächliche Bedrohung einzuschätzen, sind darüber hinaus die geografische Lage des Landes, die geringe Größe des Gebiets und die leicht passierbaren Grenzen, die Lage im Zentrum Europas und der Sitz zahlreicher europäischer und internationaler Institutionen zu berücksichtigen. Diese charakteristische geografische Realität des Landes erhöht die Risiken der Nutzung aller Beförderungsmittel durch Belgien, um terroristische Straftaten oder Straftaten der schweren Kriminalität zu begehen, erheblich. Das Land liegt geografisch somit an der Schnittstelle zahlreicher Verkehrswege im Luft-, Schienen oder Straßenverkehr, die von terroristischen und kriminellen Organisationen zur Begehung terroristischer Straftaten oder schwerer Kriminalität benutzt werden können.

B.40.2.3. Aus dem Vorstehenden geht hervor, dass die Einschätzung der Bedrohung, die die Ausdehnung des « PNR »-Systems auf alle EU-Flüge rechtfertigt, Gegenstand einer Kontrolle, im vorliegenden Fall einer gerichtlichen Kontrolle durch den Verfassungsgerichtshof war und dass ihre Realität und Aktualität festgestellt wurden.

B.40.3.1. Die der Gerichtshof der Europäischen Union betont, muss der Zeitraum der Anwendung der Maßnahmen, die durch die Einschätzung der Bedrohung gerechtfertigt sind, auf das « absolut Notwendige » beschränkt sein.

Diesbezüglich ist daran zu erinnern, dass zu den Aufträgen des KOBA der Auftrag gehört, « periodisch eine gemeinsame strategische Bewertung durchzuführen, die es ermöglichen muss zu beurteilen, ob die in Artikel 3 erwähnten Bedrohungen auftreten können oder, falls diese bereits festgestellt worden sind, wie sie sich entwickeln und welche Maßnahmen gegebenenfalls notwendig sind » (Artikel 8 Nr. 1 des vorerwähnten Gesetzes vom 10. Juli 2006) , wobei die in Artikel 3 erwähnten Bedrohungen « die in Artikel 8 Nr. 1 Buchstabe *b)* und *c)* des Grundlagengesetzes über die Nachrichten- und Sicherheitsdienste aufgezählten Bedrohungen, die die innere und äußere Sicherheit des Staates, die belgischen Interessen und die Sicherheit der belgischen Staatsangehörigen im Ausland oder jedes andere vom König auf Vorschlag des Nationalen Sicherheitsrats definierte Grundinteresse des Landes beeinträchtigen können » sind. Aus dem Vorstehenden ergibt sich, dass eine periodische Bewertung der Bedrohung geregelt und das KOBA damit beauftragt ist.

B.40.3.2. Im Übrigen sieht Artikel 52 § 1 des Gesetzes vom 25. Dezember 2016 eine Bewertung des Gesetzes drei Jahre nach seinem Inkrafttreten vor.

In Anbetracht des in B.40.2.3 Erwähnten bezüglich der Realität und Aktualität der Bedrohung obliegt es dem Gesetzgeber, auf der Grundlage der Einschätzung der Bedrohung durch das KOBA eine periodische Bewertung des Gesetzes vom 25. Dezember 2016 vorzunehmen, wobei eine erste Bewertung spätestens drei Jahre nach dem Datum der Verkündung des vorliegenden Entscheids erfolgen muss.

B.40.3.3. Sollte die Realität und Aktualität oder die Vorhersehbarkeit der Bedrohung nicht mehr erwiesen sein, obliegt es in diesem Fall dem Gesetzgeber, im Hinblick auf die verfolgten Ziele die Möglichkeit zu prüfen, das System zur Erhebung von PNR-Daten in der vom Gerichtshof der Europäischen Union in Randnummer 174 des vorerwähnten Urteils in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 angegebenen Weise zu beschränken.

B.41. Unter Berücksichtigung des in B.40.3.2 und B.40.3.3 Erwähnten ist der Klagegrund insofern, als er gegen Artikel 4 Nr. 10 des Gesetzes vom 25. Dezember 2016 gerichtet ist, unbegründet.

3. *Die Verarbeitungszwecke der PNR-Daten (Artikel 8)*

B.42. Die klagende Partei bemängelt die in Artikel 8 des Gesetzes vom 25. Dezember 2016 enthaltene Definition der Verarbeitungszwecke der PNR-Daten, die sehr viel umfassender seien als die « spezifischen Zwecke » der PNR-Richtlinie, die allein auf terroristische Straftaten und schwere Kriminalität beschränkt seien. Sie ist der Ansicht, dass diese Zwecke über das « absolut Notwendige » hinausgehen.

B.43.1. Artikel 1 Absatz 2 der PNR-Richtlinie bestimmt:

« Die nach Maßgabe dieser Richtlinie erhobenen PNR-Daten dürfen ausschließlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gemäß Artikel 6 Absatz 2 Buchstaben a, b und c verarbeitet werden ».

Artikel 6 Absatz 2 der PNR-Richtlinie bestimmt:

« 2. Die PNR-Zentralstelle verarbeitet PNR-Daten ausschließlich zu folgenden Zwecken:

a) Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat, um diejenigen Personen zu ermitteln, die von den zuständigen Behörden gemäß Artikel 7 und gegebenenfalls - im Einklang mit Artikel 10 - von Europol genauer überprüft werden müssen, da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind;

b) im Einzelfall Beantwortung von auf einer hinreichenden Grundlage gebührend begründeten Anfragen zuständiger Behörden hinsichtlich der Zurverfügungstellung und Verarbeitung von PNR-Daten in besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität, und der Zurverfügungstellung der Ergebnisse dieser Verarbeitung an die zuständigen Behörden oder gegebenenfalls an Europol, und

c) Analyse von PNR-Daten zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien zur Verwendung in gemäß Absatz 3 Buchstabe b durchgeführten Überprüfungen, die der Ermittlung von Personen gelten, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind ».

Im Erwägungsgrund 7 der PNR-Richtlinie ist weiter erläutert:

« Anhand einer Überprüfung von PNR-Daten können Personen ermittelt werden, die vor einer solchen Überprüfung nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die von den zuständigen Behörden genauer überprüft werden sollten. Durch die Verwendung von PNR-Daten ist es möglich, die Bedrohung durch terroristische Straftaten und schwere Kriminalität anders anzugehen, als dies durch Verarbeitung anderer Kategorien personenbezogener Daten möglich wäre. Damit die Verarbeitung von PNR-Daten jedoch auf das Erforderliche beschränkt bleibt, sollten die Aufstellung und Anwendung von Prüfkriterien auf terroristische Straftaten und schwere Kriminalität, für die die Anwendung solcher Kriterien maßgeblich ist, beschränkt werden. Darüber hinaus sollten die Prüfkriterien so festgelegt werden, dass die Zahl unschuldiger Personen, die fälschlicherweise vom System identifiziert werden, auf ein Minimum beschränkt wird ».

B.43.2. Die Verarbeitungszwecke der PNR-Daten, wie sie in der PNR-Richtlinie vorgesehen sind, bestehen also ausschließlich in der Zielsetzung der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

B.43.3. Artikel 3 Nummer 8 der PNR-Richtlinie definiert « terroristische Straftaten » als « die nach nationalem Recht strafbaren Handlungen im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI ».

Artikel 3 Nummer 9 der PNR-Richtlinie definiert « schwere Kriminalität » als « die in Anhang II aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind ».

Anhang II mit der Überschrift « Liste der strafbaren Handlungen gemäß Artikel 3 Nummer 9 » der PNR-Richtlinie bestimmt:

« 1. Beteiligung an einer kriminellen Vereinigung

2. Menschenhandel

3. Sexuelle Ausbeutung von Kindern und Kinderpornografie

4. Illegaler Handel mit Drogen und psychotropen Stoffen

5. Illegaler Handel mit Waffen, Munition und Sprengstoffen

6. Korruption

7. Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Union

8. Wäsche von Erträgen aus Straftaten und Geldfälschung, einschließlich Euro-Fälschung

9. Computerstraftaten/Cyberkriminalität

10. Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten

11. Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt

12. Vorsätzliche Tötung, schwere Körperverletzung

13. Illegaler Handel mit menschlichen Organen und menschlichem Gewebe

14. Entführung, Freiheitsberaubung und Geiselnahme

15. Diebstahl in organisierter Form oder mit Waffen

16. Illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen

17. Betrügerische Nachahmung und Produktpiraterie

18. Fälschung von amtlichen Dokumenten und Handel damit

19. Illegaler Handel mit Hormonen und anderen Wachstumsförderern

20. Illegaler Handel mit nuklearen und radioaktiven Substanzen

21. Vergewaltigung

22. Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen

23. Flugzeug- und Schiffsentführung

24. Sabotage

25. Handel mit gestohlenen Kraftfahrzeugen

26. Wirtschaftsspionage ».

B.44.1. In seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 hat der Gerichtshof der Europäischen Union in Bezug auf die Verarbeitungszwecke der PNR-Daten präzisiert:

« 2*) Zu den Zielsetzungen der Verarbeitungen von PNR-Daten*

141. Wie aus Art. 1 Abs. 2 der PNR-Richtlinie hervorgeht, sollen die Verarbeitungen der nach Maßgabe dieser Richtlinie erhobenen PNR-Daten zur Bekämpfung von ' terroristischen Straftaten ' und ' schwerer Kriminalität ' dienen.

142. Zu der Frage, ob die PNR-Richtlinie in diesem Bereich klare und präzise Regeln vorsieht, die die Anwendung des durch sie geschaffenen Systems auf das zu diesen Zwecken absolut Notwendige beschränken, ist zum einen festzustellen, dass der Begriff ' terroristische Straftaten ' in Art. 3 Nr. 8 der Richtlinie unter Bezugnahme auf ' die nach nationalem Recht strafbaren Handlungen im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses [2002/475] ' definiert wird.

143. Abgesehen davon, dass in den Art. 1 bis 3 des Rahmenbeschlusses 2002/475 klar und präzise definiert wurde, welche ' terroristischen Straftaten ', ' Straftaten im Zusammenhang mit einer terroristischen Vereinigung ' und ' Straftaten im Zusammenhang mit terroristischen Aktivitäten ' die Mitgliedstaaten gemäß diesem Rahmenbeschluss strafrechtlich verfolgen sollten, werden die betreffenden Straftaten auch in den Art. 3 bis 14 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475 und zur Änderung des Beschlusses 2005/671/JI des Rates (*ABl.* 2017, L 88, S. 6) klar und präzise definiert.

144. Zum anderen wird in Art. 3 Nr. 9 der PNR-Richtlinie der Begriff ' schwere Kriminalität ' unter Bezugnahme auf ' die in Anhang II [dieser Richtlinie] aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind ', definiert.

145. Zunächst werden in diesem Anhang die verschiedenen Kategorien strafbarer Handlungen, die zur ' schweren Kriminalität ' im Sinne von Art. 3 Nr. 9 der PNR-Richtlinie gehören können, abschließend aufgezählt.

146. Sodann konnte sich der Unionsgesetzgeber - angesichts der Besonderheiten, die die Strafrechtssysteme der Mitgliedstaaten beim Erlass der genannten Richtlinie mangels einer Harmonisierung der betreffenden Straftaten aufwiesen - damit begnügen, auf Kategorien strafbarer Handlungen Bezug zu nehmen, ohne ihre Tatbestandsmerkmale zu definieren, zumal diese Merkmale zwangsläufig im nationalen Recht, auf das Art. 3 Nr. 9 der PNR-Richtlinie verweist, definiert werden, da die Mitgliedstaaten den Grundsatz der Gesetzmäßigkeit im Zusammenhang mit Straftaten und Strafen als Bestandteil des gemeinsamen, mit der Union geteilten Wertes der Rechtsstaatlichkeit (Art. 2 EUV) beachten müssen (vgl. entsprechend Urteil vom 16. Februar 2022, *Ungarn/Parlament und Rat*, C-156/21, EU:C:2022:97, Rn. 136, 160 und 234), einen Grundsatz, der überdies in Art. 49 Abs. 1 der Charta verankert ist und an den sich die Mitgliedstaaten bei der Umsetzung eines Rechtsakts der Union wie der PNR-Richtlinie halten müssen (vgl. in diesem Sinne Urteil vom 10. November 2011, QB, C-405/10, EU:C:2011:722, Rn. 48 und die dort angeführte Rechtsprechung). Somit ist auch unter Berücksichtigung des gewöhnlichen Sinns der in Anhang II verwendeten Begriffe davon auszugehen, dass die strafbaren Handlungen, die schwere Kriminalität darstellen können, dort hinreichend klar und präzise bestimmt werden.

147. Die Nrn. 7, 8, 10 und 16 des Anhangs II betreffen zwar sehr allgemeine Kategorien strafbarer Handlungen (Betrugsdelikte, Wäsche von Erträgen aus Straftaten und Geldfälschung, Umweltkriminalität, illegaler Handel mit Kulturgütern), nehmen dabei aber gleichwohl Bezug auf konkrete strafbare Handlungen, die zu diesen allgemeinen Kategorien gehören. Zur Gewährleistung der auch nach Art. 49 der Charta erforderlichen hinreichenden Genauigkeit sind sie dahin auszulegen, dass sie sich auf die genannten strafbaren Handlungen in ihrer Ausgestaltung durch das einschlägige nationale Recht und/oder Unionsrecht beziehen. Werden sie in dieser Weise ausgelegt, kann davon ausgegangen werden, dass sie den Anforderungen an Klarheit und Genauigkeit genügen.

148. Schließlich ist darauf hinzuweisen, dass nach dem Grundsatz der Verhältnismäßigkeit das Ziel der Bekämpfung schwerer Kriminalität zwar geeignet ist, den mit der PNR-Richtlinie verbundenen schweren Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte zu rechtfertigen; anders verhält es sich jedoch mit dem Ziel der Bekämpfung der Kriminalität im Allgemeinen, das nur Eingriffe rechtfertigen kann, die nicht schwer sind (vgl. entsprechend Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 59 und die dort angeführte Rechtsprechung). Somit muss diese Richtlinie durch klare und präzise Regeln sicherstellen, dass sich die Anwendung des durch sie geschaffenen Systems allein auf strafbare Handlungen beschränkt, die der schweren Kriminalität zuzurechnen sind, und damit Taten aus dem Bereich der gewöhnlichen Kriminalität ausschließt.

149. Hierzu hat der Generalanwalt in Nr. 121 seiner Schlussanträge ausgeführt, dass etliche der in Anhang II der PNR-Richtlinie aufgeführten strafbaren Handlungen - wie Menschenhandel, sexuelle Ausbeutung von Kindern und Kinderpornografie, illegaler Handel mit Waffen, Munition und Sprengstoffen, Geldwäsche, Cyberkriminalität, illegaler Handel mit menschlichen Organen und menschlichem Gewebe, illegaler Handel mit Drogen und psychotropen Stoffen, illegaler Handel mit nuklearen und radioaktiven Substanzen, Flugzeug- und Schiffsentführung, Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen, vorsätzliche Tötung, Vergewaltigung, Entführung, Freiheitsberaubung und Geiselnahme - ihrem Wesen nach einen unbestreitbar hohen Schweregrad aufweisen.

150. Außerdem können andere, ebenfalls in Anhang II aufgeführte strafbare Handlungen zwar *a priori* nicht so leicht mit schwerer Kriminalität in Verbindung gebracht werden, doch ergibt sich bereits aus dem Wortlaut von Art. 3 Nr. 9 der PNR-Richtlinie, dass diese strafbaren Handlungen nur dann als schwere Kriminalität eingestuft werden können, wenn sie nach dem nationalen Recht des betreffenden Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind. Die aus dieser Bestimmung resultierenden Anforderungen, die sich auf Art und Schwere der verwirkten Strafe beziehen, sind grundsätzlich geeignet, die Anwendung des durch die Richtlinie geschaffenen Systems auf strafbare Handlungen mit hinreichendem Schweregrad zu beschränken, die den mit dem durch die Richtlinie geschaffenen System verbundenen Eingriff in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, rechtfertigen können.

151. Da sich Art. 3 Nr. 9 der PNR-Richtlinie nicht auf die jeweilige Mindeststrafe, sondern auf die jeweilige Höchststrafe bezieht, ist jedoch nicht ausgeschlossen, dass die PNR-Daten Gegenstand einer Verarbeitung zur Bekämpfung strafbarer Handlungen sein können, die, obwohl sie das in dieser Bestimmung vorgesehene Kriterium in Bezug auf den Schweregrad erfüllen, angesichts der Besonderheiten des nationalen Strafrechtssystems nicht zur schweren Kriminalität gehören, sondern zur gewöhnlichen Kriminalität.

152. Es ist daher Sache der Mitgliedstaaten, dafür zu sorgen, dass die Anwendung des durch die PNR-Richtlinie geschaffenen Systems tatsächlich auf die Bekämpfung schwerer Kriminalität beschränkt bleibt und dass dieses System nicht auf strafbare Handlungen erstreckt wird, die zur gewöhnlichen Kriminalität gehören.

3*) Zum Zusammenhang zwischen den PNR-Daten und den Zielsetzungen der Verarbeitung dieser Daten*

153. Es trifft zu, dass, wie der Generalanwalt in Nr. 119 seiner Schlussanträge im Wesentlichen ausgeführt hat, in Art. 3 Nr. 8 und in Art. 3 Nr. 9 der PNR-Richtlinie in Verbindung mit ihrem Anhang II nicht ausdrücklich auf ein Kriterium abgestellt wird, das geeignet wäre, den Anwendungsbereich der Richtlinie auf strafbare Handlungen zu beschränken, die ihrem Wesen nach - zumindest mittelbar - einen objektiven Zusammenhang mit Flugreisen und infolgedessen mit den nach der Richtlinie zu übermittelnden, zu verarbeitenden und zu speichernden Datenkategorien aufweisen können.

154. Wie der Generalanwalt in Nr. 121 seiner Schlussanträge ausgeführt hat, können jedoch bestimmte in Anhang II der PNR-Richtlinie genannte strafbare Handlungen wie Menschenhandel, Handel mit Drogen oder Waffen, Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt sowie Flugzeugentführung ihrem Wesen nach einen unmittelbaren Zusammenhang mit der Beförderung von Fluggästen aufweisen. Gleiches gilt für bestimmte terroristische Straftaten wie schwerwiegende Zerstörungen an einem Verkehrsmittel oder einer Infrastruktur oder das Kapern von Luftfahrzeugen, die in Art. 1 Abs. 1 Buchst. d und e des Rahmenbeschlusses 2002/475, auf den Art. 3 Nr. 8 der PNR-Richtlinie verweist, genannt waren, sowie für Reisen zu terroristischen Zwecken und die Organisation oder sonstige Erleichterung solcher Reisen (Art. 9 und 10 der Richtlinie 2017/541).

155. In diesem Zusammenhang ist ferner darauf hinzuweisen, dass die Kommission zur Begründung ihres Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität vom 2. Februar 2011 (KOM[2011] 32 endgültig), auf dem die PNR-Richtlinie beruht, hervorgehoben hat, dass ‘ [d]ie Terroranschläge in den Vereinigten Staaten von 2001, der vereitelte Terroranschlag vom August 2006, bei dem mehrere Flugzeuge auf dem Weg von Großbritannien in die Vereinigten Staaten in die Luft gesprengt werden sollten, und der Anschlagsversuch an Bord eines Fluges von Amsterdam nach Detroit vom Dezember 2009 ... deutlich [machen], dass Terroristen in der Lage sind, in jedem Land Anschläge zu begehen und dabei internationale Flüge ins Visier zu nehmen ’, und dass ‘ die meisten terroristischen Aktivitäten grenzüberschreitenden Charakter haben und mit Reisen in andere Länder, unter anderem in Ausbildungslager außerhalb der EU, verbunden sind ’. Außerdem verwies die Kommission zur Rechtfertigung des Erfordernisses einer Auswertung der PNR-Daten zur Bekämpfung schwerer Kriminalität als Beispiel auf den Fall eines Menschenhändlerrings, der bei der Abfertigung für einen Flug gefälschte Reisedokumente vorgelegt hatte, sowie auf einen Fall von Menschen- und Drogenhandel im großen Maßstab, bei dem Opfer von Menschenhandel zum Schmuggel von Drogen in verschiedene europäische Länder eingesetzt und deren Flugscheine mit gestohlenen Kreditkarten gekauft wurden. Alle diese Fälle betrafen strafbare Handlungen, bei denen insofern ein unmittelbarer Zusammenhang mit der Beförderung von Fluggästen bestand, als die strafbaren Handlungen auf die Beförderung von Fluggästen abzielten oder anlässlich oder mit Hilfe einer Flugreise begangen wurden.

156. Überdies ist festzustellen, dass auch strafbare Handlungen, die keinen solchen unmittelbaren Zusammenhang mit der Beförderung von Fluggästen aufweisen, je nach den Umständen des Einzelfalls einen mittelbaren Zusammenhang mit der Beförderung der Fluggäste aufweisen können. Dies gilt insbesondere dann, wenn die Beförderung auf dem Luftweg als Mittel zur Vorbereitung solcher strafbarer Handlungen dient oder dazu, sich nach deren Begehung der strafrechtlichen Verfolgung zu entziehen. Dagegen können strafbare Handlungen, die keinen auch nur mittelbaren objektiven Zusammenhang mit der Beförderung von Fluggästen haben, die Anwendung des durch die PNR-Richtlinie geschaffenen Systems nicht rechtfertigen.

157. Unter diesen Umständen verlangt Art. 3 Nrn. 8 und 9 der PNR-Richtlinie in Verbindung mit deren Anhang II und im Licht der Anforderungen, die sich aus den Art. 7 und 8 sowie aus Art. 52 Abs. 1 der Charta ergeben, von den Mitgliedstaaten, u. a. bei der in Art. 6 Abs. 5 der Richtlinie vorgesehenen individuellen Überprüfung auf nicht automatisierte Art dafür zu sorgen, dass die Anwendung des durch die Richtlinie geschaffenen Systems auf terroristische Straftaten und auf schwere Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen beschränkt wird ».

B.44.2. Aus dem Vorstehenden geht hervor, dass die Zwecke der Erhebung und Verarbeitung der PNR-Daten, um mit den Anforderungen insbesondere aus den Artikeln 7 und 8 sowie 52 Absatz 1 der Charta der Grundrechte vereinbar zu sein, strikt auf die Zwecke der Verhütung, Aufdeckung sowie der Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, unter Bezugnahme auf die abschließend in Anhang II der PNR-Richtlinie aufgezählten Kategorien von Straftaten, die einen - zumindest mittelbaren - objektiven Zusammenhang mit der betreffenden Beförderung aufweisen, beschränkt sein müssen und dieses System nicht auf Straftaten, die zur gewöhnlichen Kriminalität gehören, ausgedehnt werden darf. Was die schwere Kriminalität betrifft, darf die Anwendung des PNR-Systems nicht auf Straftaten ausgedehnt werden, die, auch wenn sie das von dieser Richtlinie vorgesehene Kriterium in Bezug auf den Schweregrad erfüllen und auch wenn sie insbesondere in Anhang II der Richtlinie aufgeführt sind, angesichts der Besonderheiten des nationalen Strafrechtssystems zur gewöhnlichen Kriminalität gehören (Randnrn. 151 und 152).

B.45.1. Artikel 8 des Gesetzes vom 25. Dezember 2016 definiert die Verarbeitungszwecke der PNR-Daten.

In seiner ursprünglichen Fassung lautete Artikel 8 des Gesetzes vom 25. Dezember 2016:

« § 1. Die Passagierdaten werden zu folgenden Zwecken verarbeitet:

1. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 90*ter* § 2 Nr. 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 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten,

2. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 196, was die Fälschung authentischer und öffentlicher Urkunden betrifft, 198, 199, 199*bis*, 207, 213, 375 und 505 des Strafgesetzbuches erwähnten Straftaten,

3. Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung durch Beobachtung der Phänomene und Gruppierungen gemäß Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 über das Polizeiamt,

4. Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Aktivitäten,

5. Ermittlung und Verfolgung der in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten.

§ 2. Die Passagierdaten werden unter den in Kapitel 11 erwähnten Bedingungen ebenfalls verarbeitet, um die Personenkontrolle an den Außengrenzen zu verbessern und die illegale Einwanderung zu bekämpfen ».

Aufgrund von Artikel 13 § 2 des Gesetzes vom 25. Dezember 2016 « darf die PNR-Zentralstelle » unbeschadet anderer gesetzlicher Bestimmungen « die aufgrund von Kapitel 9 aufbewahrten Daten nicht zu anderen als den in Artikel 8 erwähnten Zwecken benutzen ».

B.45.2.1. Wie in B.11 erwähnt, ist Artikel 8 § 1 Nr. 1 und 5 des Gesetzes vom 25. Dezember 2016 außerdem durch Artikel 62 des Gesetzes vom 15. Juli 2018 ersetzt worden.

B.45.2.2. Artikel 62 des Gesetzes vom 15. Juli 2018 ersetzt zunächst Artikel 8 § 1 Nr. 1 des Gesetzes vom 25. Dezember 2016. Ursprünglich waren die « in Artikel 90*ter* § 2 Nr. 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 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten » aufgeführt. Seit der Abänderung durch Artikel 62 des Gesetzes vom 15. Juli 2018 sind die « in Artikel 90*ter* § 2 Nr. 2, 3, 7, 8, 11, 14, 17 bis 20, 22, 24 bis 28, 30, 32, 33, 34, 36 bis 39, 43 bis 45 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten » aufgeführt.

Angesichts dieser Abänderungen ist die Nichtigkeitsklage gegenstandslos geworden, insofern in Artikel 8 § 1 Nr. 1 des Gesetzes vom 25. Dezember 2016 die in Artikel 90*ter* § 2 Nr. 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* und 16 des Strafprozessgesetzbuches erwähnten Straftaten aufgeführt sind. Hingegen behält die Nichtigkeitsklage ihren Gegenstand, insofern sie sich gegen Artikel 8 § 1 Nr. 1 des Gesetzes vom 25. Dezember 2016 richtet, insoweit in diesem Artikel die in Artikel 90*ter* § 2 Nr. 7, 8, 11, 14, 17, 18, 19 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten aufgeführt sind.

Die in Artikel 90*ter* § 2 Nr. 7, 8, 11, 14, 17, 18, 19 und § 3 des Strafprozessgesetzbuches erwähnten Straftaten sind die Straftaten, die in Artikel 210*bis* des Strafgesetzbuches (Informatikfälschung), in den Artikeln 246, 247, 248, 249 und 250 desselben Gesetzbuches (Korruption von Personen, die ein öffentliches Amt ausüben), in den Artikeln 324*bis* und 324*ter* desselben Gesetzbuches (Teilnahme an einer kriminellen Organisation), in Artikel 347*bis* desselben Gesetzbuches (Geiselnahmen), in den Artikeln 379, 380 und 383*bis* §§ 1 und 3 desselben Gesetzbuches (Anstiftung Jugendlicher zur Unzucht und Prostitution und Verstoß gegen die guten Sitten), in Artikel 393 desselben Gesetzbuches (Tötung) und in den Artikeln 394 und 397 desselben Gesetzbuches (Totschlag und Vergiftung) aufgeführt sind.

B.45.2.3. Artikel 62 des Gesetzes vom 15. Juli 2018 ersetzt anschließend Artikel 8 § 1 Nr. 5 des Gesetzes vom 25. Dezember 2016. Ursprünglich waren die « in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten » aufgeführt. Seit der Abänderung durch Artikel 62 des Gesetzes vom 15. Juli 2018 sind die « Straftaten, erwähnt in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen, in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung, in Artikel 5 des Gesetzes vom 15. Mai 2007 über die Ahndung der Nachahmung und der Piraterie von geistigen Eigentumsrechten, in Artikel 26 des Dekretes der Deutschsprachigen Gemeinschaft vom 20. Februar 2017 zum Schutz des beweglichen Kulturgutes von außerordentlicher Bedeutung sowie in Artikel 24 des Dekretes der Flämischen Gemeinschaft vom 24. Januar 2003 ' houdende bescherming van het roerend cultureel erfgoed van uitzonderlijk belang ' (Schutz des beweglichen Kulturerbes von außerordentlicher Bedeutung), im Ministeriellen Erlass vom 7. Februar 2012 zur Einführung einer Lizenzpflicht für die Einfuhr von Waren, deren Ursprung oder Herkunft Syrien ist, abgeändert durch den Ministeriellen Erlass vom 1. Juli 2014, im Ministeriellen Erlass vom 23. März 2004 zur Aufhebung des Ministeriellen Erlasses vom 17. Januar 2003 zur Einführung der Pflicht, für die Ein-, Aus- und Durchfuhr von Waren, deren Ursprung, Herkunft oder Bestimmung der Irak ist, über eine vorherige Ermächtigung zu verfügen und für die Ein-, Aus- und Durchfuhr bestimmter Waren, deren Ursprung, Herkunft oder Bestimmung der Irak ist, über eine Lizenz zu verfügen, sowie Ermittlung der Verstöße, erwähnt in Artikel 5 des Gesetzes vom 28. Juli 1981 zur Billigung des Übereinkommens über den internationalen Handel mit gefährdeten Arten freilebender Tiere und Pflanzen und der Anlagen, abgeschlossen in Washington am 3. März 1973, und der Änderung des Übereinkommens, angenommen in Bonn am 22. Juni 1979 » aufgeführt.

Da die Abänderung von Artikel 8 § 1 Nr. 5 des Gesetzes vom 25. Dezember 2016 durch Artikel 62 des Gesetzes vom 15. Juli 2018 nur den Anwendungsbereich der aufgeführten Straftaten erweitert, behält die Nichtigkeitsklage ihren Gegenstand, insofern sie gegen Artikel 8 § 1 Nr. 5 des Gesetzes vom 25. Dezember 2016 gerichtet ist, insoweit in diesem Artikel die « in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen und Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung erwähnten Straftaten » aufgeführt sind.

Unter diese Straftaten fallen die organisierte oder nicht organisierte schwere Steuerhinterziehung im Rahmen von Verstößen gegen die Rechtsvorschriften über Zölle und Akzisen.

B.45.3. In Bezug auf die an die PNR-Richtlinie angelehnten Zwecke heißt es in der Begründung des Gesetzes vom 25. Dezember 2016:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 17-20).

B.45.4. Die in Artikel 8 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecke bilden einen erschöpfenden Rahmen für die zulässigen Verarbeitungen von Passagierdaten.

Wie in B.10 erwähnt, ist Artikel 8 des Gesetzes vom 25. Dezember 2016 außerdem im Lichte des Gesetzes vom 30. Juli 2018 auszulegen.

In den in B.10.2 erwähnten Vorarbeiten zum Gesetz vom 30. Juli 2018 ist angegeben, dass die in Artikel 8 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecke in drei Kategorien unterteilt sind:

- die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Straftaten oder die Strafvollstreckung (Artikel 8 § 1 Nrn. 1, 2, 3 und 5 des Gesetzes vom 25. Dezember 2016); diese Verarbeitungen sind in Titel 2 des Gesetzes vom 30. Juli 2018 geregelt;

- die in den Artikeln 7 und 11 des Gesetzes vom 30. November 1998 erwähnten Aufträge der Nachrichten- und Sicherheitsdienste (Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016); diese Verarbeitungen sind in Titel 3 des Gesetzes vom 30. Juli 2018 geregelt;

- die Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung (Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016); diese Verarbeitungen sind in Titel 1 des Gesetzes vom 30. Juli 2018 geregelt.

B.46.1. Aus dem in B.45 Erwähnten geht hervor, dass einige der in Artikel 8 des Gesetzes vom 25. Dezember 2016 erwähnten Verarbeitungszwecke den Straftaten in Anhang II der PNR-Richtlinie gemäß den in der Richtlinie genannten Zielen der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität entsprechen (Artikel 8 § 1 Nr. 1, 2 und 5) und schwere Straftaten nach dem nationalen Recht betreffen.

Wie in B.31.1 erwähnt, stellt die Verfolgung dieser Ziele durch die Erhebung und Verarbeitung der PNR-Daten eine dem Gemeinwohl dienende Zielsetzung dar, die eine Einmischung in das Recht auf Achtung des Privatlebens und Schutz personenbezogener Daten rechtfertigen kann.

Wie der Gerichtshof der Europäischen Union in seinem in B.44 zitierten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* erkannt hat, ist die Anwendung des « PNR »-Systems auf solche Zwecke, die strikt auf die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität beschränkt sind, mit den Anforderungen des « absolut Notwendigen » vereinbar.

B.46.2. Die zur Bestimmung dieser Zwecke verwendeten Begriffe sind klar und präzise definiert, da sie auf die in den Bestimmungen des Strafgesetzbuches definierten Straftaten verweisen.

Solche Regeln, in denen die Straftaten, die man verhüten, aufdecken und verfolgen möchte, bestimmt werden, sind gemäß den in B.25 genannten Anforderungen klar und präzise und auf das absolut Notwendige beschränkt.

B.47.1. Jedoch kommen einige Verarbeitungszwecke der PNR-Daten zu denjenigen hinzu, die in der PNR-Richtlinie vorgesehen sind. Dies gilt für:

- die « Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung durch Beobachtung der Phänomene und Gruppierungen gemäß Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 über das Polizeiamt » (Artikel 8 § 1 Nr. 3);

- die « Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Aktivitäten » (Artikel 8 § 1 Nr. 4);

- die Verbesserung der Personenkontrolle an den Außengrenzen und die Bekämpfung der illegalen Einwanderung (Artikel 8 § 2).

B.47.2. Es ist zu prüfen, ob diese weiteren Zwecke in klaren, präzisen und auf das absolut Notwendige beschränkten Regeln gemäß den in B.25 genannten Anforderungen zum Ausdruck gebracht wurden, unter Berücksichtigung des in B.44 in Erinnerung gerufenen Urteils des Gerichtshofes der Europäischen Union.

B.48. Was den Zweck der « Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung durch Beobachtung der Phänomene und Gruppierungen gemäß Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 über das Polizeiamt » (Artikel 8 § 1 Nr. 3) betrifft, hat der Gerichtshof mit seinem Entscheid Nr. 135/2019 geurteilt:

« B.53.1. Was den Zweck der Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung betrifft, der in Artikel 8 § 1 Nr. 3 des Gesetzes vom 25. Dezember 2016 erwähnt ist, wird auf die Beobachtung der ' Phänomene ' und ' Gruppierungen ' gemäß Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 ' über das Polizeiamt ' (nachstehend: Gesetz vom 5. August 1992) Bezug genommen.

Artikel 44/1 des Gesetzes vom 5. August 1992 sieht vor, dass die Polizeidienste im Rahmen der Erfüllung ihrer Aufträge Informationen und personenbezogene Daten verarbeiten können.

Gemäß Artikel 44/2 des Gesetzes vom 5. August 1992 werden diese personenbezogenen Daten und Informationen in einer operativen polizeilichen Datenbank (1. Allgemeine Nationale Datenbank, 2. Basisdatenbanken oder 3. besondere Datenbanken) gemäß den jeweiligen Zwecken der Kategorien der Datenbanken verarbeitet, wenn die Polizeidienste zur Erfüllung der verwaltungspolizeilichen und gerichtspolizeilichen Aufträge diese so strukturieren müssen, dass sie direkt wieder aufgefunden werden können.

Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 bestimmt:

' Die personenbezogenen Daten, die zu verwaltungspolizeilichen Zwecken in den in Artikel 44/2 § 1 Absatz 2 Nr. 1 und 2 erwähnten Datenbanken verarbeitet werden, sind folgende:

[...]

2. Daten in Bezug auf Personen, die von verwaltungspolizeilichen Phänomenen betroffen sind, das heißt von allen Problemen, die eine Störung der öffentlichen Ordnung darstellen und angepasste verwaltungspolizeiliche Maßnahmen notwendig machen, weil sie gleicher Art sind und wiederkehren, von denselben Personen begangen werden oder gegen dieselben Kategorien von Opfern oder Orten gerichtet sind,

3. Daten in Bezug auf Mitglieder einer nationalen oder internationalen Gruppierung, die die in Artikel 14 erwähnte öffentliche Ordnung stören könnten,

[...]

§ 2. Die Liste der in § 1 Nr. 2 erwähnten Phänomene und der in § 1 Nr. 3 erwähnten Gruppierungen wird mindestens jährlich vom Minister des Innern erstellt, auf der Grundlage eines gemeinsamen Vorschlags der föderalen Polizei, des Koordinierungsorgans für die Bedrohungsanalyse und der Nachrichten- und Sicherheitsdienste '.

B.53.2. In Bezug auf den in Artikel 8 § 1 Nr. 3 erwähnten Zweck heißt es in der Begründung:

‘ 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*) ’ (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 18-19).

Der Minister der Sicherheit und des Innern hat auch erläutert, dass der Begriff der gewalttätigen Radikalisierung ‘ im Sinne des Rundschreibens verstanden werden ’ muss (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/003, S. 31).

B.53.3. Aus dem Vorstehenden geht hervor, dass der Zweck der Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung auf eine schwerwiegende Bedrohung für die öffentliche Ordnung, die sich aus der gewalttätigen Radikalisierung im Sinne des ministeriellen Rundschreibens GPI 78 vom 31. Januar 2014 ‘ über die Informationsverarbeitung für eine integrierte Vorgehensweise gegen den Terrorismus und die gewalttätige Radikalisierung durch die Polizei ’ (nachstehend: ministerielles Rundschreiben) ergibt, beschränkt ist.

B.53.4. Bei diesem Zweck findet im Übrigen im Rahmen der Vorabüberprüfung der Passagiere eine eingeschränktere Verarbeitung als bei den anderen Zwecken zur Verhinderung und Ermittlung der in Artikel 8 § 1 des Gesetzes vom 25. Dezember 2016 erwähnten Straftaten statt.

So sieht Artikel 24 § 3 des Gesetzes vom 25. Dezember 2016 vor, dass im Rahmen der in Artikel 8 § 1 Nr. 3 erwähnten Zwecke ‘ die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und den in § 2 Nr. 1 erwähnten Datenbanken [beruht] ’. Zudem sieht Artikel 26 § 1 des Gesetzes vom 25. Dezember 2016 vor, dass für den in Artikel 8 § 1 Nr. 3 erwähnten Zweck nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten (API-Daten), die sich auf die Person(en) beziehen, für die sich ein Treffer ergeben hat, zugänglich sind. Schließlich schließt es Artikel 27 des Gesetzes vom 25. Dezember 2016 aus, dass gezielte Recherchen zu den in Artikel 8 § 1 Nr. 3 erwähnten Zwecken durchgeführt werden.

In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 heißt es:

‘ 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 ’ (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 30).

B.53.5. Zwar sind die Begriffe ‘ Phänomene ’ und ‘ Gruppierungen ’ in Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 definiert, aber dies gilt nicht für den Begriff ‘ gewalttätige Radikalisierung ’, der nicht gesetzlich definiert ist.

Jedoch definiert Artikel 3 Nr. 15 des Grundlagengesetzes vom 30. November 1998 ‘ über die Nachrichten- und Sicherheitsdienste ’ (nachstehend: Gesetz vom 30. November 1998) den ‘ Radikalisierungsprozess ’ als einen ‘ Prozess, bei dem ein Individuum oder eine Gruppe von Individuen so beeinflusst wird, dass dieses Individuum beziehungsweise diese Gruppe von Individuen mental darauf vorbereitet ist oder bereit ist, Terrorakte zu begehen ’.

Außerdem ist in Artikel 1 des ministeriellen Rundschreibens die ‘ gewalttätige Radikalisierung ’ wie folgt definiert:

‘ 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 ’.

Auch wenn der Begriff ‘ gewalttätige Radikalisierung ’ nicht gesetzlich definiert ist, deutet seine Definition durch das ministerielle Rundschreiben darauf hin, dass er anhand der Begriffe ‘ Phänomene ’ und ‘ Gruppierungen ’, die gesetzlich in Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 definiert sind, zu verstehen ist. Einer solchen Maßnahme mangelt es also nicht an Klarheit und Präzision.

B.53.6. Aus dieser Definition wird außerdem ersichtlich, dass die anhand der ‘ Phänomene ’ und ‘ Gruppierungen ’ verstandene gewalttätige Radikalisierung im direkten Zusammenhang mit terroristischen Taten oder schwerer Kriminalität steht, die sowohl durch die PNR-Richtlinie als auch durch das Gesetz vom 25. Dezember 2016 verhütet, aufgedeckt und verfolgt werden sollen.

Eine solche Maßnahme ist somit klar und präzise und in Anbetracht der im vorliegenden Fall verfolgten legitimen Zielsetzung nicht unverhältnismäßig ».

B.49.1. Wie der Verfassungsgerichtshof in seinem vorerwähnten Entscheid Nr. 135/2019 geurteilt hat, ist der Zweck der Verhinderung « schwerer Störungen » der öffentlichen Sicherheit im Rahmen der « gewalttätigen Radikalisierung » ein Ausdruck, der auf ein Gruppenphänomen abzielt, das die öffentliche Sicherheit ernsthaft gefährdet, und der in direktem Zusammenhang mit terroristischen Straftaten oder schwerer Kriminalität steht, die sowohl die PNR-Richtlinie als auch das Gesetz vom 25. Dezember 2016 verhüten, aufdecken und verfolgen sollen.

Daraus ergibt sich, dass die Verhinderung « schwerer Störungen » der öffentlichen Sicherheit im Rahmen der « gewalttätigen Radikalisierung », die nur im Zusammenhang mit der Begehung gemeinrechtlicher Straftaten steht, nicht unter den in Artikel 8 § 1 Nr. 3 des Gesetzes vom 25. Dezember 2016 erwähnten Zweck fällt.

Die Verarbeitung und Erhebung von PNR-Daten für diesen so verstandenen Zweck fällt daher unter die von der PNR-Richtlinie verfolgten Ziele, wie sie vom Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 dargelegt wurden. Wie in B.53.4 des vorerwähnten Entscheids Nr. 135/2019 erwähnt, ist die Verarbeitung von PNR-Daten für diesen Zweck außerdem eingeschränkter als bei den anderen Zwecken zur Verhinderung und Ermittlung der in Artikel 8 § 1 des Gesetzes vom 25. Dezember 2016 erwähnten Straftaten.

B.49.2. Wie der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat*, auf das in B.44 hingewiesen wurde, ausgeführt hat, müssen die Verarbeitungszwecke der PNR-Daten zudem einen – zumindest mittelbaren – objektiven Zusammenhang mit der betreffenden Beförderung aufweisen.

Daraus folgt, dass die Verhinderung « schwerer Störungen » der öffentlichen Sicherheit im Rahmen der « gewalttätigen Radikalisierung », für die keine Benutzung von Beförderungsmitteln erforderlich ist, nicht zum Anwendungsbereich des in Artikel 8 § 1 Nr. 3 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecks gehören kann.

B.49.3. Vorbehaltlich dessen, dass der Zweck der Verhinderung « schwerer Störungen » der öffentlichen Sicherheit im Rahmen der « gewalttätigen Radikalisierung » dahin ausgelegt wird, dass er strikt auf die Zwecke der Verhütung und Aufdeckung allein von terroristischen Straftaten und allein von schwerer Kriminalität, unter Bezugnahme auf die abschließend in Anhang II der PNR-Richtlinie aufgezählten Kategorien von Straftaten, die einen – zumindest mittelbaren – objektiven Zusammenhang mit der betreffenden Beförderung aufweisen, beschränkt ist, überschreitet Artikel 8 § 1 Nr. 3 des Gesetzes vom 25. Dezember 2016 nicht das « absolut Notwendige ».

B.50.1. Gemäß Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 dient die Verarbeitung der PNR-Daten zur Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Gesetzes vom 30. November 1998 erwähnten Aktivitäten.

Artikel 7 des Gesetzes vom 30. November 1998 bestimmt:

« Die Staatssicherheit ist beauftragt:

1. Nachrichten in Bezug auf jegliche Aktivität, die die innere Sicherheit des Staates und den Fortbestand der demokratischen und verfassungsmäßigen Ordnung, die äußere Sicherheit des Staates und die internationalen Beziehungen, das vom Nationalen Sicherheitsrat definierte wissenschaftliche oder wirtschaftliche Potential oder jedes andere vom König auf Vorschlag des Nationalen Sicherheitsrats definierte grundlegende Interesse des Landes gefährdet oder gefährden könnte, zu ermitteln, zu analysieren und zu verarbeiten,

[...]

3/1. Nachrichten in Bezug auf die Aktivitäten der ausländischen Nachrichtendienste auf belgischem Staatsgebiet zu ermitteln, zu analysieren und zu verarbeiten,

[...] ».

Artikel 11 § 1 des Gesetzes vom 30. November 1998 bestimmt:

« Der Allgemeine Nachrichten- und Sicherheitsdienst ist beauftragt:

1. Nachrichten in Bezug auf Faktoren, die die nationale und internationale Sicherheit beeinflussen oder beeinflussen können, sofern die Streitkräfte darin verwickelt sind oder sein könnten, indem sie ihre laufenden oder eventuellen zukünftigen Einsätze mit Informationen unterstützen, sowie Nachrichten in Bezug auf jegliche Aktivität, die Folgendes gefährdet oder gefährden könnte, zu ermitteln, zu analysieren und zu verarbeiten:

a) die Integrität des Staatsgebiets oder die Bevölkerung,

b) die militärischen Verteidigungspläne,

c) das wissenschaftliche und wirtschaftliche Potential in Zusammenhang mit den Akteuren, sowohl natürlichen als auch juristischen Personen, die in den mit der Verteidigung verbundenen wirtschaftlichen und industriellen Sektoren tätig sind und die in einer auf Vorschlag des Ministers der Justiz und des Ministers der Landesverteidigung vom Nationalen Sicherheitsrat gebilligten Liste aufgeführt sind,

d) die Erfüllung der Aufträge der Streitkräfte,

e) die Sicherheit von belgischen Staatsangehörigen im Ausland,

f) jedes andere vom König auf Vorschlag des Nationalen Sicherheitsrats definierte grundlegende Interesse des Landes

und die zuständigen Minister unverzüglich davon in Kenntnis zu setzen sowie der Regierung auf Verlangen Stellungnahmen im Hinblick auf die Bestimmung ihrer internen und auswärtigen Sicherheits- und Verteidigungspolitik abzugeben,

2. für die Gewährleistung der militärischen Sicherheit des Personals, das dem Ministerium der Landesverteidigung untersteht, und von militärischen Anlagen, Waffen und Waffensystemen, Munition, Ausrüstung, Plänen, Schriftstücken, Dokumenten, EDV- und Kommunikationssystemen oder anderen militärischen Gegenstände zu sorgen und im Rahmen der Cyberattacken auf Waffensysteme, militärische EDV- und Kommunikationssysteme oder auf die vom Ministerium der Landesverteidigung verwalteten Systeme die Attacke zu neutralisieren und deren Urheber zu identifizieren, unbeschadet des Rechts, sofort unter Einhaltung der Bestimmungen des Rechts des bewaffneten Konflikts mit einer eigenen Cyberattacke zu reagieren,

3. das Geheimnisse zu wahren, das aufgrund der internationalen Verpflichtungen Belgiens oder zur Wahrung der Integrität des Staatsgebiets und zur Erfüllung der Aufträge der Streitkräfte für militärische Anlagen, Waffen, Munition, Ausrüstung, Pläne, Schriftstücke, Dokumente oder andere militärische Gegenstände, militärische Nachrichten und Kommunikationen sowie militärische EDV- und Kommunikationssysteme oder die vom Ministerium der Landesverteidigung verwalteten Systemen geboten ist,

[...]

5. Nachrichten in Bezug auf die Aktivitäten der ausländischen Nachrichtendienste auf belgischem Staatsgebiet zu ermitteln, zu analysieren und zu verarbeiten ».

B.50.2. In der Begründung ist in Bezug auf diesen Zweck angegeben:

« 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 » (ebenda, SS. 19-20).

B.51.1. Auf die Frage des Verfassungsgerichtshofes zu dem Zweck der Beaufsichtigung von Aktivitäten durch die Nachrichten- und Sicherheitsdienste hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 geantwortet:

« 229. Mit seiner fünften Frage möchte das vorlegende Gericht wissen, ob Art. 6 der PNR-Richtlinie im Licht der Art. 7 und 8 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er nationalen Rechtsvorschriften entgegensteht, nach denen die Verarbeitung der PNR-Daten, die im Einklang mit der Richtlinie erhoben wurden, zur Beaufsichtigung von Aktivitäten durch die Nachrichten- und Sicherheitsdienste zulässig ist.

230. Aus dem Vorabentscheidungsersuchen geht hervor, dass diese Frage des vorlegenden Gerichts insbesondere Aktivitäten betrifft, mit denen die Sûreté de l'État (Staatssicherheit, Belgien) und der Service général du renseignement et de la sécurité (Allgemeiner Nachrichten- und Sicherheitsdienst, Belgien) im Rahmen ihrer jeweiligen den Schutz der nationalen Sicherheit betreffenden Aufgaben befasst sind.

231. Insoweit hat der Unionsgesetzgeber, damit die insbesondere in Art. 52 Abs. 1 der Charta genannten Grundsätze der Gesetzmäßigkeit und der Verhältnismäßigkeit gewahrt werden, klare und präzise Regeln für die Ziele der in der PNR-Richtlinie vorgesehenen Maßnahmen aufgestellt, die mit Eingriffen in die durch die Art. 7 und 8 der Charta garantierten Grundrechte verbunden sind.

232. In Art. 1 Abs. 2 der PNR-Richtlinie heißt es nämlich ausdrücklich, dass die nach Maßgabe dieser Richtlinie erhobenen PNR-Daten ' ausschließlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gemäß Artikel 6 Absatz 2 Buchstaben a, b und c [dieser Richtlinie] ' verarbeitet werden dürfen. Die letztgenannte Bestimmung bestätigt den in Art. 1 Abs. 2 aufgestellten Grundsatz, indem sie systematisch auf die Begriffe ' terroristische Straftat ' und ' schwere Kriminalität ' Bezug nimmt.

233. Aus dem Wortlaut dieser Bestimmungen geht somit klar hervor, dass die darin enthaltene Aufzählung der mit der Verarbeitung von PNR-Daten gemäß der PNR-Richtlinie verfolgten Ziele abschließend ist.

234. Diese Auslegung wird insbesondere durch den elften Erwägungsgrund der PNR-Richtlinie bestätigt, wonach die Verarbeitung von PNR-Daten in einem angemessenen Verhältnis zu den mit der Richtlinie verfolgten ' bestimmten Sicherheitsinteressen ' stehen sollte, und durch ihren Art. 7 Abs. 4, wonach die PNR-Daten und die Ergebnisse ihrer Verarbeitung, die aus der PNR-Zentralstelle eingehen, ' ausschließlich zum bestimmten Zweck der Verhütung, Aufdeckung, Ermittlung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität ' weiterverarbeitet werden dürfen.

235. Überdies folgt aus dem abschließenden Charakter der in Art. 1 Abs. 2 der PNR-Richtlinie genannten Ziele, dass die PNR-Daten auch nicht in einer einheitlichen Datenbank gespeichert werden dürfen, die zur Verfolgung sowohl dieser als auch anderer Ziele konsultiert werden kann. Die Speicherung dieser Daten in einer solchen Datenbank brächte nämlich die Gefahr einer Verwendung der Daten zu anderen als den in Art. 1 Abs. 2 genannten Zwecken mit sich.

236. Da im vorliegenden Fall nach den Angaben des vorlegenden Gerichts die im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften als Zweck der Verarbeitung der PNR-Daten die Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste zulassen und damit diesen Zweck in die Verhütung, Aufdeckung, Ermittlung und Verfolgung terroristischer Straftaten und schwerer Kriminalität einbeziehen, missachten diese Rechtsvorschriften möglicherweise den abschließenden Charakter der Aufzählung der mit der Verarbeitung von PNR-Daten nach der PNR-Richtlinie verfolgten Ziele; dies zu prüfen ist Sache des vorlegenden Gerichts.

237. Daher ist auf die fünfte Frage zu antworten, dass Art. 6 der PNR-Richtlinie im Licht der Art. 7 und 8 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er nationalen Rechtsvorschriften entgegensteht, nach denen die Verarbeitung der PNR-Daten, die im Einklang mit dieser Richtlinie erhoben wurden, zu anderen als den in Art. 1 Abs. 2 der Richtlinie ausdrücklich genannten Zwecken zulässig ist ».

B.51.2. Aus dem Vorstehenden ergibt sich, dass der Gerichtshof der Europäischen Union in Anbetracht der abschließenden Beschaffenheit der in Artikel 1 Absatz 2 der PNR-Richtlinie erwähnten Zwecke der Auffassung ist, dass Rechtsvorschriften wie das Gesetz vom 25. Dezember 2016, indem sie als Zweck der Verarbeitung der PNR-Daten auf die Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste abzielen und damit diesen Zweck in die Verhütung, Aufdeckung, Ermittlung und Verfolgung terroristischer Straftaten und schwerer Kriminalität einbeziehen, möglicherweise den abschließenden Charakter der Aufzählung der mit der Verarbeitung von PNR-Daten nach der PNR-Richtlinie verfolgten Ziele missachten; dies zu prüfen ist Sache des Verfassungsgerichtshofes (Randnr. 236).

Der Gerichtshof der Europäischen Union betont ebenfalls, dass « aus dem abschließenden Charakter der in Art. 1 Abs. 2 der PNR-Richtlinie genannten Ziele [folgt], dass die PNR-Daten auch nicht in einer einheitlichen Datenbank gespeichert werden dürfen, die zur Verfolgung sowohl dieser als auch anderer Ziele konsultiert werden kann. Die Speicherung dieser Daten in einer solchen Datenbank brächte nämlich die Gefahr einer Verwendung der Daten zu anderen als den in Art. 1 Abs. 2 genannten Zwecken mit sich » (Randnr. 235).

B.52.1. Wie der Verfassungsgerichtshof in seinem vorerwähnten Entscheid Nr. 135/2019 geurteilt hat, tragen die Aufträge der Nachrichten- und Sicherheitsdienste, auf die in B.50 hingewiesen wurde, tragen die Aufträge der Nachrichten- und Sicherheitsdienste zwar allgemein zur nationalen und internationalen Sicherheit bei, aber die Verarbeitung der PNR-Daten im Rahmen des in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecks erscheint sehr vage und allgemein (B.54.3). Man kann nämlich nicht davon ausgehen, dass die erwähnten Aktivitäten der Nachrichten- und Sicherheitsdienste ausschließlich und immer darauf abzielen, terroristische Straftaten oder schwere Kriminalität zu verhüten. Im Gegensatz zu dem, was der Ministerrat in seinem Ergänzungsschriftsatz vorbringt, kann aufgrund der « hybriden » Beschaffenheit, die terroristische Straftaten und schwere Kriminalität aufweisen, nicht davon ausgegangen werden, dass der Zweck der Beaufsichtigung der in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnten Aktivitäten die Grenzen des « absolut Notwendigen » einhält.

Der Verfassungsgerichtshof stellt daher fest, dass bei der « Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste » kein direkter Zusammenhang zwischen diesem Zweck und der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, die die mit der Verarbeitung von PNR-Daten nach der PNR-Richtlinie verfolgten Ziele sind, hergestellt werden kann.

Außerdem kann bei diesem Zweck nicht davon ausgegangen werden, dass er einen – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Passagieren aufweist, den die Verarbeitungszwecke der PNR-Daten haben müssen, wie der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022, auf das in B.44 hingewiesen wurde, ausgeführt hat.

B.52.2. In Anbetracht der abschließenden Beschaffenheit der in Artikel 1 Absatz 2 der PNR-Richtlinie erwähnten Zwecke ist davon auszugehen, dass der in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnte Zweck die Grenzen des « absolut Notwendigen » überschreitet.

B.53.1. Bezüglich des Zwecks, die Personenkontrollen an den Außengrenzen zu verbessern und insbesondere die illegale Einwanderung zu bekämpfen, der in Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016 erwähnt ist, hat der Verfassungsgerichtshof in seinem Entscheid Nr. 135/2019 geurteilt:

« B.55.1. Schließlich gestattet es Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016, die PNR-Daten unter den in Kapitel 11 (Artikel 28 bis 31) des Gesetzes vom 25. Dezember 2016 erwähnten Bedingungen zu verarbeiten, um die Personenkontrolle an den Außengrenzen zu verbessern und insbesondere um die illegale Einwanderung zu bekämpfen.

B.55.2. In der Begründung ist in Bezug auf diesen Zweck angegeben:

‘ 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 ’ (ebenda, SS. 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 ’ (ebenda, S. 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 ’ (ebenda, S. 33).

Die Gesetzgebungsabteilung des Staatsrates hat ebenfalls Folgendes bemerkt:

‘ 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 ’ (ebenda, S. 97).

B.55.3. Die Verarbeitung der Passagierdaten im Rahmen des in Artikel 8 § 2 erwähnten Zwecks ist in den Artikeln 28 bis 31 des Gesetzes vom 25. Dezember 2016 geregelt.

Nur die in Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 erwähnten Passagierdaten werden an die in Artikel 14 § 1 Nr. 2 Buchstabe *a)* erwähnten Polizeidienste und an das Ausländeramt übermittelt, damit sie ihre gesetzlichen Aufträge ausführen können (Artikel 29). Es sind nur die Passagiere betroffen, die beabsichtigen, über die Außengrenzen Belgiens ins Hoheitsgebiet zu kommen, oder bereits über die Außengrenzen Belgiens ins Hoheitsgebiet gekommen sind (Artikel 29 § 2 Nr. 1) und die Passagiere, die beabsichtigen, das Hoheitsgebiet über die Außengrenzen Belgiens zu verlassen, oder die das Hoheitsgebiet bereits über die Außengrenzen Belgiens verlassen haben (Artikel 29 § 2 Nr. 2) und die Passagiere, die beabsichtigen, sich in einer in Belgien gelegenen internationalen Transitzone aufzuhalten, sich dort aufhalten oder sich dort aufgehalten haben (Artikel 29 § 2 Nr. 3).

Diese Daten werden unmittelbar nach ihrer Speicherung in der Passagierdatenbank an die in Artikel 14 § 1 Nr. 2 Buchstabe *a)* erwähnten Polizeidienste und an das Ausländeramt, wenn es sie für die Ausführung seiner gesetzlichen Aufträge benötigt, übermittelt; diese Daten werden in einer temporären Datei aufbewahrt und innerhalb von vierundzwanzig Stunden nach ihrer Übermittlung vernichtet (Artikel 29 §§ 3 und 4). Das Ausländeramt kann außerdem nach Ablauf dieser Frist eine gebührend mit Gründen versehene Anfrage an die PNR-Zentralstelle richten, um auf diese Daten zuzugreifen (Artikel 29 § 4 Absatz 2). Das Ausländeramt übermittelt dem Ausschuss für den Schutz des Privatlebens, nunmehr die Datenschutzbehörde, monatlich einen Bericht über die Anwendung von Artikel 29 § 4 Absatz 2 (Artikel 29 § 4 Absatz 3).

Ein Protokoll in Bezug auf die technischen Sicherungs-, Zugriffs- und Übermittlungsmodalitäten der Passagierdaten an die mit der Grenzkontrolle beauftragten Polizeidienste und an das Ausländeramt muss in Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens (Datenschutzbehörde) zwischen dem leitenden Beamten der PNR-Zentralstelle einerseits und dem Generalkommissar der föderalen Polizei und dem leitenden Beamten des Ausländeramtes andererseits für ihren jeweiligen Bereich abgeschlossen werden (Artikel 30).

Binnen vierundzwanzig Stunden nach dem Ende der in Artikel 4 Nr. 3 bis 6 erwähnten Beförderung löschen die Beförderungsunternehmen und Reiseunternehmen alle in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, die sie gemäß Artikel 7 übermitteln (Artikel 31 in der durch das Gesetz vom 15. Juli 2018 abgeänderten Fassung).

B.55.4. Aus dem Vorstehenden ergibt sich, dass nur die in Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 erwähnten API-Daten bestimmter Passagierkategorien im Hinblick auf den Zweck im Zusammenhang mit der Bekämpfung der illegalen Einwanderung und der Grenzkontrolle, der in Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016 aufgeführt ist, unter den in Kapitel 11 des Gesetzes vom 25. Dezember 2016 erwähnten Bedingungen verarbeitet werden dürfen.

Wie in den in B.55.2 zitierten Vorarbeiten angegeben ist, erfolgt eine solche Maßnahme im Rahmen der Umsetzung der Richtlinie 2004/82/EG, deren Ziel gemäß ihrem Erwägungsgrund 1 darin besteht, die illegale Einwanderung wirksam zu bekämpfen und die Grenzkontrollen zu verbessern. Insbesondere Kapitel 11 des Gesetzes vom 25. Dezember 2016 übernimmt den angepassten Inhalt des königlichen Erlasses vom 11. Dezember 2006 ‘ über die Verpflichtung von Fluggesellschaften, Angaben über die beförderten Personen zu übermitteln ’, der vor seiner Aufhebung durch den königlichen Erlass vom 18. Juli 2017 die Richtlinie 2004/82/EG in innerstaatliches Recht umsetzte.

B.55.5. Unter Berücksichtigung der verschiedenen in B.55.3 aufgezählten Einschränkungen für die Verarbeitung der Daten im Rahmen des in Artikel 8 § 2 erwähnten Zwecks ist diese Maßnahme ausreichend klar und präzise und auf das absolut Notwendige beschränkt und ist somit nicht unverhältnismäßig ».

B.53.2. In diesem Entscheid hat der Verfassungsgerichtshof geurteilt, dass der in Artikel 8 § 2 des angefochtenen Gesetzes erwähnte Zweck auf das absolut Notwendige beschränkt ist und sich dabei einerseits auf den Umstand, dass die erwähnten Daten auf die API-Daten begrenzt sind, und andererseits auf den Umstand gestützt, dass die Verarbeitung dieser Daten von den verschiedenen Garantien eingegrenzt ist, die in den Artikeln 28 bis 31 des Gesetzes vom 25. Dezember 2016 vorgesehen sind.

Der Verfassungsgerichtshof hat den Gerichtshof der Europäischen Union nicht dazu befragt, ob die PNR-Richtlinie dahin auszulegen ist, dass sie nationalen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das als Verarbeitungszweck der PNR-Daten den Zweck der Verbesserung der Personenkontrollen an den Außengrenzen und insbesondere der Bekämpfung der illegalen Einwanderung zulässt.

Der Verfassungsgerichtshof hat sich somit endgültig zur Vereinbarkeit des in Artikel 8 § 2 des angefochtenen Gesetzes erwähnten Zwecks mit den im ersten Klagegrund erwähnten Bestimmungen geäußert.

Die gegen die Artikel 28 bis 31 in Verbindung mit Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016 gerichteten Beschwerdegründe werden im Rahmen des zweiten Klagegrunds geprüft.

B.54.1. Auf die Frage des Verfassungsgerichtshofes zur Auslegung der API-Richtlinie (neunte Frage Buchstabe *b)* hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 geurteilt:

« 287. Im Übrigen werden nach den Angaben im Vorabentscheidungsersuchen mit den im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften die PNR-Richtlinie, die API-Richtlinie und teilweise die Richtlinie 2010/65 in einem Rechtsakt umgesetzt. Dabei sehen sie die Anwendung des in der PNR-Richtlinie vorgesehenen Systems auf alle EU-Flüge sowie auf alle Beförderungen auf dem Schienen-, Land- oder Wasserweg innerhalb der Union nach, von und durch Belgien vor, sie gelten auch für Reiseunternehmen und verfolgen weitere Ziele neben der bloßen Bekämpfung terroristischer Straftaten und schwerer Kriminalität. Nach diesen Angaben werden offenbar alle Daten, die im Rahmen des durch diese nationalen Rechtsvorschriften geschaffenen Systems erhoben wurden, von der PNR-Zentralstelle in einer einzigen Datenbank gespeichert, die die PNR-Daten, einschließlich der in Art. 3 Abs. 2 der API-Richtlinie genannten Daten, für alle Passagiere der von diesen Rechtsvorschriften erfassten Beförderungen enthält.

288. Soweit das vorlegende Gericht in diesem Zusammenhang in Buchst. b seiner neunten Frage auf das mit der API-Richtlinie verfolgte Ziel der Verbesserung der Grenzkontrollen und der Bekämpfung illegaler Einwanderung Bezug genommen hat, ist darauf hinzuweisen, dass die Aufzählung der mit der Verarbeitung von PNR-Daten gemäß der PNR-Richtlinie verfolgten Ziele abschließend ist (siehe oben, Rn. 233, 234 und 237), so dass nationale Rechtsvorschriften, die es gestatten, gemäß dieser Richtlinie erhobene PNR-Daten zu anderen als den von ihr vorgesehenen Zwecken, insbesondere zur Verbesserung der Grenzkontrollen und zur Bekämpfung illegaler Einwanderung zu verarbeiten, im Licht der Charta gegen Art. 6 der Richtlinie verstoßen.

289. Außerdem dürfen die Mitgliedstaaten keine einheitliche Datenbank errichten, die sowohl die gemäß der PNR-Richtlinie erhobenen PNR-Daten für Drittstaatsflüge und für EU-Flüge enthält als auch die Daten der Nutzer anderer Beförderungsmittel sowie die in Art. 3 Abs. 2 der API-Richtlinie genannten Daten, insbesondere wenn diese Datenbank nicht nur zur Verfolgung der in Art. 1 Abs. 2 der PNR-Richtlinie genannten Zwecke konsultiert werden kann, sondern auch zur Verfolgung anderer Zwecke (siehe oben, Rn. 235).

290. Schließlich können, wie der Generalanwalt in Nr. 281 seiner Schlussanträge ausgeführt hat, die Art. 28 bis 31 des Gesetzes vom 25. Dezember 2016 jedenfalls nur dann mit dem Unionsrecht, insbesondere mit Art. 67 Abs. 2 AEUV, vereinbar sein, wenn sie dahin ausgelegt und angewandt werden, dass sie nur die Übermittlung und Verarbeitung der API-Daten beförderter Personen betreffen, die die Außengrenzen Belgiens zu Drittstaaten überschreiten. Eine Maßnahme, mit der ein Mitgliedstaat die Bestimmungen der API-Richtlinie, insbesondere die in ihrem Art. 3 Abs. 1 vorgesehene Pflicht zur Übermittlung der Angaben über die beförderten Personen, zum Zweck der Verbesserung der Grenzkontrollen und der Bekämpfung illegaler Einwanderung auf EU-Flüge oder gar auf andere Arten der Personenbeförderung innerhalb der Union aus dem, in den oder durch den Mitgliedstaat ausdehnen würde, liefe nämlich darauf hinaus, es den zuständigen Behörden zu gestatten, sich bei der Überschreitung der Binnengrenzen des betreffenden Mitgliedstaats systematisch zu vergewissern, dass diese Personen in sein Hoheitsgebiet einreisen oder es verlassen dürfen, und hätte damit die gleiche Wirkung wie Kontrollen an den Außengrenzen zu Drittstaaten.

291. Nach alledem ist auf Buchst. b der neunten Frage zu antworten, dass das Unionsrecht, insbesondere Art. 2 der PNR-Richtlinie, im Licht von Art. 3 Abs. 2 EUV, Art. 67 Abs. 2 AEUV und Art. 45 der Charta wie folgt auszulegen ist:

- Es steht nationalen Rechtsvorschriften entgegen, die, ohne dass der betreffende Mitgliedstaat mit einer realen und aktuellen oder vorhersehbaren terroristischen Bedrohung konfrontiert ist, ein System vorsehen, wonach die PNR-Daten aller EU-Flüge und aller Beförderungen mit anderen Mitteln innerhalb der Union aus diesem, in diesen oder durch diesen Mitgliedstaat zur Bekämpfung terroristischer Straftaten und schwerer Kriminalität von den Beförderungsunternehmen und den Reiseunternehmen übermittelt sowie von den zuständigen Behörden verarbeitet werden. In einer solchen Situation muss die Anwendung des durch die PNR-Richtlinie geschaffenen Systems auf die Übermittlung und Verarbeitung der PNR-Daten von Flügen und/oder Beförderungen beschränkt werden, die insbesondere bestimmte Verbindungen, bestimmte Reisemuster oder bestimmte Flughäfen, Bahnhöfe oder Seehäfen betreffen, für die es Anhaltspunkte gibt, die seine Anwendung rechtfertigen können. Es ist Sache des betreffenden Mitgliedstaats, die EU-Flüge und/oder die Beförderungen mit anderen Mitteln innerhalb der Union, für die es solche Anhaltspunkte gibt, auszuwählen und sie nach Maßgabe der Entwicklung der Bedingungen, die ihre Auswahl gerechtfertigt haben, regelmäßig zu überprüfen, um sicherzustellen, dass sich die Anwendung dieses Systems auf solche EU-Flüge und/oder Beförderungen stets auf das absolut Notwendige beschränkt.

- Es steht nationalen Rechtsvorschriften entgegen, die zum Zweck der Verbesserung der Grenzkontrollen und der Bekämpfung illegaler Einwanderung ein solches System der Übermittlung und Verarbeitung der genannten Daten vorsehen ».

B.54.2. Aus diesem Urteil geht hervor, dass einerseits die Verarbeitung von PNR-Daten zu anderen als den von der PNR-Richtlinie vorgesehenen Zwecken, insbesondere zur Verbesserung der Grenzkontrollen und zur Bekämpfung illegaler Einwanderung, die abschließende Beschaffenheit der Aufzählung der mit der Verarbeitung der PNR-Daten verfolgten Ziele missachtet (Randnr. 288), die die Mitgliedstaaten daran hindert, eine einheitliche Datenbank zu errichten, die sowohl die gemäß der PNR-Richtlinie erhobenen PNR-Daten enthält als auch die in Artikel 3 Absatz 2 der API-Richtlinie genannten Daten, insbesondere wenn diese Datenbank nicht nur zur Verfolgung der in Artikel 1 Absatz 2 der PNR-Richtlinie genannten Zwecke konsultiert werden kann, sondern auch zur Verfolgung anderer Zwecke (Randnr. 289), und dass andererseits die Verarbeitung der API-Daten nur beförderte Personen betreffen darf, die die Außengrenzen der Union zu Drittstaaten überschreiten, da sie ansonsten die gleiche Wirkung wie Kontrollen an den Außengrenzen zu Drittstaaten hätte (Randnr. 290).

B.55.1. Im Unterschied zu dem, was der Verfassungsgerichtshof in seinem Entscheid Nr. 135/2019 geurteilt hat, scheint das Urteil des Gerichtshofs der Europäischen Union zu beinhalten, dass der Zweck der Verbesserung der Grenzkontrollen und der Bekämpfung illegaler Einwanderung für die Verarbeitung von PNR-Daten nicht verfolgt werden darf, auch wenn diese Daten auf die API-Daten beschränkt sind und auch wenn die Verarbeitung dieser Daten durch die Garantien eingegrenzt ist, die in den Artikeln 28 bis 31 des Gesetzes vom 25. Dezember 2016 vorgesehen sind, wenn diese Daten in einer einheitlichen Datenbank gemäß der PNR-Richtlinie erhoben werden und beförderte Personen betreffen, die nicht die Außengrenzen der Union überschreiten.

B.55.2. Der Entscheid Nr. 135/2019 des Verfassungsgerichtshofes ist aber in diesem Punkt endgültig und kann nicht mehr angefochten werden (Artikel 116 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof). Mit diesem Entscheid hat der Gerichtshof seine Gerichtsbarkeit erschöpft, was den erwähnten Punkt betrifft. Der Gerichtshof kann seine endgültigen Entscheidungen nicht rückgängig machen, weil dies « durch keinen Umstand zu rechtfertigen ist » (siehe u.a. Entscheid Nr. 172/2008 vom 3. Dezember 2008, ECLI:BE:GHCC:2008:ARR.172, B.15). Das ist nämlich « eine[r] der wesentlichen Grundsätze des Rechtsstaates » (Entscheid Nr. 199/2009 vom 17. Dezember 2009, ECLI:BE:GHCC:2009:ARR.199, B.8). Das Unionsrecht verlangt es auch nicht, eine endgültige gerichtliche Entscheidung rückgängig zu machen, selbst wenn dies es ermöglichen würde, einem Verstoß gegen eine Bestimmung des Unionsrechts abzuhelfen (EuGH, Große Kammer, 6. Oktober 2015, C-69/14, *Târşia*, ECLI:EU:C:2015:662, Randnrn. 28-29; 4. März 2020, C-34/19, *Telecom Italia*, ECLI:EU:C:2020:148, Randnr. 69). Der Verfassungsgerichtshof könnte diese rechtliche Frage nicht in einem anderen Sinne entscheiden, ohne erneut befasst zu werden. Es ist folglich Sache des Gesetzgebers, das angefochtene Gesetz mit dem Urteil des Gerichtshofs der Europäischen Union in dem strittigen Punkt zu harmonisieren.

B.56. Unter dem Vorbehalt der Auslegung in B.49 ist der Klagegrund unbegründet, insofern er gegen Artikel 8 § 1 Nr. 3 und § 2 des Gesetzes vom 25. Dezember 2016 gerichtet ist.

Insofern er gegen Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 gerichtet ist, ist der Klagegrund begründet. Folglich ist Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 für nichtig zu erklären.

4. *Die Verwaltung der Passagierdatenbank und die Verarbeitung der Daten im Rahmen der Vorabüberprüfung und der gezielten Recherchen (Artikel* 12 *bis* 16 *und* 24 *bis* 27 *und Artikel* 50 *und* 51*)*

B.57. Die klagende Partei ist der Auffassung, dass die verschiedenen Verarbeitungen und Übermittlungen von personenbezogenen Daten offenkundig unverhältnismäßig seien.

Sie bemängelt einerseits die Schaffung der Passagierdatenbank, die von der innerhalb des FÖD Inneres geschaffenen PNR-Zentralstelle verwaltet werde und die Informationen mit den ausländischen PNR-Zentralstellen und Europol austausche. Sie vertritt die Ansicht, dass die Verarbeitung der Passagierdaten nicht die Schaffung einer Datenbank erfordere.

Andererseits bemängelt sie die Korrelation zwischen den Datenbanken und dem « *Pre-Screening* », das anhand von im Voraus festgelegten Kriterien, die als Indikator für eine Bedrohung dienten, durchgeführt werden müsste.

Schließlich bemängelt sie den Umstand, dass die entsandten Mitglieder der zuständigen Dienste über eine Anfrage auf individuellen Zugriff im Rahmen gezielter Recherchen befinden können.

B.58.1. Nach Artikel 4 Absatz 1 der PNR-Richtlinie errichtet oder benennt jeder Mitgliedstaat eine für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständige Behörde oder eine Abteilung einer solchen Behörde, die als seine PNR-Zentralstelle handelt.

Gemäß Artikel 4 Absatz 2 der PNR-Richtlinie ist die PNR-Zentralstelle verantwortlich für:

« *a)* die Erhebung der PNR-Daten bei Fluggesellschaften, für die Speicherung und Verarbeitung dieser Daten sowie die Übermittlung dieser Daten oder der Ergebnisse ihrer Verarbeitung an die zuständigen Behörden nach Artikel 7;

b) den Austausch sowohl von PNR-Daten als auch der Ergebnisse der Verarbeitung dieser Daten mit den PNR-Zentralstellen anderer Mitgliedstaaten und mit Europol gemäß den Artikeln 9 und 10 ».

B.58.2. In Bezug auf die Datenverarbeitung bestimmt Artikel 6 der PNR-Richtlinie:

« 1. Die von den Fluggesellschaften übermittelten PNR-Daten werden von der PNR-Zentralstelle des betreffenden Mitgliedstaats gemäß Artikel 8 erhoben. Wenn die von Fluggesellschaften übermittelten PNR-Daten andere als die in Anhang I genannten Daten beinhalten, werden diese Daten von der PNR-Zentralstelle unmittelbar nach ihrem Eingang dauerhaft gelöscht.

2. Die PNR-Zentralstelle verarbeitet PNR-Daten ausschließlich zu folgenden Zwecken:

a) Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat, um diejenigen Personen zu ermitteln, die von den zuständigen Behörden gemäß Artikel 7 und gegebenenfalls — im Einklang mit Artikel 10 — von Europol genauer überprüft werden müssen, da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind;

b) im Einzelfall Beantwortung von auf einer hinreichenden Grundlage gebührend begründeten Anfragen zuständiger Behörden hinsichtlich der Zurverfügungstellung und Verarbeitung von PNR-Daten in besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität, und der Zurverfügungstellung der Ergebnisse dieser Verarbeitung an die zuständigen Behörden oder gegebenenfalls an Europol, und

c) Analyse von PNR-Daten zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien zur Verwendung in gemäß Absatz 3 Buchstabe b durchgeführten Überprüfungen, die der Ermittlung von Personen gelten, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind.

3. Bei der Durchführung der in Absatz 2 Buchstabe a genannten Überprüfungen darf die PNR-Zentralstelle

a) die PNR-Daten mit Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, einschließlich Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und Unionsvorschriften abgleichen; oder

b) die PNR-Daten anhand im Voraus festgelegter Kriterien abgleichen.

4. Die Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat anhand im Voraus festgelegter Kriterien gemäß Absatz 3 Buchstabe b erfolgt in nichtdiskriminierender Weise. Diese im Voraus festgelegten Kriterien müssen zielgerichtet, verhältnismäßig und bestimmt sein. Die Mitgliedstaaten stellen sicher, dass diese Kriterien von der PNR-Zentralstelle aufgestellt und von ihr in Zusammenarbeit mit den in Artikel 7 genannten zuständigen Behörden regelmäßig überprüft werden. Die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person dürfen unter keinen Umständen als Grundlage für diese Kriterien dienen.

5. Die Mitgliedstaaten stellen sicher, dass jeder einzelne Treffer bei der automatisierten Verarbeitung von PNR-Daten nach Maßgabe von Absatz 2 Buchstabe a auf andere, nicht-automatisierte Art individuell überprüft wird, um zu klären, ob die zuständige Behörde gemäß Artikel 7 Maßnahmen im Einklang mit dem nationalen Recht ergreifen muss.

6. Die PNR-Zentralstelle eines Mitgliedstaats übermittelt die PNR-Daten von nach Absatz 2 Buchstabe a ermittelten Personen oder die Ergebnisse der Verarbeitung dieser Daten zur weiteren Überprüfung an die zuständigen Behörden gemäß Artikel 7 desselben Mitgliedstaats. Derartige Übermittlungen dürfen nur im Einzelfall erfolgen und im Fall einer automatisierten Verarbeitung der PNR-Daten nur nach einer individuellen Überprüfung auf andere, nicht-automatisierte Art.

7. Die Mitgliedstaaten stellen sicher, dass der Datenschutzbeauftragte Zugang zu sämtlichen von der PNR-Zentralstelle verarbeiteten Daten erhält. Wenn der Datenschutzbeauftragte der Auffassung ist, dass eine Verarbeitung von Daten nicht rechtmäßig war, kann er die Angelegenheit an die nationale Kontrollstelle verweisen.

8. Die Speicherung, Verarbeitung und Auswertung von PNR-Daten durch die PNR-Zentralstelle erfolgt ausschließlich an einem gesicherten Ort bzw. gesicherten Orten im Hoheitsgebiet der Mitgliedstaaten.

9. Das Recht zur Einreise von Personen, die im Hoheitsgebiet des betreffenden Mitgliedstaats gemäß der Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates das Unionsrecht auf freien Personenverkehr genießen, darf von den Auswirkungen der Überprüfungen von Fluggästen gemäß Absatz 2 Buchstabe a dieses Artikels nicht beeinträchtigt werden. Darüber hinaus müssen, wenn Überprüfungen in Bezug auf EU-Flüge zwischen Mitgliedstaaten vorgenommen werden, für die die Verordnung (EG) Nr. 562/2006 des Europäischen Parlaments und des Rates gilt, die Auswirkungen solcher Überprüfungen mit der genannten Verordnung im Einklang stehen ».

B.59.1. Auf die Frage des Verfassungsgerichtshofes zur Gültigkeit der PNR-Richtlinie hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 mehrere Klarstellungen zur Vorabüberprüfung der « PNR »-Daten mittels automatisierter Verarbeitungen vorgenommen (Randnrn. 176 bis 213) - unter Berücksichtigung (i) des Datenbankabgleichs der PNR-Daten (ii) der Verarbeitung der PNR-Daten anhand im Voraus festgelegter Kriterien und (iii) der Garantien im Zusammenhang mit der automatisierten Verarbeitung von PNR-Daten - und zur nachträglichen Zurverfügungstellung und Überprüfung der PNR-Daten (Randnrn. 214-227):

« 5*) Zur Vorabüberprüfung der PNR-Daten mittels automatisierter Verarbeitungen*

176. Nach Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie sollen durch die dort vorgesehene Vorabüberprüfung diejenigen Personen ermittelt werden, die u. a. von den zuständigen Behörden gemäß Art. 7 der Richtlinie genauer überprüft werden müssen, da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind.

177. Diese Vorabüberprüfung vollzieht sich in zwei Schritten. Zunächst nimmt die PNR-Zentralstelle des betreffenden Mitgliedstaats automatisierte Verarbeitungen der PNR-Daten in Form eines Abgleichs mit Datenbanken oder anhand im Voraus festgelegter Kriterien vor (Art. 6 Abs. 3 der PNR-Richtlinie). Falls diese automatisierten Verarbeitungen zu einem Treffer (‘ hit ’) führen, nimmt die Zentralstelle sodann die in Art. 6 Abs. 5 der Richtlinie vorgeschriebene individuelle Überprüfung auf andere, nicht automatisierte Art vor, um zu klären, ob die in der Richtlinie genannten zuständigen Behörden gemäß Art. 7 Maßnahmen im Einklang mit dem nationalen Recht ergreifen müssen (‘ match ’).

178. Wie oben in Rn. 106 ausgeführt, weisen automatisierte Verarbeitungen zwangsläufig eine erhebliche Fehlerquote auf, da sie anhand von nicht überprüften personenbezogenen Daten durchgeführt werden und auf im Voraus festgelegten Kriterien beruhen.

179. Unter diesen Umständen – und in Anbetracht der im vierten Erwägungsgrund der Präambel der Charta hervorgehobenen Notwendigkeit, den Schutz der Grundrechte insbesondere angesichts der wissenschaftlichen und technologischen Entwicklungen zu stärken – ist sicherzustellen, dass die zuständigen Behörden Entscheidungen, aus denen sich eine nachteilige Rechtsfolge oder ein sonstiger schwerwiegender Nachteil für die betroffene Person ergibt, unter keinen Umständen allein auf der Grundlage der automatisierten Verarbeitung der PNR-Daten treffen (20. Erwägungsgrund und Art. 7 Abs. 6 der PNR-Richtlinie). Zudem darf die PNR-Zentralstelle selbst die PNR-Daten erst nach einer individuellen Überprüfung auf andere, nicht automatisierte Art an die zuständigen Behörden übermitteln (Art. 6 Abs. 6 der Richtlinie). Neben diesen von der PNR-Zentralstelle und den zuständigen Behörden selbst vorzunehmenden Prüfungen muss die Rechtmäßigkeit sämtlicher automatisierter Verarbeitungen schließlich vom Datenschutzbeauftragten und von der nationalen Kontrollstelle (Art. 6 Abs. 7 und Art. 15 Abs. 3 Buchst. b der Richtlinie) sowie von den nationalen Gerichten im Rahmen eines gerichtlichen Rechtsbehelfs (Art. 13 Abs. 1 der Richtlinie) überprüft werden können.

180. Wie der Generalanwalt in Nr. 207 seiner Schlussanträge im Wesentlichen ausgeführt hat, müssen die nationale Kontrollstelle, der Datenschutzbeauftragte und die PNR-Zentralstelle mit den nötigen materiellen und personellen Mitteln für die Ausübung der ihnen nach der PNR-Richtlinie obliegenden Kontrolle ausgestattet werden. Außerdem müssen in der nationalen Regelung, mit der diese Richtlinie in innerstaatliches Recht umgesetzt wird und die darin vorgesehenen automatisierten Verarbeitungen gebilligt werden, klare und präzise Vorschriften für die Bestimmung der Datenbanken sowie der herangezogenen Analysekriterien aufgestellt werden; auf andere Methoden, die in Art. 6 Abs. 2 der Richtlinie nicht ausdrücklich vorgesehen sind, darf für die Zwecke der Vorabüberprüfung nicht zurückgegriffen werden.

181. Im Übrigen folgt aus Art. 6 Abs. 9 der PNR-Richtlinie, dass die Auswirkungen der Vorabüberprüfung gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie nicht das Einreiserecht von Personen, die im Hoheitsgebiet des betreffenden Mitgliedstaats gemäß der Richtlinie 2004/38 das Recht auf Freizügigkeit genießen, beeinträchtigen dürfen und mit der Verordnung Nr. 562/2006 im Einklang stehen müssen. Das durch die PNR-Richtlinie geschaffene System erlaubt es den zuständigen Behörden somit nicht, dieses Recht über das in der Richtlinie 2004/38 und der Verordnung Nr. 562/2006 vorgesehene Maß hinaus zu beschränken.

i) Zum Datenbankabgleich der PNR-Daten

182. Nach Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie ‘ darf ’ die PNR-Zentralstelle bei der Durchführung der in Art. 6 Abs. 2 Buchst. a genannten Überprüfungen die PNR-Daten mit Datenbanken abgleichen, die zum Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität ‘ maßgeblich ’ sind, ‘ einschließlich Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und Unionsvorschriften ’.

183. Zwar ergibt sich bereits aus dem Wortlaut von Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie, insbesondere aus dem Wort ‘ einschließlich ’, dass die Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, zu den ‘ maßgeblichen ’ Datenbanken im Sinne dieser Bestimmung gehören. Indes geht aus ihr nicht hervor, welche anderen Datenbanken angesichts der mit dieser Richtlinie verfolgten Ziele ebenfalls als ‘ maßgeblich ’ angesehen werden könnten. Wie der Generalanwalt in Nr. 217 seiner Schlussanträge ausgeführt hat, gibt es in der genannten Bestimmung nämlich keine ausdrücklichen Angaben zur Art der Daten, die solche Datenbanken enthalten können, und zu ihrem Verhältnis zu den mit der Richtlinie verfolgten Zielen; aus ihr geht auch nicht hervor, ob die PNR-Daten ausschließlich mit behördlich verwalteten Datenbanken abzugleichen sind oder ob sie auch mit Datenbanken abgeglichen werden können, die von Privatpersonen verwaltet werden.

184. Unter diesen Umständen könnte Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie auf den ersten Blick dahin ausgelegt werden, dass die PNR-Daten als bloße Suchkriterien für die Durchführung von Analysen anhand verschiedener Datenbanken verwendet werden können, einschließlich solcher, die von den Sicherheits- und Nachrichtendiensten der Mitgliedstaaten in Verfolgung anderer Ziele als der der Richtlinie verwaltet und betrieben werden, und dass solche Analysen die Form einer Datenexploration (data mining) annehmen können. Bestünde die Möglichkeit, solche Analysen durchzuführen und die PNR-Daten mit solchen Datenbanken abzugleichen, könnte aber bei den Fluggästen der Eindruck entstehen, dass ihr Privatleben einer Art der Überwachung unterliegt. Auch wenn die in dieser Bestimmung vorgesehene Vorabüberprüfung von einer relativ begrenzten Gesamtheit von Daten - den PNR-Daten - ausgeht, kann einer solchen Auslegung von Art. 6 Abs. 3 Buchst. a daher nicht gefolgt werden, da sie zu einer unverhältnismäßigen Nutzung dieser Daten führen könnte, die es ermöglichen würde, ein genaues Profil der betreffenden Personen zu erstellen, nur weil sie eine Flugreise unternehmen wollen.

185. Daher ist Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie im Einklang mit der oben in den Rn. 86 und 87 angeführten Rechtsprechung so auszulegen, dass die uneingeschränkte Achtung der in den Art. 7 und 8 der Charta verankerten Grundrechte gewährleistet ist.

186. Insoweit ergibt sich aus den Erwägungsgründen 7 und 15 der PNR-Richtlinie, dass die in ihrem Art. 6 Abs. 3 Buchst. a vorgesehene automatisierte Verarbeitung auf das zur Bekämpfung terroristischer Straftaten und schwerer Kriminalität absolut Notwendige beschränkt werden und zugleich ein hohes Niveau des Schutzes dieser Grundrechte gewährleisten muss.

187. Außerdem gestattet es, wie die Kommission in Beantwortung einer Frage des Gerichtshofs im Wesentlichen ausgeführt hat, der Wortlaut dieser Bestimmung, wonach die PNR-Zentralstelle die PNR-Daten mit den dort genannten Datenbanken abgleichen ‘ darf ’, dieser Stelle, nach Maßgabe der konkreten Situation eine auf das absolut Notwendige beschränkte Modalität der Verarbeitung zu wählen. In Anbetracht der zur Gewährleistung des Schutzes der in den Art. 7 und 8 der Charta verankerten Grundrechte erforderlichen Beachtung der Anforderungen an Klarheit und Genauigkeit ist die PNR-Zentralstelle verpflichtet, die in Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie vorgesehene automatisierte Verarbeitung allein auf die Datenbanken zu beschränken, die sich anhand dieser Bestimmung ermitteln lassen. Insoweit ist zwar die darin enthaltene Bezugnahme auf ‘ maßgebliche ’ Datenbanken keiner die erfassten Datenbanken hinreichend klar und genau präzisierenden Auslegung zugänglich. Anders verhält es sich aber bei der Bezugnahme auf ‘ Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und Unionsvorschriften ’.

188. Daher ist, wie der Generalanwalt im Wesentlichen in Nr. 219 seiner Schlussanträge ausgeführt hat, Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie im Licht dieser Grundrechte dahin auszulegen, dass die PNR-Zentralstelle die PNR-Daten allein mit den letztgenannten Datenbanken abgleichen darf.

189. Zu den Anforderungen, denen diese Datenbanken genügen müssen, ist festzustellen, dass nach Art. 6 Abs. 4 der PNR-Richtlinie die Vorabüberprüfung anhand im Voraus festgelegter Kriterien gemäß Art. 6 Abs. 3 Buchst. b der Richtlinie in nicht diskriminierender Weise erfolgen muss, dass diese Kriterien zielgerichtet, verhältnismäßig und bestimmt sein müssen und dass sie von den PNR-Zentralstellen aufgestellt und von ihnen in Zusammenarbeit mit den in Art. 7 der Richtlinie genannten zuständigen Behörden regelmäßig überprüft werden müssen. Zwar bezieht sich Art. 6 Abs. 4 der Richtlinie - aufgrund des Verweises auf Art. 6 Abs. 3 Buchst. b - nur auf die Verarbeitung von PNR-Daten anhand im Voraus festgelegter Kriterien, doch er ist im Licht der Art. 7, 8 und 21 der Charta dahin auszulegen, dass die Anforderungen, die er aufstellt, *mutatis mutandis* für den Abgleich dieser Daten mit den in der vorstehenden Randnummer genannten Datenbanken gelten müssen, zumal diese Anforderungen im Wesentlichen denen entsprechen, die in der aus dem Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017 (EU:C:2017:592, Rn. 172) hervorgegangenen Rechtsprechung für den Abgleich von PNR-Daten mit Datenbanken herangezogen wurden.

190. Insoweit ist klarzustellen, dass das Erfordernis des nicht diskriminierenden Charakters der genannten Datenbanken u. a. voraussetzt, dass die Eintragung in Datenbanken betreffend Personen, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, auf objektiven und nicht diskriminierenden Kriterien beruht, die durch die für solche Datenbanken geltenden nationalen, internationalen und unionsrechtlichen Vorschriften festgelegt werden (vgl. entsprechend Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 78).

191. Um dem Erfordernis zu genügen, dass die im Voraus festgelegten Kriterien zielgerichtet, verhältnismäßig und bestimmt sind, müssen die oben in Rn. 188 genannten Datenbanken außerdem im Zusammenhang mit der Bekämpfung terroristischer Straftaten und schwerer Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Fluggästen betrieben werden.

192. Überdies müssen die gemäß Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie genutzten Datenbanken in Anbetracht der oben in den Rn. 183 und 184 angestellten Erwägungen von den in Art. 7 der Richtlinie genannten zuständigen Behörden verwaltet werden oder, soweit es sich um Unionsdatenbanken und um internationale Datenbanken handelt, von diesen Behörden im Rahmen ihrer Aufgabe der Bekämpfung terroristischer Straftaten und schwerer Kriminalität betrieben werden. Dies ist bei Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, gemäß den für solche Datenbanken geltenden nationalen, internationalen und unionsrechtlichen Vorschriften der Fall.

ii) Zur Verarbeitung der PNR-Daten anhand im Voraus festgelegter Kriterien

193. Nach Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie darf die PNR-Zentralstelle die PNR-Daten auch anhand im Voraus festgelegter Kriterien abgleichen. Aus Art. 6 Abs. 2 Buchst. a dieser Richtlinie geht hervor, dass die Vorabüberprüfung und damit die Verarbeitung der PNR-Daten anhand im Voraus festgelegter Kriterien im Wesentlichen zur Ermittlung von Personen dient, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind.

194. Zu den Kriterien, die die PNR-Zentralstelle dabei heranziehen kann, ist zunächst festzustellen, dass sie nach dem Wortlaut von Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie ‘ im Voraus festgelegt ’ worden sein müssen. Wie der Generalanwalt in Nr. 228 seiner Schlussanträge ausgeführt hat, steht dieses Erfordernis der Heranziehung von Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme (‘ machine learning ’) entgegen, die - ohne menschliche Einwirkung und Kontrolle - den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können.

195. Darüber hinaus brächte der Rückgriff auf solche Technologien die Gefahr mit sich, dass der nach den Bestimmungen der PNR-Richtlinie erforderlichen individuellen Überprüfung der Treffer und der Rechtmäßigkeitsprüfung die praktische Wirksamkeit genommen wird. Wie der Generalanwalt in Nr. 228 seiner Schlussanträge im Wesentlichen ausgeführt hat, kann es sich nämlich angesichts der für die Funktionsweise von Technologien der künstlichen Intelligenz kennzeichnenden mangelnden Nachvollziehbarkeit als unmöglich erweisen, den Grund zu erkennen, aus dem ein bestimmtes Programm einen Treffer erzielt hat. Unter diesen Umständen könnte die Nutzung solcher Technologien den Betroffenen auch ihr in Art. 47 der Charta verankertes Recht auf einen wirksamen gerichtlichen Rechtsbehelf nehmen, das nach dem 28. Erwägungsgrund der PNR-Richtlinie auf hohem Schutzniveau gewährleistet werden soll, damit insbesondere gerügt werden kann, dass die erzielten Ergebnisse nicht frei von Diskriminierung seien.

196. Was sodann die aus Art. 6 Abs. 4 der PNR-Richtlinie resultierenden Anforderungen betrifft, heißt es dort in Satz 1, dass die Vorabüberprüfung anhand im Voraus festgelegter Kriterien in nicht diskriminierender Weise erfolgt, und in Satz 4 wird hinzugefügt, dass die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person unter keinen Umständen als Grundlage für diese Kriterien dienen dürfen.

197. Die Mitgliedstaaten dürfen daher Kriterien, die auf den in der vorstehenden Randnummer genannten Merkmalen beruhen und deren Verwendung zu Diskriminierungen führen kann, nicht als im Voraus festgelegte Kriterien heranziehen. Insoweit ergibt sich aus dem Wortlaut von Art. 6 Abs. 4 Satz 4 der PNR-Richtlinie, wonach die im Voraus festgelegten Kriterien ‘ unter keinen Umständen ’ auf diesen Merkmalen beruhen dürfen, dass die Bestimmung sowohl unmittelbare als auch mittelbare Diskriminierungen erfasst. Diese Auslegung wird im Übrigen durch Art. 21 Abs. 1 der Charta bestätigt, in dessen Licht die genannte Bestimmung auszulegen ist und der Diskriminierungen aufgrund dieser Merkmale generell verbietet. Unter diesen Umständen sind die im Voraus festgelegten Kriterien so zu bestimmen, dass ihre Anwendung, auch wenn sie neutral formuliert sind, nicht geeignet ist, Personen mit den geschützten Merkmalen besonders zu benachteiligen.

198. Aus dem in Art. 6 Abs. 4 Satz 2 der PNR-Richtlinie aufgestellten Erfordernis, wonach die im Voraus festgelegten Kriterien zielgerichtet, verhältnismäßig und bestimmt sein müssen, ist abzuleiten, dass die bei der Vorabüberprüfung herangezogenen Kriterien so festzulegen sind, dass sie speziell auf Personen abzielen, bei denen der begründete Verdacht einer Beteiligung an terroristischen Straftaten oder schwerer Kriminalität im Sinne dieser Richtlinie bestehen könnte. Diese Auslegung wird durch den Wortlaut von Art. 6 Abs. 2 Buchst. a der Richtlinie bestätigt, der darauf abstellt, dass die betreffenden Personen ‘ möglicherweise ’ ‘ an einer ’ terroristischen Straftat oder ‘ an ’ schwerer Kriminalität beteiligt sind. Desgleichen wird im siebten Erwägungsgrund der Richtlinie ausgeführt, dass die Aufstellung und die Anwendung von Prüfkriterien auf terroristische Straftaten und schwere Kriminalität beschränkt werden sollten, ‘ für die die Anwendung solcher Kriterien maßgeblich ist ’.

199. Um die genannten Personen in dieser Weise zu erfassen, können sich die PNR-Zentralstelle und die zuständigen Behörden - angesichts der mit Kriterien, die auf den in Art. 6 Abs. 4 Satz 4 der PNR-Richtlinie genannten Merkmalen beruhen, verbundenen Gefahr einer Diskriminierung - grundsätzlich nicht auf diese Merkmale stützen. Dagegen können sie, wie die deutsche Regierung in der mündlichen Verhandlung ausgeführt hat, u. a. den Besonderheiten des tatsächlichen Verhaltens von Personen im Zusammenhang mit der Vorbereitung und Durchführung von Flugreisen Rechnung tragen, die nach den von den zuständigen Behörden getroffenen Feststellungen und nach den von ihnen gewonnenen Erfahrungen darauf hindeuten könnten, dass Personen, die sich in dieser Weise verhalten, möglicherweise an terroristischen Straftaten oder an schwerer Kriminalität beteiligt sind.

200. In diesem Kontext sind, wie die Kommission in Beantwortung einer Frage des Gerichtshofs ausgeführt hat, die im Voraus festgelegten Kriterien so zu bestimmen, dass sowohl ‘ belastende ’ als auch ‘ entlastende ’ Gesichtspunkte berücksichtigt werden. Dieses Erfordernis kann zur Zuverlässigkeit der Kriterien beitragen und insbesondere ihre Verhältnismäßigkeit sicherstellen, wie es Art. 6 Abs. 4 Satz 2 der PNR-Richtlinie verlangt.

201. Schließlich müssen nach Art. 6 Abs. 4 Satz 3 der PNR-Richtlinie die im Voraus festgelegten Kriterien regelmäßig überprüft werden. Im Rahmen dieser Überprüfung müssen die Kriterien nach Maßgabe der Entwicklung der Bedingungen, die ihre Heranziehung bei der Vorabüberprüfung gerechtfertigt haben, angepasst werden, damit u. a. auf Entwicklungen bei der Bekämpfung terroristischer Straftaten und schwerer Kriminalität in dem oben in Rn. 157 dargelegten Sinne reagiert werden kann (vgl. entsprechend Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 82). Bei der Überprüfung muss insbesondere die im Rahmen der Anwendung der im Voraus festgelegten Kriterien gewonnene Erfahrung berücksichtigt werden, um die Zahl ‘ falsch positiver ’ Ergebnisse so weit wie möglich zu verringern und dadurch dazu beizutragen, dass die Anwendung dieser Kriterien absolut notwendig ist.

iii) Zu den Garantien im Zusammenhang mit der automatisierten Verarbeitung von PNR-Daten

202. Die Beachtung der in Art. 6 Abs. 4 der PNR-Richtlinie aufgestellten Anforderungen an die automatisierte Verarbeitung von PNR-Daten ist nicht nur im Rahmen der Aufstellung und Überprüfung der Datenbanken sowie der in dieser Bestimmung vorgesehenen im Voraus festgelegten Kriterien geboten, sondern auch, wie der Generalanwalt in Nr. 230 seiner Schlussanträge ausgeführt hat, während des gesamten Prozesses der Verarbeitung dieser Daten.

203. Speziell in Bezug auf die im Voraus festgelegten Kriterien ist zunächst darauf hinzuweisen, dass die PNR-Zentralstelle zwar, wie es im siebten Erwägungsgrund der PNR-Richtlinie heißt, die Prüfkriterien so festlegen muss, dass die Zahl unschuldiger Personen, die fälschlicherweise mit dem durch die Richtlinie geschaffenen System identifiziert werden, auf ein Minimum beschränkt wird. Gemäß Art. 6 Abs. 5 und 6 der Richtlinie muss sie gleichwohl jeden einzelnen Treffer auf nicht automatisierte Art individuell überprüfen, um etwaige ‘ falsch positive ’ Ergebnisse so weit wie möglich zu erkennen. Außerdem muss sie, ungeachtet dessen, dass sie die Prüfkriterien in nicht diskriminierender Weise festzulegen hat, eine solche Überprüfung durchführen, um etwaige diskriminierende Ergebnisse auszuschließen. Die gleiche Prüfpflicht obliegt der PNR-Zentralstelle beim Abgleich der PNR-Daten mit den Datenbanken.

204. Dabei muss die PNR-Zentralstelle von der Übermittlung der Ergebnisse dieser automatisierten Verarbeitungen an die zuständigen Behörden im Sinne von Art. 7 der PNR-Richtlinie absehen, wenn sie in Anbetracht der oben in Rn. 198 angestellten Erwägungen im Anschluss an die Überprüfung nicht über Anhaltspunkte verfügt, aus denen sich in rechtlich hinreichender Weise der begründete Verdacht einer Beteiligung der mittels der automatisierten Verarbeitungen identifizierten Personen an terroristischen Straftaten oder schwerer Kriminalität ergibt oder wenn sie über Anhaltspunkte dafür verfügt, dass die genannten Verarbeitungen zu diskriminierenden Ergebnissen führen.

205. Hinsichtlich der von der PNR-Zentralstelle insoweit vorzunehmenden Überprüfungen ergibt sich aus Art. 6 Abs. 5 und 6 der PNR-Richtlinie in Verbindung mit ihren Erwägungsgründen 20 und 22, dass die Mitgliedstaaten klare und präzise Regeln vorsehen müssen, die Leitlinien und einen Rahmen für die von den Bediensteten, die mit der individuellen Überprüfung betraut sind, vorzunehmende Analyse vorgeben, um für die uneingeschränkte Achtung der in den Art. 7, 8 und 21 der Charta verankerten Grundrechte zu sorgen und insbesondere eine dem Diskriminierungsverbot Rechnung tragende kohärente Verwaltungspraxis innerhalb der PNR-Zentralstelle zu gewährleisten.

206. Angesichts der oben in Rn. 106 erwähnten erheblichen Zahl ‘ falsch positiver ’ Ergebnisse müssen sich die Mitgliedstaaten insbesondere vergewissern, dass die PNR-Zentralstelle in klarer und präziser Weise Kriterien für die objektive Überprüfung aufstellt, die es ihren Bediensteten ermöglichen, zum einen zu prüfen, ob und inwieweit ein Treffer (‘ hit ’) tatsächlich eine Person betrifft, die möglicherweise an terroristischen Straftaten oder an schwerer Kriminalität in dem oben in Rn. 157 dargelegten Sinne beteiligt ist und deshalb einer weiteren Überprüfung durch die zuständigen Behörden gemäß Art. 7 der Richtlinie unterzogen werden muss, und zum anderen, ob die in der Richtlinie vorgesehenen automatisierten Verarbeitungen und namentlich die im Voraus festgelegten Kriterien und die herangezogenen Datenbanken keinen diskriminierenden Charakter haben.

207. In diesem Kontext haben die Mitgliedstaaten dafür zu sorgen, dass die PNR-Zentralstelle im Einklang mit Art. 13 Abs. 5 der PNR-Richtlinie in Verbindung mit ihrem 37. Erwägungsgrund jede Verarbeitung von PNR-Daten, die im Rahmen der Vorabüberprüfung, einschließlich der individuellen Überprüfung auf nicht automatisierte Art, vorgenommen wird, zum Zweck der Überprüfung ihrer Rechtmäßigkeit und zur Selbstkontrolle dokumentiert.

208. Ferner dürfen die zuständigen Behörden Entscheidungen, aus denen sich eine nachteilige Rechtsfolge oder ein sonstiger schwerwiegender Nachteil für die betroffene Person ergibt, unter keinen Umständen allein auf der Grundlage der automatisierten Verarbeitung der PNR-Daten treffen (Art. 7 Abs. 6 Satz 1 der PNR-Richtlinie); dies bedeutet, dass sie im Rahmen der Vorabüberprüfung dem Ergebnis der individuellen Überprüfung auf nicht automatisierte Art durch die PNR-Zentralstelle Rechnung tragen und ihm gegebenenfalls Vorrang vor dem Ergebnis der automatisierten Verarbeitungen einräumen müssen. Nach Art. 7 Abs. 6 Satz 2 dürfen solche Entscheidungen nicht diskriminierend sein.

209. In diesem Rahmen müssen sich die zuständigen Behörden vergewissern, dass sowohl die automatisierten Verarbeitungen als auch die individuelle Überprüfung rechtmäßig sind und namentlich keinen diskriminierenden Charakter haben.

210. Insbesondere müssen sich die zuständigen Behörden vergewissern, dass der Betroffene - ohne es ihm im Verwaltungsverfahren zwangsläufig zu ermöglichen, von den im Voraus festgelegten Prüfkriterien und den Programmen zu ihrer Anwendung Kenntnis zu erlangen - die Funktionsweise dieser Kriterien und Programme verstehen und deshalb in Kenntnis aller Umstände entscheiden kann, ob er von seinem in Art. 13 Abs. 1 der PNR-Richtlinie garantierten Recht auf Einlegung von Rechtsbehelfen Gebrauch macht, um gegebenenfalls zu rügen, dass die genannten Kriterien rechtswidrig und namentlich diskriminierend seien (vgl. entsprechend Urteil vom 24. November 2020, *Minister van Buitenlandse Zaken*, C-225/19 und C-226/19, EU:C:2020:951, Rn. 43 und die dort angeführte Rechtsprechung). Das Gleiche muss für die oben in Rn. 206 genannten Kriterien der Überprüfung gelten.

211. Im Rahmen eines gemäß Art. 13 Abs. 1 der PNR-Richtlinie eingelegten Rechtsbehelfs müssen schließlich das Gericht, das mit der Rechtmäßigkeitsprüfung der Entscheidung der zuständigen Behörden betraut ist, sowie, außer in Fällen einer Bedrohung der Sicherheit des Staates, der Betroffene selbst sowohl von allen Gründen als auch von den Beweisen, auf deren Grundlage diese Entscheidung getroffen wurde, Kenntnis erlangen können (vgl. entsprechend Urteil vom 4. Juni 2013, ZZ, C-300/11, EU:C:2013:363, Rn. 54 bis 59), einschließlich der im Voraus festgelegten Prüfkriterien und der Funktionsweise der Programme, mit denen diese Kriterien angewandt werden.

212. Im Übrigen obliegt es nach Art. 6 Abs. 7 bzw. Art. 15 Abs. 3 Buchst. b der PNR-Richtlinie dem Datenschutzbeauftragten und der nationalen Kontrollbehörde, die Kontrolle der Rechtmäßigkeit der von der PNR-Zentralstelle im Rahmen der Vorabüberprüfung vorgenommenen automatisierten Verarbeitungen zu gewährleisten. Diese Kontrolle erstreckt sich insbesondere darauf, dass die Verarbeitungen keinen diskriminierenden Charakter haben. In der erstgenannten Bestimmung heißt es hierzu, dass der Datenschutzbeauftragte Zugang zu sämtlichen von der PNR-Zentralstelle verarbeiteten Daten erhält, wobei sich dieser Zugang zwangsläufig auf die im Voraus festgelegten Kriterien und die von der Zentralstelle genutzten Datenbanken erstrecken muss, damit der vom Datenschutzbeauftragten nach dem 37. Erwägungsgrund der Richtlinie zu gewährleistende wirksame und weitreichende Datenschutz sichergestellt ist. Desgleichen können sich auch die von der nationalen Kontrollstelle nach der letztgenannten Bestimmung durchgeführten Ermittlungen, Inspektionen und Audits auf die im Voraus festgelegten Kriterien und die Datenbanken beziehen.

213. Nach alledem lassen sich die Bestimmungen der PNR-Richtlinie über die Vorabüberprüfung der PNR-Daten gemäß Art. 6 Abs. 2 Buchst. a der Richtlinie in einer Weise auslegen, die mit den Art. 7, 8 und 21 der Charta im Einklang steht und die Grenzen des absolut Notwendigen einhält.

6*) Zur nachträglichen Zurverfügungstellung und Überprüfung der PNR-Daten*

214. Nach Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie können die PNR-Daten ferner den zuständigen Behörden auf deren Anfrage zur Verfügung gestellt und nach der planmäßigen Ankunft in einem Mitgliedstaat oder nach dem Abflug von dort überprüft werden.

215. Zu den Voraussetzungen, unter denen eine solche Zurverfügungstellung und eine solche Überprüfung stattfinden können, ergibt sich aus dem Wortlaut dieser Bestimmung, dass die PNR-Zentralstelle die PNR-Daten verarbeiten darf, um ‘ im Einzelfall ... auf einer hinreichenden Grundlage gebührend begründete Anfragen ’ der zuständigen Behörden hinsichtlich der Zurverfügungstellung und Verarbeitung dieser Daten ‘ in besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität ’ zu beantworten. Für den Fall, dass die Anfrage nach Ablauf einer Frist von sechs Monaten ab der Übermittlung der PNR-Daten an die PNR-Zentralstelle erfolgt - so dass nach Art. 12 Abs. 2 der Richtlinie alle PNR-Daten durch Unkenntlichmachung bestimmter Datenelemente depersonalisiert werden -, bestimmt Art. 12 Abs. 3 der Richtlinie, dass die Offenlegung der vollständigen PNR-Daten - d. h. einer nicht depersonalisierten Fassung - nur zulässig ist, wenn zum einen berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Art. 6 Abs. 2 Buchst. b der Richtlinie erforderlich ist, und es zum anderen durch eine Justizbehörde oder eine andere nationale Behörde, die dafür nach nationalem Recht zuständig ist, genehmigt wird.

216. Insoweit ergibt sich zunächst schon aus dem Wortlaut von Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie, dass die PNR-Zentralstelle nicht systematisch die PNR-Daten aller Fluggäste zur Verfügung stellen und nachträglich überprüfen darf, sondern nur ‘ im Einzelfall ’ Anfragen hinsichtlich solcher Verarbeitungen ‘ in besonderen Fällen ’ beantworten kann. Da in dieser Bestimmung von ‘ besonderen Fällen ’ die Rede ist, müssen sich die Verarbeitungen allerdings nicht unbedingt auf die PNR-Daten eines einzigen Fluggasts beschränken, sondern können sich, wie die Kommission in Beantwortung einer Frage des Gerichtshofs ausgeführt hat, auch auf eine größere Zahl von Personen beziehen, sofern die betreffenden Personen eine Reihe gemeinsamer Merkmale aufweisen, die es erlauben, sie für die Zwecke der begehrten Zurverfügungstellung und Überprüfung zusammen als ‘ besonderen Fall ’ anzusehen.

217. Was sodann die materiellen Voraussetzungen dafür betrifft, dass die PNR-Daten von Fluggästen zur Verfügung gestellt und nachträglich überprüft werden dürfen, beziehen sich Art. 6 Abs. 2 Buchst. b und Art. 12 Abs. 3 Buchst. a der PNR-Richtlinie zwar auf ‘ gebührend begründete Anfragen ’ bzw. auf einen ‘ berechtigten Grund ’, ohne die Art dieser Gründe ausdrücklich zu präzisieren, doch ergibt sich schon aus dem Wortlaut der erstgenannten Bestimmung, der auf die in Art. 1 Abs. 2 der Richtlinie angegebenen Zwecke Bezug nimmt, dass die nachträgliche Zurverfügungstellung und Überprüfung der PNR-Daten nur erfolgen dürfen, um zu prüfen, ob Anhaltspunkte für eine mögliche Beteiligung der betreffenden Personen an terroristischen Straftaten oder an schwerer Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Fluggästen bestehen (siehe oben, Rn. 157).

218. Im Rahmen des durch die PNR-Richtlinie geschaffenen Systems betreffen die Zurverfügungstellung und die Verarbeitung von PNR-Daten gemäß Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie die Daten von Personen, die bereits vor ihrer planmäßigen Ankunft in dem betreffenden Mitgliedstaat oder vor ihrem Abflug von dort Gegenstand einer Vorabüberprüfung waren. Außerdem wird sich eine Anfrage zwecks nachträglicher Überprüfung vor allem auf Personen beziehen, deren PNR-Daten den zuständigen Behörden im Anschluss an die Vorabüberprüfung nicht übermittelt wurden, da sich keine Anhaltspunkte für ihre mögliche Beteiligung an terroristischen Straftaten oder an schwerer Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Fluggästen ergeben hatten. Unter diesen Umständen müssen die Zurverfügungstellung und die Verarbeitung dieser Daten zum Zweck ihrer nachträglichen Überprüfung auf neue Umstände gestützt werden, die eine solche Verwendung rechtfertigen (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 200 und die dort angeführte Rechtsprechung).

219. Was die Art der Umstände betrifft, die eine Zurverfügungstellung und Verarbeitung von PNR-Daten zum Zweck ihrer nachträglichen Überprüfung rechtfertigen können, so muss sich nach ständiger Rechtsprechung die betreffende Regelung, sei es die Unionsregelung oder eine nationale Vorschrift zu ihrer Umsetzung, bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugriff auf die fraglichen Daten zu gewähren ist, auf objektive Kriterien stützen, denn ein allgemeiner Zugang zu allen gespeicherten Daten kann unabhängig davon, ob irgendein - zumindest mittelbarer - Zusammenhang mit dem verfolgten Ziel besteht, nicht als auf das absolut Notwendige beschränkt angesehen werden. Insoweit darf im Zusammenhang mit dem Ziel, die Kriminalität zu bekämpfen, Zugriff grundsätzlich nur auf die Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Allerdings kann in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, auch Zugriff auf die Daten anderer Personen gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung derartiger Aktivitäten leisten könnten (Urteile vom 2. März 2021, *Prokuratuur* [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 50 und die dort angeführte Rechtsprechung, sowie vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 105).

220. Daher sind die Wendungen ‘ gebührend begründete Anfragen ’ und ‘ berechtigter Grund ’ in Art. 6 Abs. 2 Buchst. b bzw. Art. 12 Abs. 3 Buchst. a der PNR-Richtlinie im Licht der Art. 7 und 8 der Charta dahin auszulegen, dass sie sich auf objektive Anhaltspunkte beziehen, die geeignet sind, den begründeten Verdacht einer irgendwie gearteten Beteiligung der betreffenden Person an schwerer Kriminalität zu wecken, die - zumindest mittelbar - einen objektiven Zusammenhang mit der Beförderung von Fluggästen aufweist, während dieses Erfordernis bei terroristischen Straftaten, die einen solchen Zusammenhang aufweisen, erfüllt ist, wenn es objektive Anhaltspunkte dafür gibt, dass die PNR-Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung derartiger Straftaten leisten könnten.

221. Was schließlich die das Verfahren betreffenden Voraussetzungen für die Zurverfügungstellung und die Verarbeitung von PNR-Daten zum Zweck ihrer nachträglichen Überprüfung angeht, verlangt Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie für den Fall einer Anfrage, die nach Ablauf einer Frist von sechs Monaten ab der Übermittlung der PNR-Daten an die PNR-Zentralstelle erfolgt - so dass nach Art. 12 Abs. 2 die PNR-Daten durch Unkenntlichmachung der dort genannten Datenelemente depersonalisiert wurden -, dass die Offenlegung der vollständigen PNR-Daten, d. h. die Übermittlung einer nicht depersonalisierten Fassung, durch eine Justizbehörde oder eine andere nationale Behörde, die dafür nach nationalem Recht zuständig ist, genehmigt wird. In diesem Kontext haben die genannten Behörden die Begründetheit der Anfrage in vollem Umfang zu prüfen; ihre Prüfung muss sich insbesondere darauf erstrecken, ob die zur Stützung der Anfrage vorgelegten Beweise geeignet sind, die in der vorstehenden Randnummer genannte materielle Voraussetzung des Vorliegens eines ‘ berechtigten Grundes - zu untermauern.

222. Für den Fall, in dem die nachträgliche Zurverfügungstellung und Überprüfung der PNR-Daten vor Ablauf der Frist von sechs Monaten nach ihrer Übermittlung angefragt werden, sieht Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie zwar eine solche das Verfahren betreffende Voraussetzung nicht ausdrücklich vor. Bei der Auslegung der genannten Bestimmung ist jedoch der 25. Erwägungsgrund der PNR-Richtlinie zu berücksichtigen, aus dem hervorgeht, dass der Unionsgesetzgeber mit dieser das Verfahren betreffenden Voraussetzung für den Zugang zu PNR-Daten in einer Form, die eine unmittelbare Identifizierung der betroffenen Person ermöglicht, „das höchste Datenschutzniveau ... gewährleisten“ wollte. Jede Anfrage zwecks nachträglicher Zurverfügungstellung und Überprüfung geht aber mit einem solchen Zugang zu diesen Daten einher, unabhängig davon, ob die Anfrage vor Ablauf der Sechsmonatsfrist nach Übermittlung der PNR-Daten an die PNR-Zentralstelle oder nach deren Ablauf gestellt wird.

223. Um in der Praxis die uneingeschränkte Achtung der Grundrechte in dem durch die PNR-Richtlinie geschaffenen System und insbesondere die oben in den Rn. 218 und 219 genannten Bedingungen zu gewährleisten, ist es insbesondere unabdingbar, dass die Zurverfügungstellung der PNR-Daten zum Zweck einer nachträglichen Überprüfung grundsätzlich - außer in hinreichend begründeten Eilfällen - einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass die Entscheidung dieses Gerichts oder dieser Stelle im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird. In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 202 und die dort angeführte Rechtsprechung, sowie Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 110).

224. Unter diesen Umständen muss das in Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie für Anfragen zwecks Zurverfügungstellung der PNR-Daten, die nach Ablauf der Sechsmonatsfrist ab der Übermittlung dieser Daten an die PNR-Zentralstelle gestellt werden, vorgesehene Erfordernis einer vorherigen Kontrolle *mutatis mutandis* gelten, wenn die Anfrage vor Ablauf dieser Frist gestellt wird.

225. Überdies geht zwar aus Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie nicht ausdrücklich hervor, welchen Anforderungen die mit der vorherigen Kontrolle betraute Behörde genügen muss. Nach ständiger Rechtsprechung muss diese Behörde jedoch, um sicherzustellen, dass sich der mit einem Zugang zu personenbezogenen Daten verbundene Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte auf das absolut Notwendige beschränkt, über alle Befugnisse verfügen und alle Garantien aufweisen, die erforderlich sind, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden Interessen und Rechte miteinander in Einklang gebracht werden. Speziell im Fall strafrechtlicher Ermittlungen verlangt eine solche Kontrolle, dass die Behörde in der Lage ist, für einen gerechten Ausgleich zwischen den Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen (Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 107 und die dort angeführte Rechtsprechung).

226. Hierzu muss eine solche Behörde über eine Stellung verfügen, die es ihr erlaubt, bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch zu handeln, ohne jede Einflussnahme von außen. Das Erfordernis der Unabhängigkeit gebietet, dass es sich bei ihr um eine andere Stelle als die den Zugang zu den Daten begehrende Behörde handelt, damit diese Stelle in der Lage ist, ihre Kontrolle objektiv und unparteiisch, geschützt vor jeder Einflussnahme von außen, auszuüben. Im strafrechtlichen Bereich impliziert das Erfordernis der Unabhängigkeit insbesondere, dass die mit der vorherigen Kontrolle betraute Behörde zum einen nicht an der Durchführung des fraglichen Ermittlungsverfahrens beteiligt ist und zum anderen eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren hat (vgl. in diesem Sinne Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 108 und die dort angeführte Rechtsprechung).

227. Folglich lassen sich die Bestimmungen der PNR-Richtlinie über die nachträgliche Zurverfügungstellung und Überprüfung der PNR-Daten gemäß Art. 6 Abs. 2 Buchst. b der Richtlinie in einer Weise auslegen, die mit den Art. 7 und 8 sowie mit Art. 52 Abs. 1 der Charta im Einklang steht und die Grenzen des absolut Notwendigen einhält ».

B.59.2. Aus diesem Urteil geht hervor, dass der Gerichtshof der Europäischen Union mehrere Klarstellungen zur Auslegung der verschiedenen Verarbeitungen von PNR-Daten vornimmt, damit diese mit den Artikeln 7 und 8 sowie Artikel 52 Absatz 1 der Charta im Einklang stehen und damit die Grenzen des « absolut Notwendigen » einhalten.

Zunächst darf die PNR-Zentralstelle, was die Vorabüberprüfung der PNR-Daten betrifft, die das Ziel hat, die Personen zu ermitteln, die vor ihrer Ankunft oder ihrer Abreise genauer überprüft werden sollten, und die in einem ersten Schritt mittels automatisierter Verarbeitungen durchgeführt wird, diese Daten nur mit Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, abgleichen. Diese Datenbanken müssen nichtdiskriminierend sein und von den zuständigen Behörden im Zusammenhang mit der Bekämpfung terroristischer Straftaten und schwerer Kriminalität, die einen – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen aufweisen, betrieben werden (Randnrn. 186 bis 191).

Was sodann die im Voraus festgelegten Kriterien betrifft, auf denen die Vorabüberprüfung beruht, darf die PNR-Zentralstelle keine Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme (*machine learning*) heranziehen, die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung dieser Kriterien ändern können. Diese Kriterien müssen so festgelegt werden, dass ihre Anwendung speziell auf Personen abzielt, bei denen der begründete Verdacht einer Beteiligung an terroristischen Straftaten oder schwerer Kriminalität bestehen könnte, und dass sowohl « belastende » als auch « entlastende» Gesichtspunkte berücksichtigt werden und dass sie zugleich nicht zu unmittelbaren oder mittelbaren Diskriminierungen führen (Randnrn. 194 bis 200).

Um die Fehlerquote durch « falsch positive » Ergebnisse, die zwangsläufig durch eine automatisierte Verarbeitung generiert werden, zu begrenzen, ist es wesentlich, dass die PNR-Zentralstelle in einem zweiten Schritt eine individuelle Überprüfung auf andere, nicht automatisierte Art nach klaren und präzisen Regeln vornimmt, die Leitlinien und einen Rahmen für die von den Bediensteten der PNR-Zentralstelle, die mit der individuellen Überprüfung betraut sind, vorzunehmende Analyse vorgeben, um für eine dem Diskriminierungsverbot Rechnung tragende kohärente Verwaltungspraxis innerhalb der PNR-Zentralstelle zu sorgen (Randnrn. 178 bis 180). Insbesondere müssen sich die Mitgliedstaaten vergewissern, dass die PNR-Zentralstelle Kriterien für die objektive Überprüfung aufstellt, die es ihren Bediensteten ermöglichen, zum einen zu prüfen, ob und inwieweit ein Treffer (*hit*) tatsächlich eine Person betrifft, die möglicherweise an terroristischen Straftaten oder an schwerer Kriminalität beteiligt ist, und zum anderen, ob die automatisierten Verarbeitungen keinen diskriminierenden Charakter haben (Randnrn. 203 bis 209). Die PNR-Zentralstelle muss jede Verarbeitung von PNR-Daten, die im Rahmen der Vorabüberprüfung, einschließlich der individuellen Überprüfung auf nicht automatisierte Art, vorgenommen wird, zum Zweck der Überprüfung ihrer Rechtmäßigkeit und zur Selbstkontrolle dokumentieren (Randnr. 207).

Die zuständigen Behörden müssen sich auch vergewissern, dass der Betroffene die Funktionsweise der im Voraus festgelegten Prüfkriterien und Programme zu ihrer Anwendung verstehen und deshalb in Kenntnis aller Umstände entscheiden kann, ob er von seinem Recht auf Einlegung von Rechtsbehelfen Gebrauch macht, in dessen Rahmen das Gericht, das mit der Rechtmäßigkeitsprüfung der Entscheidung der zuständigen Behörden betraut ist, sowie, außer in Fällen einer Bedrohung der Sicherheit des Staates, der Betroffene selbst sowohl von allen Gründen als auch von den Beweisen, auf deren Grundlage diese Entscheidung getroffen wurde, Kenntnis erlangen können, einschließlich der im Voraus festgelegten Prüfkriterien und der Funktionsweise der Programme, mit denen diese Kriterien angewandt werden (Randnrn. 210 bis 211).

Was schließlich die nachträgliche Zurverfügungstellung und Überprüfung der PNR-Daten betrifft, das heißt nach der Ankunft oder der Abreise der betroffenen Person, ist der Gerichtshof der Europäischen Union der Auffassung, dass sie nur auf der Grundlage neuer Umstände und objektiver Anhaltspunkte vorgenommen werden dürfen, die entweder geeignet sind, den begründeten Verdacht einer Beteiligung dieser Person an schwerer Kriminalität zu wecken, die - zumindest mittelbar - einen objektiven Zusammenhang mit der Beförderung von Passagieren aufweist, oder wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung terroristischer Straftaten, die einen solchen Zusammenhang aufweisen, leisten könnten (Randnrn. 217 bis 220). Die Zurverfügungstellung von PNR-Daten zum Zweck einer solchen nachträglichen Überprüfung muss grundsätzlich - außer in hinreichend begründeten Eilfällen - auf einen mit Gründen versehenen Antrag der zuständigen Behörden einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen werden, und zwar unabhängig davon, ob dieser Antrag vor oder nach Ablauf der Sechsmonatsfrist ab der Übermittlung dieser Daten an die PNR-Zentralstelle gestellt wurde (Randnrn. 221 bis 226).

B.59.3. Aus dem Vorstehenden geht hervor, dass die Vereinbarkeit der PNR-Richtlinie mit den Artikeln 7 und 8 der Charta der Grundrechte und mit den Anforderungen des absolut Notwendigen von der Einhaltung der verschiedenen in B.59.2 aufgezählten Garantien abhängt, die sich aus der vom Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 gelieferten konformen Auslegung ergeben. Die Vereinbarkeit von nationalen Rechtsvorschriften zur Umsetzung der PNR-Richtlinie mit den Artikeln 7 und 8 der Charta der Grundrechte und mit den Anforderungen des absolut Notwendigen hängt daher von den gleichen Bedingungen ab.

B.59.4. Die Vereinbarkeit des vom Gesetz vom 25. Dezember 2016 eingerichteten Systems mit den verschiedenen im Klagegrund erwähnten Referenznormen erfordert es daher, das Gesetz vom 25. Dezember 2016 dahin auszulegen, dass es die in B.59.2 aufgezählten Garantien einbezieht, die zur Umsetzung der PNR-Richtlinie gehören, wie sie vom Gerichtshof der Europäischen Union ausgelegt wurde.

Es obliegt der PNR-Zentralstelle und den verschiedenen betroffenen Behörden, für die Einhaltung dieser Garantien bei der Umsetzung des Gesetzes vom 25. Dezember 2016 zu sorgen.

a) Die Verwaltung der Passagierdatenbank durch die PNR-Zentralstelle (Artikel 12 *bis* 16*)*

B.60.1. Nach Artikel 5 des Gesetzes vom 25. Dezember 2016 erhebt und übermittelt jedes Beförderungsunternehmen und Reiseunternehmen die Daten zu den in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet beförderten Passagieren, über die es verfügt, damit sie in der in Artikel 15 dieses Gesetzes erwähnten Passagierdatenbank gespeichert werden. Aufgrund von Artikel 6 des Gesetzes vom 25. Dezember 2016 teilen die Beförderungsunternehmen und Reiseunternehmen den betreffenden Personen mit, dass ihre Daten der PNR-Zentralstelle übermittelt werden und später zu den in Artikel 8 desselben Gesetzes erwähnten Zwecken verarbeitet werden können.

Diese Passagierdatenbank wird von der PNR-Zentralstelle verwaltet, die innerhalb des Föderalen Öffentlichen Dienstes Inneres geschaffen wird (Artikel 12). Die PNR-Zentralstelle ist verantwortlich für die Erhebung, Aufbewahrung und Verarbeitung der Passagierdaten sowie die Verwaltung der Passagierdatenbank und den Austausch der Daten und Ergebnisse ihrer Verarbeitung mit den PNR-Zentralstellen anderer Mitgliedstaaten der Europäischen Union und Europol (Artikel 13). Die PNR-Zentralstelle setzt sich zusammen aus einem leitenden Beamten, dem ein Unterstützungsdienst beisteht, und entsandten Mitgliedern der zuständigen Dienste (Artikel 14).

Der königliche Erlass vom 21. Dezember 2017 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung verschiedener Bestimmungen in Bezug auf die PNR-Zentralstelle und den Datenschutzbeauftragten » (nachstehend: königlicher Erlass vom 21. Dezember 2017) definiert unter anderem die Modalitäten der Zusammensetzung und Organisation der PNR-Zentralstelle.

B.60.2. Gemäß Artikel 15 § 1 des Gesetzes vom 25. Dezember 2016 wird eine vom Föderalen Öffentlichen Dienst Inneres verwaltete Passagierdatenbank geschaffen, in der die Passagierdaten gespeichert werden. Der leitende Beamte der PNR-Zentralstelle ist der für die Verarbeitung Verantwortliche der Passagierdaten im Sinne von Artikel 26 Nr. 8 des Gesetzes vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » (Artikel 15 § 2 des Gesetzes vom 25. Dezember 2016, abgeändert durch das Gesetz vom 2. Mai 2019).

Die aufgrund des vorliegenden Gesetzes vorgenommenen Verarbeitungen der Passagierdaten unterliegen dem vorerwähnten Gesetz vom 30. Juli 2018 (Artikel 15 § 4 des Gesetzes vom 25. Dezember 2016, abgeändert durch das Gesetz vom 2. Mai 2019).

Im Rahmen der in Artikel 8 § 1 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecke ist die Passagierdatenbank der PNR-Zentralstelle direkt zugänglich für die in den Artikeln 24 bis 27 desselben Gesetzes erwähnten Verarbeitungen gemäß den Bestimmungen von Kapitel 9 (Artikel 16). In Kapitel 9 des Gesetzes vom 25. Dezember 2016, das die Artikel 18 bis 23 umfasst, sind die Aufbewahrungsfristen der Passagierdaten vorgesehen.

Ein Vereinbarungsprotokoll, das der Umsetzung der technischen Sicherungs- und Zugriffsmodalitäten dient, wird vom leitenden Beamten der PNR-Zentralstelle und den zuständigen Diensten nach Absprache mit dem Datenschutzbeauftragten und nach Stellungnahme der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde abgeschlossen (Artikel 17, ersetzt durch das Gesetz vom 15. Juli 2018).

B.60.3. In Bezug auf die Schaffung der Passagierdatenbank ist in den Vorarbeiten erläutert:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 24).

B.61.1. Durch die Schaffung einer Passagierdatenbank, mit deren Verwaltung die PNR-Zentralstelle beauftragt ist, regelt das Gesetz vom 25. Dezember 2016 eine zentrale Speicherung der Passagierdaten unter der Verantwortung der PNR-Zentralstelle mit zahlreichen Garantien in Bezug auf die Sicherung, den Zugriff auf und die Speicherung von diesen Daten und indem die Datenverarbeitungen, die von der PNR-Zentralstelle im Rahmen der in Artikel 8 § 1 erwähnten Zwecke vorgenommen werden dürfen, eingeschränkt werden. Durch die präzise Benennung des Speicherortes dieser Daten ermöglicht es die Schaffung einer solchen Datenbank, den Datenfluss zu begrenzen.

Auch wenn sie nicht ausdrücklich durch die PNR-Richtlinie vorgesehen ist, stellt die Schaffung einer Passagierdatenbank, die mit den in B.60 genannten Garantien versehen ist, ein wesentliches Element des Systems dar, das durch die PNR-Richtlinie, die das Gesetz vom 25. Dezember 2016 umsetzt, eingeführt wurde.

B.61.2.1. Wie in B.60.1 erwähnt, setzt sich die PNR-Zentralstelle zusammen aus einem leitenden Beamten, dem ein Unterstützungsdienst beisteht, und entsandten Mitgliedern der zuständigen Dienste, die in Artikel 14 § 1 Absatz 1 Nr. 2 des Gesetzes vom 25. Dezember 2016 aufgezählt sind, das heißt (a) der im Gesetz vom 7. Dezember 1998 zur Organisation eines auf zwei Ebenen strukturierten integrierten Polizeidienstes erwähnten Polizeidienste, (b) der im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Staatssicherheit, (c) des im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Allgemeinen Nachrichten- und Sicherheitsdienstes und (d) der Enquetendienste, Ermittlungsdienste und Dienste der Generalverwaltung Zoll und Akzisen, die mit der Aufsicht, Kontrolle und Feststellung beauftragt sind.

Der leitende Beamte der PNR-Zentralstelle hat die letztendliche Verantwortung für die Aufgaben und Aufträge, mit denen das Gesetz die PNR-Zentralstelle beauftragt, und trifft zu diesem Zweck die notwendigen Entscheidungen (Artikel 3 des königlichen Erlasses vom 21. Dezember 2017); er muss Inhaber einer nationalen und EU-Sicherheitsermächtigung der Stufe « STRENG GEHEIM » gemäß dem Gesetz vom 11. Dezember 1998 sein (Artikel 11 Absatz 1 des königlichen Erlasses vom 21. Dezember 2017).

Bei ihrem Amtsantritt müssen die Mitglieder des Unterstützungsdienstes Inhaber einer nationalen und EU-Sicherheitsermächtigung mindestens der Stufe « GEHEIM » gemäß dem Gesetz vom 11. Dezember 1998 sein (Artikel 11 Absatz 2 des königlichen Erlasses vom 21. Dezember 2017).

Während ihrer Entsendung unterliegen die Mitglieder der zuständigen Dienste der funktionellen und hierarchischen Amtsgewalt des leitenden Beamten der PNR-Zentralstelle (Artikel 14 § 1 Absatz 2 des Gesetzes vom 25. Dezember 2016). Diese entsandten Mitglieder werden auf der Grundlage ihres Profils ausgewählt und müssen ein Gespräch vor einer Kommission aus drei Personen führen, der der leitende Beamte der PNR-Zentralstelle vorsteht und die nach dem Gespräch eine begründete Einstufung der Bewerber erstellt, auf deren Grundlage die entsandten Mitglieder benannt werden (Artikel 12 des königlichen Erlasses vom 21. Dezember 2017). Zum Zeitpunkt seiner Benennung muss das entsandte Mitglied insbesondere im Hinblick auf die Aufträge der PNR-Zentralstelle über eine einschlägige Erfahrung von mindestens drei Jahren verfügen und sich bereit zeigen, sich bei der Analyse der Passagier-Daten und bei der Zusammenarbeit mit den zuständigen Diensten einzubringen (Artikel 13 Nr. 3 des königlichen Erlasses vom 21. Dezember 2017), und Inhaber einer nationalen und EU-Sicherheitsermächtigung mindestens der Stufe « GEHEIM » gemäß dem Gesetz vom 11. Dezember 1998 sein (Artikel 14 des königlichen Erlasses vom 21. Dezember 2017).

B.61.2.2. Die Zusammensetzung der PNR-Zentralstelle und die Definition der « zuständigen Dienste » bieten Garantien der Fachkompetenz und der Vertraulichkeit bezüglich der Verwaltung der Passagierdatenbank im Hinblick auf die ausschließlichen Zwecke, die strikt auf die Zwecke der Verhütung, Aufdeckung sowie der Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität beschränkt sind, unter Bezugnahme auf die abschließend in Anhang II der PNR-Richtlinie aufgezählten Kategorien von Straftaten, die einen - zumindest mittelbaren - objektiven Zusammenhang mit der betreffenden Beförderung aufweisen. Dies gilt ebenfalls, sofern Mitglieder der Staatssicherheit und des Allgemeinen Nachrichten- und Sicherheitsdienstes in die PNR-Zentralstelle entsandt werden. Das, was in B.52 bezüglich des Zwecks der Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste, der in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnt ist, geurteilt wurde, ändert nichts an dieser Feststellung.

Bei den Mitgliedern der vorerwähnten Dienste kann nämlich davon ausgegangen werden, dass sie über eine umfassende Fachkompetenz im Bereich der Bekämpfung der Kriminalität verfügen, und daher die erforderlichen Kompetenzen besitzen, um die in der PNR-Richtlinie abschließend aufgezählten Zwecke zu verfolgen. Es geht außerdem aus dem Vorstehenden hervor, dass die entsandten Bediensteten auf der Grundlage eines direkt mit der Verwaltung der Passagierdatenbank zusammenhängenden Profils ausgewählt und benannt werden und dass sie ihre Aufgaben in diesem Rahmen allein unter der funktionellen und hierarchischen Amtsgewalt des leitenden Beamten der PNR-Zentralstelle wahrnehmen.

Wenn diese Bediensteten ihre Aufgaben zur Verwaltung der Passagierdatenbank wahrnehmen, dürfen sie daher ihre Aufgaben nur für die Verarbeitung zu allein den Zwecken, die nach der PNR-Richtlinie zulässig sind, wahrnehmen.

B.61.3. In Anbetracht des in B.61.2.2 Erwähnten und angesichts der verschiedenen in B.60 aufgeführten Garantien, mit denen die Schaffung und Verwaltung der Passagierdatenbank einhergeht, ist diese Maßnahme nicht unverhältnismäßig.

b) Die Verarbeitung von Passagierdaten im Rahmen der Vorabüberprüfung der Passagiere (Artikel 24 *bis* 26*)*

B.62.1. Artikel 16 des Gesetzes vom 25. Dezember 2016 sieht vor, dass die Passagierdaten im Rahmen der in Artikel 8 § 1 erwähnten Zwecke Gegenstand der in den Artikeln 24 bis 27 erwähnten Verarbeitungen sind.

Die Artikel 24 bis 26 betreffen die Verarbeitung von Passagierdaten im Rahmen der Vorabüberprüfung der Passagiere.

B.62.2. Gemäß Artikel 24 § 1 des Gesetzes vom 25. Dezember 2016 werden die Passagierdaten im Hinblick auf die Durchführung einer Vorabüberprüfung der Passagiere vor ihrer Ankunft im nationalen Hoheitsgebiet, ihrer Abreise aus dem nationalen Hoheitsgebiet oder ihrer Durchreise durch das nationale Hoheitsgebiet verarbeitet, um diejenigen Personen zu ermitteln, die genauer überprüft werden müssen (Artikel 24 § 1).

In den Vorarbeiten zum Gesetzes vom 25. Dezember 2016 heißt es:

« 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 » (ebenda, S. 28).

B.62.3.1. Die Vorabüberprüfung erfolgt auf zwei Wegen: einerseits die Korrelation der Passagierdaten mit den Datenbanken und andererseits die Korrelation der Daten mit im Voraus festgelegten Kriterien.

Diese Überprüfung beruht auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und:

- den von den zuständigen Diensten verwalteten Datenbanken und den von der PNR-Zentralstelle im Voraus festgelegten Überprüfungskriterien im Rahmen der Zwecke, die in Artikel 8 § 1 Nr. 1, 2, 4 und 5 erwähnt sind oder sich auf Bedrohungen beziehen, die in den Artikeln 8 Nr. 1 Buchstabe *a)*, *b)*, *c)*, *d)*, *f)*, *g)* und 11 § 2 des Gesetzes vom 30. November 1998 aufgeführt sind (Artikel 24 § 2, ersetzt durch das Gesetz vom 15. Juli 2018); für diese Zwecke sind alle in Artikel 9 erwähnten Passagierdaten zugänglich (Artikel 26 § 2, ersetzt durch das Gesetz vom 15. Juli 2018);

- den von den zuständigen Diensten verwalteten Datenbanken im Rahmen der in Artikel 8 § 1 Nr. 3 erwähnten Zwecke (Artikel 24 § 3). Für diesen Zweck sind nur die in Artikel 9 § 1 Nr. 18 erwähnten Passagierdaten, die sich auf die Person(en) beziehen, für die sich ein Treffer ergeben hat, zugänglich (Artikel 26 § 1).

Der Treffer wird innerhalb von vierundzwanzig Stunden nach Eingang der automatisierten Mitteilung des Treffers von der PNR-Zentralstelle validiert (Artikel 24 § 4). Ab dieser Validierung sorgt der zuständige Dienst, von dem der Treffer herkommt, schnellstmöglich für die weitere Bearbeitung (Artikel 24 § 5).

Schließlich wurde Artikel 24 § 2 des Gesetzes vom 25. Dezember 2016 aufgrund von Artikel 5 des Gesetzes vom 2. Mai 2019 durch einen neuen Absatz ergänzt. Mit dieser Abänderung « soll in Artikel 24 § 2 vorgesehen werden, dass die Vorabüberprüfung der Passagiere ebenfalls auf einer Analyse der anderen Passagierdaten im Zusammenhang mit einem Treffer beruht » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3652/001, S. 5).

B.62.3.2. Bezüglich der Korrelation mit den Datenbanken heißt es in den Vorarbeiten zum Gesetz vom 25. Dezember 2016:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 28-29).

Bezüglich der Korrelation mit den im Voraus festgelegten Kriterien heißt es in den Vorarbeiten zum Gesetz vom 25. Dezember 2016:

« 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 » (ebenda, SS. 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 » (ebenda, S. 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 » (ebenda, SS. 30-31).

B.62.4.1. In Bezug auf die im Voraus von der PNR-Zentralstelle festgelegten Überprüfungskriterien sieht Artikel 25 des Gesetzes vom 25. Dezember 2016 vor, dass für diese Kriterien nicht Daten als Grundlage dienen dürfen, aus denen die rassische oder ethnische Herkunft einer Person, ihre religiösen oder weltanschaulichen Überzeugungen, ihre politischen Meinungen, ihre Mitgliedschaft in einer Gewerkschaftsorganisation, ihr Gesundheitszustand, ihr Sexualleben oder ihre sexuelle Orientierung hervorgehen (§ 3).

Die Überprüfung der Passagiere vor ihrer Ankunft, ihrer Durchreise oder ihrer Abreise anhand im Voraus festgelegter Kriterien erfolgt in nichtdiskriminierender Weise. Diese Kriterien dürfen nicht darauf abzielen, eine Person zu identifizieren, und müssen zielgerichtet, verhältnismäßig und bestimmt sein (§ 2).

Die Passagierdaten können von der PNR-Zentralstelle zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien benutzt werden, die dazu bestimmt sind, bei den Vorabüberprüfungen der Passagiere Einzelpersonen ins Visier zu nehmen (Artikel 25 § 1).

B.62.4.2. In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wurde diesbezüglich dargelegt:

« 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 » (ebenda, S. 23; siehe ebenfalls *Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/003, S. 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 31).

B.63.1. Das System der Vorabüberprüfung bedeutet, dass die PNR-Daten aller Passagiere mit Datenbanken oder im Voraus festgelegten Kriterien abgeglichen werden, um Treffer zur Ermittlung der Personen, die genauer überprüft werden müssen, festzustellen.

Aus den vorstehenden im Lichte des in B.59 Erwähnten ausgelegten Elementen geht hervor, dass die Artikel 24 bis 26 des Gesetzes vom 25. Dezember 2016 die Grenzen des « absolut Notwendigen » einhalten.

B.63.2.1. Die Datenbanken, mit denen die PNR-Daten abgeglichen werden können, sind in Artikel 24 des Gesetzes vom 25. Dezember 2016 genau definiert und aufgezählt. Dies sind die Datenbanken der « zuständigen Dienste », das heißt der Polizeidienste, der Staatssicherheit, des Allgemeinen Nachrichten- und Sicherheitsdienstes und des Zolldienstes, aber es kann sich auch - wie in den in B.62.3.2 zitierten Vorarbeiten präzisiert ist - um eine Korrelation mit internationalen Datenbanken wie SIS II, Interpol (SLTD), auf die die zuständigen Dienste im Rahmen der Wahrnehmung ihrer Aufträge Zugriff haben, handeln.

Artikel 24 § 2 Nr. 1 des Gesetzes vom 25. Dezember 2016 erlaubt auch eine Korrelation mit « Personenlisten, die von den zuständigen Diensten im Rahmen ihrer Aufträge erstellt werden ». Wie in B.61.2.2 erwähnt, kann bei den Mitgliedern der vorerwähnten Dienste nämlich davon ausgegangen werden, dass sie über eine umfassende Fachkompetenz im Bereich der Bekämpfung der Kriminalität verfügen, und daher die erforderlichen Kompetenzen besitzen, um die in der PNR-Richtlinie abschließend aufgezählten Zwecke zu verfolgen.

B.63.2.2. Aus den in B.62.3.2 zitierten Vorarbeiten geht hervor, dass das verfolgte Ziel nicht darin besteht, sämtliche Datenbanken der Dienste mit der Passagierdatenbank zu verbinden, sondern die Korrelationen mit den Datenbanken in direktem Zusammenhang mit den Zwecken, die strikt auf die Bekämpfung terroristischer Straftaten und schwerer Kriminalität, die einen – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Passagieren aufweisen, beschränkt sind, technisch zu beschränken.

Der Gesetzgeber hatte daher das Ziel, die technischen Korrelationen im Rahmen der Vorabüberprüfung klar zu beschränken, um nur die Profile zu ermitteln, die im Hinblick auf ausschließlich die in der PNR-Richtlinie abschließend aufgezählten Ziele genauer überprüft werden sollten.

B.63.2.3. Der Abgleich der PNR-Daten mit den in Artikel 24 § 2 Nr. 1 des Gesetzes vom 25. Dezember 2016 erwähnten Datenbanken und Listen ist daher unter Berücksichtigung des Urteils des Gerichtshofes der Europäischen Union in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022, auf das in B.59 hingewiesen wurde, dahin auszulegen, dass er strikt auf ausschließlich die Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, technisch beschränkt ist, wobei diese Datenbanken von den zuständigen Behörden in nichtdiskriminierender Weise im Zusammenhang mit der Bekämpfung terroristischer Straftaten und schwerer Kriminalität, die einen - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Passagieren aufweisen, betrieben werden.

Es obliegt der PNR-Zentralstelle dafür zu sorgen, dass aus technischer Sicht die automatisierte Verarbeitung, die diese Korrelationen ermöglicht, nicht die Grenzen des absolut Notwendigen überschreitet.

B.63.3.1. In Bezug auf die im Voraus festgelegten Prüfkriterien verlangt Artikel 6 Absatz 4 der PNR-Richtlinie, dass diese im Voraus festgelegten Kriterien « zielgerichtet, verhältnismäßig und bestimmt » sein müssen und dass die Mitgliedstaaten sicherstellen, dass diese Kriterien « von der PNR-Zentralstelle aufgestellt und von ihr regelmäßig überprüft werden ».

Artikel 25 des Gesetzes vom 25. Dezember 2016 gewährleistet ausdrücklich, dass die Überprüfung der Passagiere vor ihrer Ankunft, ihrer Durchreise oder ihrer Abreise anhand im Voraus festgelegter Kriterien in nichtdiskriminierender Weise erfolgt und dass diese Kriterien nicht darauf abzielen dürfen, eine Person zu identifizieren, und zielgerichtet, verhältnismäßig und bestimmt sein müssen (§ 2). In den in B.62.4.2 zitierten Vorarbeiten ist präzisiert, dass sie nicht auf Namen bezogen sind. Zudem dürfen für diese Kriterien nicht Daten als Grundlage dienen, aus denen die rassische oder ethnische Herkunft einer Person, ihre religiösen oder weltanschaulichen Überzeugungen, ihre politischen Meinungen, ihre Mitgliedschaft in einer Gewerkschaftsorganisation, ihr Gesundheitszustand, ihr Sexualleben oder ihre sexuelle Orientierung hervorgehen (§ 3).

Analog zu den Korrelationen mit den Datenbanken ist die Ausarbeitung der im Voraus festgelegten Kriterien so zu verstehen, dass sie technisch auf die Ermittlung von Personen beschränkt ist, die im Hinblick auf die Zwecke genauer überprüft werden sollten, die strikt auf die Bekämpfung terroristischer Straftaten und schwerer Kriminalität, die einen - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Fluggästen aufweisen, beschränkt sind.

B.63.3.2. Die Ausarbeitung der in Artikel 25 des Gesetzes vom 25. Dezember 2016 erwähnten im Voraus festgelegten Kriterien ist daher unter Berücksichtigung des vorerwähnten Urteils des Gerichtshofes der Europäischen Union in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022, auf das in B.59 hingewiesen wurde, dahin auszulegen, dass sie die PNR-Zentralstelle daran hindert, Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme (*machine learning*) heranzuziehen, die Änderungen ohne menschliche Einwirkung und Kontrolle vornehmen können. Außerdem müssen die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien so festgelegt werden, dass ihre Anwendung speziell auf Personen abzielt, bei denen der begründete Verdacht einer Beteiligung an terroristischen Straftaten oder schwerer Kriminalität bestehen könnte, und dass sowohl « belastende » als auch « entlastende» Gesichtspunkte berücksichtigt werden und dass sie zugleich nicht zu unmittelbaren oder mittelbaren Diskriminierungen führen.

Es obliegt der PNR-Zentralstelle dafür zu sorgen, dass aus technischer Sicht die Ausarbeitung der im Voraus festgelegten Kriterien nicht die Grenzen des absolut Notwendigen überschreitet.

B.63.4.1. Was das Bestreben betrifft, die Fehlerquote durch « falsch positive » Ergebnisse zu begrenzen, ist festzustellen, dass Artikel 24 §§ 4 und 5 des Gesetzes vom 25. Dezember 2016 vorsieht, dass die PNR-Zentralstelle eine individuelle Überprüfung vornimmt, indem sie den positiven Treffer innerhalb von vierundzwanzig Stunden validiert und so gewährleistet, dass im Fall eines positiven Treffers die automatisierte systematische Verarbeitung Gegenstand einer individuellen Überprüfung auf andere nicht automatisierte Art ist, um zu klären, ob die zuständige Behörde Maßnahmen im Einklang mit dem nationalen Recht ergreifen muss, wie es Artikel 6 Absatz 5 der PNR-Richtlinie erfordert.

Außerdem gewährleistet Artikel 21 § 3 Absatz 2 des Gesetzes vom 25. Dezember 2016, dass, wenn die in Artikel 24 § 4 erwähnte anschließende individuelle Überprüfung negativ ausfällt, dieses Ergebnis dennoch gespeichert werden kann, um künftige falsche Treffer zu vermeiden, solange die dazugehörigen Daten nicht aufgrund von Artikel 18 gelöscht sind.

Diese individuelle Überprüfung ist unter Berücksichtigung des vorerwähnten Urteils des Gerichtshofes der Europäischen Union in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022, auf das in B.59 hingewiesen wurde, dahin auszulegen, dass sie nach klaren und präzisen Regeln durchgeführt wird, die es ermöglichen, für eine dem Diskriminierungsverbot Rechnung tragende kohärente Verwaltungspraxis innerhalb der PNR-Zentralstelle zu sorgen und zu prüfen, ob und inwieweit ein Treffer (*hit*) tatsächlich eine Person betrifft, die möglicherweise an terroristischen Straftaten oder an schwerer Kriminalität beteiligt ist.

Es obliegt der PNR-Zentralstelle für die Einhaltung dieser Anforderungen zu sorgen.

B.63.4.2. Darüber hinaus gewährleistet Artikel 23 § 1 des Gesetzes vom 25. Dezember 2016, dass die Datenverarbeitung protokolliert wird, was in Artikel 4 Nr. 11 desselben Gesetzes definiert ist als « de[r] in Artikel 23 § 2 erwähnten Mechanismus, durch den die Rückverfolgbarkeit der durchgeführten Datenverarbeitungen ermöglicht wird, damit es möglich ist, die Person, die Daten abgefragt hat, die abgefragten Daten, den Zeitpunkt und den Zweck dieses Abfragens zu identifizieren ».

Artikel 23 § 2 des Gesetzes vom 25. Dezember 2016 gewährleistet, dass die PNR-Zentralstelle alle ihrer Zuständigkeit unterliegenden Verarbeitungssysteme und -verfahren während fünf Jahren dokumentiert. Diese Dokumentation muss zumindest folgende Unterlagen enthalten: Name und Kontaktangaben der Organisation und des Personals, die innerhalb der PNR-Zentralstelle mit der Verarbeitung der Passagierdaten beauftragt sind, sowie ihre Anfragen und die verschiedenen Ebenen ihrer Zugriffsberechtigung (1) Register der Verarbeitungsvorgänge, das zumindest die Identität der Person enthält, die die Passagierdaten verarbeitet hat (2) Anfragen von zuständigen Behörden und PNR-Zentralstellen anderer Mitgliedstaaten der Europäischen Union (3) jede Anfrage und jede Übermittlung von Daten durch beziehungsweise an Drittstaaten (4). Die PNR-Zentralstelle stellt der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde auf deren Anfrage diese Dokumentation zur Verfügung (Artikel 23 § 2 Absatz 2).

Diese Bestimmung gewährleistet somit, dass die PNR-Zentralstelle jede Verarbeitung von PNR-Daten, die im Rahmen der Vorabüberprüfung, einschließlich der individuellen Überprüfung auf nicht automatisierte Art, vorgenommen wird, zum Zweck der Überprüfung ihrer Rechtmäßigkeit und zur Selbstkontrolle dokumentiert.

B.63.5. Schließlich hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022, das in B.59 zitiert wurde, bezüglich der Rechte und Information der betreffenden Personen präzisiert, dass die zuständigen Behörden sich auch vergewissern müssen, dass der Betroffene die Funktionsweise der im Voraus festgelegten Prüfkriterien und Programme zu ihrer Anwendung verstehen und deshalb in Kenntnis aller Umstände entscheiden kann, ob er von seinem in Artikel 13 Absatz 1 der PNR-Richtlinie gewährleisteten Recht auf Einlegung von Rechtsbehelfen Gebrauch macht, in dessen Rahmen das Gericht, das mit der Rechtmäßigkeitsprüfung der Entscheidung der zuständigen Behörden betraut ist, sowie, außer in Fällen einer Bedrohung der Sicherheit des Staates, der Betroffene selbst sowohl von allen Gründen als auch von den Beweisen, auf deren Grundlage diese Entscheidung getroffen wurde, Kenntnis erlangen können, einschließlich der im Voraus festgelegten Prüfkriterien und der Funktionsweise der Programme, mit denen diese Kriterien angewandt werden (Randnrn. 210-211).

Es obliegt den zuständigen Behörden, für die Einhaltung dieser Anforderungen zu sorgen.

c) Die gezielten Recherchen (Artikel 27, 50 *und* 51*)*

B.64.1. In Artikel 27 des Gesetzes vom 25. Dezember 2016 in seiner ursprünglichen Fassung wird die Verarbeitung von Passagierdaten gestattet, um gezielte Recherchen zu den in Artikel 8 § 1 Nr. 1, 2, 4 und 5 desselben Gesetzes erwähnten Zwecken und unter den in Artikel 46*septies* des Strafprozessgesetzbuches oder in Artikel 16/3 des Gesetzes vom 30. November 1998 vorgesehenen Bedingungen durchzuführen, die jeweils durch die Artikel 50 und 51 des Gesetzes vom 25. Dezember 2016 eingefügt wurden. Durch Artikel 6 des Gesetzes vom 2. Mai 2019, der nicht angefochten wurde, wurde Artikel 27 des Gesetzes vom 25. Dezember 2016 abgeändert, um diese gezielten Recherchen zu den in Artikel 281 § 4 des am 18. Juli 1977 koordinierten allgemeinen Gesetzes über Zölle und Akzisen vorgesehenen Bedingungen zu ermöglichen.

Gemäß Artikel 20 des Gesetzes vom 25. Dezember 2016 gelten die Anwendungsbedingungen von Artikel 27 desselben Gesetzes ebenfalls für die Mitteilung der vollständigen Passagierdaten nach Ablauf des in Artikel 19 des besagten Gesetzes vorgesehenen sechsmonatigen Zeitraums.

B.64.2. Artikel 46*septies* des Strafprozessgesetzbuches, eingefügt durch Artikel 50 des Gesetzes vom 25. Dezember 2016, bestimmt:

« Bei der Ermittlung von Verbrechen und Vergehen, die in Artikel 8 § 1 Nr. 1, 2 und 5 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten erwähnt sind, kann der Prokurator des Königs durch einen mit Gründen versehenen schriftlichen Beschluss den Gerichtspolizeioffizier damit beauftragen, die PNR-Zentralstelle aufzufordern, die Passagierdaten gemäß Artikel 27 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten mitzuteilen.

Die Begründung spiegelt die Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und die Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe wider.

Die Maßnahme kann eine Gesamtheit von Daten in Bezug auf eine spezifische Ermittlung betreffen. In diesem Fall bestimmt der Prokurator des Königs die Dauer der Maßnahme, die einen Monat ab dem Beschluss nicht überschreiten darf, unbeschadet einer Erneuerung.

In Fällen äußerster Dringlichkeit kann jeder Gerichtspolizeioffizier mit der mündlichen und vorherigen Zustimmung des Prokurators des Königs durch einen mit Gründen versehenen schriftlichen Beschluss den leitenden Beamten der PNR-Zentralstelle auffordern, die Passagierdaten mitzuteilen. Der Gerichtspolizeioffizier teilt dem Prokurator des Königs diesen mit Gründen versehenen schriftlichen Beschluss sowie die erhaltenen Informationen binnen vierundzwanzig Stunden mit und begründet außerdem die äußerste Dringlichkeit ».

Diese Bestimmung betrifft also gezielte Recherchen im Rahmen der in Artikel 8 § 1 Nr. 1, 2, und 5 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecke. Diese Maßnahme ist mit mehreren Garantien versehen, darunter die vorherige Zustimmung des Prokurators des Königs.

B.64.3. Artikel 16/3 des Gesetzes vom 30. November 1998, eingefügt durch Artikel 51 des Gesetzes vom 25. Dezember 2016, bestimmt:

« § 1. Die Nachrichten- und Sicherheitsdienste können im Interesse der Ausübung ihrer Aufträge und ordnungsgemäß begründet beschließen, auf die in Artikel 27 des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten erwähnten Passagierdaten zuzugreifen.

§ 2. Der in § 1 erwähnte Beschluss wird von einem Dienstleiter gefasst und der in Kapitel 7 des vorerwähnten Gesetzes erwähnten PNR-Zentralstelle schriftlich übermittelt. Der Beschluss wird zusammen mit seiner Begründung dem Ständigen Ausschuss N notifiziert.

Der Ständige Ausschuss N verbietet den Nachrichten- und Sicherheitsdiensten, die gesammelten Daten unter Bedingungen zu benutzen, die die gesetzlichen Bedingungen nicht einhalten.

Der Beschluss kann eine Gesamtheit von Daten in Bezug auf eine spezifische nachrichtendienstliche Untersuchung betreffen. In diesem Fall wird dem Ständigen Ausschuss N einmal pro Monat die Liste der Abfragen der Passagierdaten übermittelt ».

Diese Bestimmung betrifft also gezielte Recherchen im Rahmen des in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnten Zwecks. Diese Maßnahme ist mit mehreren Garantien versehen, darunter die Information und Kontrolle des Ständigen Ausschusses N.

B.62.4. In Bezug auf die gezielten Recherchen heißt es in den Vorarbeiten zum Gesetz vom 25. Dezember 2016:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 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* » (ebenda, S. 43).

B.65.1. Die klagende Partei führt des Weiteren an, dass die entsandten Mitglieder der Polizeidienste, die der PNR-Zentralstelle angehören, nicht ausreichend unabhängig seien, um auf die Zugriffsanfragen im Rahmen dieser gezielten Recherchen zu antworten.

B.65.2. Nach Artikel 14 § 1 des Gesetzes vom 25. Dezember 2016 setzt sich die PNR-Zentralstelle zusammen aus einem leitenden Beamten, dem ein Unterstützungsdienst beisteht, (Artikel 14 § 1 Nr. 1) sowie aus entsandten Mitgliedern, die aus den Polizeidiensten, der Staatssicherheit, dem Allgemeinen Nachrichten- und Sicherheitsdienst und der Verwaltung Ermittlung und Fahndung und den Enquetendiensten, Ermittlungsdiensten und Diensten der Generalverwaltung Zoll und Akzisen, die mit der Aufsicht, Kontrolle und Feststellung beauftragt sind, stammen (Artikel 14 § 1 Nr. 2, ersetzt durch das Gesetz vom 15. Juli 2018).

In Bezug auf die Zusammensetzung der PNR-Zentralstelle heißt es in den Vorarbeiten:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 22).

Der Minister der Sicherheit und des Innern hat ebenfalls erläutert:

« 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 » (*Parl. Dok.*, Kammer, 2016-2017, DOC 54-2069/003, S. 24).

B.65.3. In Ausführung von Artikel 14 § 4 des Gesetzes vom 25. Dezember 2016 bestimmt der königliche Erlass vom 21. Dezember 2017 « zur Ausführung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten und zur Festlegung verschiedener Bestimmungen in Bezug auf die PNR-Zentralstelle und den Datenschutzbeauftragten » die Modalitäten der Zusammensetzung und Organisation der PNR-Zentralstelle.

Im Bericht an den König, der diesem königlichen Erlass vorausging, heißt es diesbezüglich:

« 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 » (*Belgisches Staatsblatt* vom 29. Dezember 2017, zweite Ausgabe, S. 116833).

Das Entsendeverfahren ist in den Artikeln 12 bis 21 des vorgenannten königlichen Erlasses vom 21. Dezember 2017 geregelt.

B.65.4. Wie in B.61.2 erwähnt wurde, soll durch den Umstand, dass die entsandten Mitglieder der zuständigen Dienste an der Arbeitsweise der PNR-Zentralstelle beteiligt sind, gewährleistet werden, dass sich diese PNR-Zentralstelle aus Personen zusammensetzt, die über ein gewisses Fachwissen verfügen, um so die Effizienz der PNR-Zentralstelle zu verstärken.

Diese Möglichkeit der Entsendung ist außerdem ausdrücklich in Artikel 4 Absatz 3 der PNR-Richtlinie vorgesehen, der bestimmt:

« Das Personal der PNR-Zentralstelle kann aus Mitarbeitern zuständiger Behörden bestehen, die zu diesem Zweck abgeordnet wurden. [...] ».

Nichts deutet darauf hin, dass diese Personen, auch wenn sie das Statut ihres ursprünglichen Dienstes behalten, ihre Aufgaben innerhalb der PNR-Zentralstelle nicht unabhängig ausüben. Artikel 14 § 1 Absatz 2 des Gesetzes vom 25. Dezember 2016 präzisiert außerdem, dass « die Mitglieder der zuständigen Dienste [während der Entsendung] der funktionellen und hierarchischen Amtsgewalt des leitenden Beamten der PNR-Zentralstelle [unterliegen] ».

Die Mitglieder der PNR-Zentralstelle machen sich zudem strafbar, wenn sie gegen die Schweigepflicht verstoßen oder wissentlich und willentlich Informationen, Daten und Auskünfte zurückhalten, wodurch die in Artikel 8 vorgesehenen Zwecke behindert werden (Artikel 48 und 49 desselben Gesetzes).

B.65.5.1. Was den Zugriff auf die PNR-Daten nach einer sechsmonatigen Frist betrifft, bestimmt Artikel 12 Absatz 3 der PNR-Richtlinie:

« Nach Ablauf der in Absatz 2 genannten Frist von sechs Monaten ist die Offenlegung der vollständigen PNR-Daten nur zulässig, wenn:

a) berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Artikels 6 Absatz 2 Buchstabe b erforderlich ist und

b) dies genehmigt wird durch

i) eine Justizbehörde oder

ii) eine andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind, vorbehaltlich der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten ».

B.65.5.2. Gemäß Artikel 20 des Gesetzes vom 25. Dezember 2016 gelten die Anwendungsbedingungen von Artikel 27 desselben Gesetzes ebenfalls für die Mitteilung der vollständigen Passagierdaten nach der in Artikel 19 vorgesehenen sechsmonatigen Frist. Durch die Ausdehnung der in Artikel 27 des besagten Gesetzes erwähnten Regelung der gezielten Recherchen auf die Mitteilung der vollständigen Passagierdaten nach Ablauf der sechsmonatigen Frist weicht Artikel 20 von dem in Artikel 19 des Gesetzes vom 25. Dezember 2016 festgelegten Grundsatz ab, dass nach Ablauf einer sechsmonatigen Frist ab der Speicherung der Passagierdaten in der Passagierdatenbank alle Passagierdaten depersonalisiert werden.

In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 wurde diesbezüglich dargelegt:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 26).

Es ergibt sich daher aus der Verbindung der Artikel 20 und 27 des Gesetzes vom 25. Dezember 2016, dass die Bedingungen für den Zugriff auf die PNR-Daten im Rahmen von gezielten Recherchen auf die Mitteilung der Daten nach Ablauf einer sechsmonatigen Frist nach der Übermittlung dieser Daten an die PNR-Zentralstelle übertragen wurden. Nach dieser Frist müssen diese Daten depersonalisiert werden.

B.66.1. Da – wie in B.52 geurteilt wurde – der in Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 erwähnte Zweck die Anforderungen des « absolut Notwendigen » überschreitet, gilt das Gleiche für Bestimmungen, die es den Nachrichten- und Sicherheitsdiensten gestatten würden, durch eine einfache mit Gründen versehene Entscheidung für diesen Zweck, der über die Zwecke hinausgeht, die abschließend in der PNR-Richtlinie aufgezählt sind, auf die Daten der Passagierdatenbank zuzugreifen.

B.66.2. Aus den gleichen Gründen wie denjenigen, die bezüglich Artikel 8 § 1 Nr. 4 des Gesetzes vom 25. Dezember 2016 angeführt wurden, überschreitet Artikel 51 des Gesetzes vom 25. Dezember 2016 die Anforderungen des « absolut Notwendigen ».

B.67. Der Gerichtshof muss nun prüfen, ob die Regelung der Mitteilung der PNR-Daten, die von den Artikeln 27 und 50 des Gesetzes vom 25. Dezember 2016 festgelegt wird, die Anforderungen des absolut Notwendigen sowie die Garantien in Bezug auf die Unabhängigkeit der Behörde, die dafür zuständig ist, diesen Zugriff zu erlauben, einhält.

B.68.1. Wie in B.59 erwähnt, ist der Gerichtshof der Europäischen Union in Bezug auf die nachträgliche Zurverfügungstellung und Überprüfung der PNR-Daten, das heißt nach der Ankunft oder der Abreise der betroffenen Person, der Auffassung, dass sie nur auf der Grundlage neuer Umstände und objektiver Anhaltspunkte vorgenommen werden dürfen, die entweder geeignet sind, den begründeten Verdacht einer Beteiligung dieser Person an schwerer Kriminalität zu wecken, die - zumindest mittelbar - einen objektiven Zusammenhang mit der Beförderung von Passagieren aufweist, oder wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung terroristischer Straftaten, die einen solchen Zusammenhang aufweisen, leisten könnten.

Die Zurverfügungstellung von PNR-Daten zum Zweck einer solchen nachträglichen Überprüfung muss grundsätzlich - außer in hinreichend begründeten Eilfällen - auf einen mit Gründen versehenen Antrag der zuständigen Behörden einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen werden, und zwar unabhängig davon, ob dieser Antrag vor oder nach Ablauf der Sechsmonatsfrist ab der Übermittlung dieser Daten an die PNR-Zentralstelle gestellt wurde.

Insbesondere präzisiert der Gerichtshof der Europäischen Union, dass das in Artikel 12 Absatz 3 Buchstabe *b)* der PNR-Richtlinie für Anfragen zwecks Zurverfügungstellung der PNR-Daten, die nach Ablauf der Sechsmonatsfrist ab der Übermittlung dieser Daten an die PNR-Zentralstelle gestellt werden, vorgesehene Erfordernis einer vorherigen Kontrolle *mutatis mutandis* gelten muss, wenn die Anfrage vor Ablauf dieser Frist gestellt wird (Randnr. 224).

B.68.2. Auf die Frage des Verfassungsgerichtshofes nach der Auslegung einer « andere[n] nationale[n] Behörde, die [...] zuständig ist » im Sinne von Artikel 12 Absatz 3 der PNR-Richtlinie hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 erkannt:

« 241. In der Sache ist festzustellen, dass der Wortlaut von Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie, in dessen Ziff. i und ii von einer ' Justizbehörde ' und einer ' andere[n] nationale[n] Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind ', die Rede ist, diese beiden Behörden auf die gleiche Stufe stellt, wie sich aus der Verwendung der Konjunktion ' oder ' zwischen den Ziff. i und ii ergibt. Aus diesem Wortlaut ergibt sich somit, dass die ' andere ' zuständige nationale Behörde eine Alternative zur Justizbehörde darstellt und daher ein mit ihr vergleichbares Niveau an Unabhängigkeit und Unparteilichkeit aufweisen muss.

242. Dieses Ergebnis wird durch das im 25. Erwägungsgrund der PNR-Richtlinie genannte Ziel bestätigt, hinsichtlich des Zugriffs auf die vollständigen PNR-Daten, die eine unmittelbare Identifizierung der betroffenen Person ermöglichen, das höchste Datenschutzniveau zu gewährleisten. Ferner heißt es dort, dass ein solcher Zugriff nach Ablauf der Frist von sechs Monaten ab Übermittlung der PNR-Daten an die PNR-Zentralstelle nur unter sehr strengen Bedingungen gewährt werden sollte.

243. Das genannte Ergebnis wird zudem durch die Entstehungsgeschichte der PNR-Richtlinie bestätigt. Während nämlich der oben in Rn. 155 erwähnte Richtlinienvorschlag, auf dem die PNR-Richtlinie beruht, lediglich vorsah, dass ' [d]er Zugriff auf die vollständigen PNR-Daten ... vom Leiter der PNR-Zentralstelle genehmigt werden muss ', werden in der letztlich vom Unionsgesetzgeber gewählten Fassung von Art. 12 Abs. 3 Buchst. b der Richtlinie die Justizbehörde und eine ' andere nationale Behörde ', die für die Prüfung zuständig ist, ob die Bedingungen für die Offenlegung der vollständigen PNR-Daten erfüllt sind, benannt und auf die gleiche Stufe gestellt.

244. Überdies und vor allem ist es im Einklang mit der oben in den Rn. 223, 225 und 226 angeführten ständigen Rechtsprechung unabdingbar, dass der Zugriff der zuständigen Behörden auf die gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass die Entscheidung dieses Gerichts oder dieser Stelle im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von diesen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird. Das Erfordernis der Unabhängigkeit der mit der Wahrnehmung der vorherigen Kontrolle betrauten Stelle gebietet es zudem, dass sie gegenüber der den Zugriff auf die Daten begehrenden Behörde die Eigenschaft eines Dritten hat, damit diese Stelle in der Lage ist, ihre Kontrolle in objektiver und unparteiischer Weise, geschützt vor jeder Einflussnahme von außen, auszuüben. Insbesondere impliziert das Erfordernis der Unabhängigkeit im strafrechtlichen Bereich, dass die mit der vorherigen Kontrolle betraute Behörde zum einen nicht an der Durchführung des fraglichen Ermittlungsverfahrens beteiligt ist und zum anderen eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren einnimmt.

245. Wie der Generalanwalt in Nr. 271 seiner Schlussanträge ausgeführt hat, sieht Art. 4 der PNR-Richtlinie in seinen Abs. 1 und 3 vor, dass die in jedem Mitgliedstaat errichtete oder benannte PNR-Zentralstelle eine für die Verhütung, Aufdeckung, Ermittlung und Verfolgung terroristischer Straftaten und schwerer Kriminalität zuständige Behörde ist und dass ihr Personal aus zu diesem Zweck abgeordneten Mitarbeitern zuständiger Behörden im Sinne von Art. 7 der Richtlinie bestehen kann, so dass die PNR-Zentralstelle zwangsläufig mit diesen Behörden verbunden ist. Die PNR-Zentralstelle kann zudem nach Art. 6 Abs. 2 Buchst. b der Richtlinie PNR-Daten verarbeiten und stellt die Ergebnisse dieser Verarbeitung den genannten Behörden zur Verfügung. In Anbetracht dessen kann nicht davon ausgegangen werden, dass die PNR-Zentralstelle gegenüber diesen Behörden die Eigenschaft eines Dritten hat und damit alle Merkmale der Unabhängigkeit und Unparteilichkeit aufweist, die erforderlich sind, um die in der vorstehenden Randnummer genannte vorherige Kontrolle auszuüben und zu prüfen, ob die in Art. 12 Abs. 3 Buchst. b der Richtlinie vorgesehenen Voraussetzungen für die Offenlegung der vollständigen PNR-Daten erfüllt sind.

246. Im Übrigen vermag der Umstand, dass die letztgenannte Bestimmung in Ziff. ii für den Fall der Genehmigung einer Offenlegung der vollständigen PNR-Daten durch eine ' andere nationale Behörde ' den Vorbehalt ' der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten ' aufstellt, während dies bei der Genehmigung durch eine Justizbehörde nicht der Fall ist, diese Beurteilung nicht in Frage zu stellen. Nach gefestigter Rechtsprechung ermöglicht eine nachträgliche Kontrolle wie die vom Datenschutzbeauftragten vorgenommene es nämlich nicht, das Ziel der vorherigen Kontrolle zu erreichen, das darin besteht, zu verhindern, dass ein über das absolut Notwendige hinausgehender Zugang zu den fraglichen Daten genehmigt wird (vgl. in diesem Sinne Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 110 und die dort angeführte Rechtsprechung).

247. Nach alledem ist auf die siebte Frage zu antworten, dass Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie dahin auszulegen ist, dass er nationalen Rechtsvorschriften entgegensteht, nach denen die als PNR-Zentralstelle errichtete Behörde zugleich die für die Genehmigung der Offenlegung der PNR-Daten nach Ablauf der Frist von sechs Monaten ab ihrer Übermittlung an die PNR-Zentralstelle zuständige nationale Behörde ist. ».

B.68.3. Aus dem Vorstehenden geht hervor, dass an die nachträgliche Zurverfügungstellung und Überprüfung der PNR-Daten sowohl die Organisation betreffende als auch substanzielle Anforderungen gestellt werden.

Einerseits kann in Bezug auf die Organisation die PNR-Zentralstelle nicht als die « zuständige nationale Behörde » angesehen werden, die für die Genehmigung der Offenlegung der PNR-Daten entweder vor oder nach Ablauf der Frist von sechs Monaten ab ihrer Übermittlung an die PNR-Zentralstelle zuständig ist. Nach Auffassung des Gerichtshofs der Europäischen Union muss eine solche zuständige nationale Behörde ein mit einer Justizbehörde vergleichbares Niveau an Unabhängigkeit und Unparteilichkeit aufweisen, was impliziert, dass die mit der vorherigen Kontrolle betraute Behörde zum einen nicht an der Durchführung des fraglichen Ermittlungsverfahrens beteiligt ist und zum anderen eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren einnimmt (Randnr. 244). Eine nachträgliche Kontrolle wie die vom Datenschutzbeauftragten vorgenommene ermöglicht es nicht, das Ziel der vorherigen Kontrolle zu erreichen (Randnr. 246).

Andererseits darf in substanzieller Hinsicht diese Zurverfügungstellung zudem nur auf der Grundlage neuer Umstände und objektiver Anhaltspunkte vorgenommen werden, die entweder geeignet sind, den begründeten Verdacht einer Beteiligung dieser Person an schwerer Kriminalität zu wecken, die - zumindest mittelbar - einen objektiven Zusammenhang mit der Beförderung von Passagieren aufweist, oder wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung terroristischer Straftaten, die einen solchen Zusammenhang aufweisen, leisten könnten.

B.69.1. Wie in B.64.1 und B.64.2 erwähnt, gestattet Artikel 27 des Gesetzes vom 25. Dezember 2016 die Mitteilung der PNR-Daten, um gezielte Recherchen unter den insbesondere in Artikel 46*septies* des Strafprozessgesetzbuches vorgesehenen Bedingungen durchzuführen, der durch Artikel 50 des Gesetzes vom 25. Dezember 2016 eingefügt wurde.

Diese Bestimmung beschränkt die Anwendung des vorerwähnten Artikels 27 auf die Zwecke, die in Artikel 8 § 1 Nr. 1, 2 und 5 des Gesetzes vom 25. Dezember 2016 erwähnt sind, und sieht die vorherige Zustimmung des Prokurators des Königs durch einen mit Gründen versehenen schriftlichen Beschluss vor, der die Verhältnismäßigkeit der Maßnahme unter Berücksichtigung des Privatlebens und die Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe widerspiegelt; diese Maßnahme darf einen Monat ab dem Beschluss nicht überschreiten, unbeschadet einer Erneuerung.

In substanzieller Hinsicht ist die Regelung der vorherigen Zustimmung, die in Artikel 27 des Gesetzes vom 25. Dezember 2016 vorgesehen ist, unter Berücksichtigung des Urteils des Gerichtshofes der Europäischen Union in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022, auf das in B.59 hingewiesen wurde, dahin auszulegen, dass sie es erfordert, dass die Behörde, die auf einen mit Gründen versehenen Antrag der zuständigen Behörden die vorherige Kontrolle der Notwendigkeit der Zurverfügungstellung der PNR-Daten durchführt, in jedem Einzelfall das Vorliegen neuer Umstände und objektiver Anhaltspunkte, die entweder geeignet sind, den begründeten Verdacht einer Beteiligung dieser Person an schwerer Kriminalität zu wecken, die - zumindest mittelbar - einen objektiven Zusammenhang mit der Beförderung von Fluggästen aufweist, oder objektiver Anhaltspunkte dafür, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung terroristischer Straftaten, die einen solchen Zusammenhang aufweisen, leisten könnten, bewertet.

In dieser Weise ausgelegt, steht die von Artikel 27 des Gesetzes vom 25. Dezember 2016 vorgesehene Regelung in substanzieller Hinsicht mit den im Klagegrund erwähnten Bestimmungen im Einklang.

B.69.2. Was die Organisation betrifft, kann hingegen die Regelung in Artikel 27 des Gesetzes vom 25. Dezember 2016, die für gezielte Recherchen gilt und, wie in B.65.5 erwähnt, durch Artikel 20 desselben Gesetzes auf die Mitteilung von Daten nach Ablauf eines sechsmonatigen Zeitraums ausgedehnt wird, nicht so bewertet werden, dass die vorherige Kontrolle der Entscheidung über die Zurverfügungstellung einer « unabhängigen nationalen Behörde » übertragen wurde.

Zunächst kann die PNR-Zentralstelle, wie in B.68.3 erwähnt, nicht als eine « unabhängige nationale Behörde » angesehen werden, wenn sie auf Antrag von zuständigen Behörden Passagierdaten übermittelt.

Sodann sieht Artikel 46*septies* des Strafprozessgesetzbuches, der durch Artikel 50 des Gesetzes vom 25. Dezember 2016 eingefügt wurde und auf den Artikel 27 desselben Gesetzes verweist, zwar eine vorherige Beteiligung des Prokurators des Königs vor, aber gemäß dem vorerwähnten Artikel 46*septies* ist es Letzterer, der durch einen mit Gründen versehenen schriftlichen Beschluss selbst entscheidet, den Gerichtspolizeioffizier damit zu beauftragen, die PNR-Zentralstelle aufzufordern, die Passagierdaten gemäß Artikel 27 des Gesetzes vom 25. Dezember 2016 mitzuteilen. Zudem kann der Prokurator des Königs, da er mit der Ermittlung von Straftaten beauftragt ist, nicht als eine unabhängige nationale Behörde angesehen werden, die die vorherige Kontrolle der Zurverfügungstellung der Daten durchführt, wie es der Gerichtshof der Europäischen Union in Randnummer 244 seines vorerwähnten Urteils in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 verlangt.

Überdies ist festzustellen, dass Artikel 281 § 4 des am 18. Juli 1977 koordinierten allgemeinen Gesetzes über Zölle und Akzisen, der durch Artikel 6 des Gesetzes vom 2. Mai 2019 eingefügt wurde und auf den Artikel 27 des Gesetzes vom 25. Dezember 2016 in der durch dasselbe Gesetz vom 2. Mai 2019 abgeänderten Fassung verweist, vorsieht, dass der für die für Streitsachen zuständige Verwaltung bestimmte Generalberater durch einen mit Gründen versehenen schriftlichen Beschluss einen Bediensteten der Zoll- und Akzisenverwaltung damit beauftragen kann, die PNR-Zentralstelle aufzufordern, die Passagierdaten mitzuteilen. Was die Regelung betrifft, die in Artikel 16/3 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste, der durch Artikel 51 des Gesetzes vom 25. Dezember 2016 eingefügt wurde - der die Anforderungen des absolut Notwendigen überschreitet, wie der Gerichtshof in B.66 geurteilt hat - vorgesehen war, so sah er wiederum vor, dass die Nachrichten- und Sicherheitsdienste im Interesse der Ausübung ihrer Aufträge und ordnungsgemäß begründet beschließen konnten, auf die in Artikel 27 des Gesetzes vom 25. Dezember 2016 erwähnten Passagierdaten zuzugreifen.

Solche Verfahren, auf die Artikel 27 des Gesetzes vom 25. Dezember 2016 verweist, halten daher die Anforderung einer vorherigen Kontrolle vor der Zurverfügungstellung der Daten durch eine unabhängige Verwaltungsstelle, wie sind vom Gerichtshof der Europäischen Union in den Randnummern 244 bis 246 seines vorerwähnten Urteils in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 definiert wurde, nicht ein.

B.69.3. Insofern er die Zurverfügungstellung von PNR-Daten zum Zweck einer nachträglichen Überprüfung - außer in hinreichend begründeten Eilfällen - nicht einer vorherigen Kontrolle durch ein Gericht oder eine « unabhängige Verwaltungsstelle » auf einen mit Gründen versehenen Antrag der zuständigen Behörden unterwirft, verstößt Artikel 27 des Gesetzes vom 25. Dezember 2016 gegen die im Klagegrund erwähnten Bestimmungen.

B.69.4. Es ist Sache des Gesetzgebers, das Organ, das damit beauftragt wird, diese vorherige Kontrolle durchzuführen, unter Berücksichtigung dessen, was der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 sowohl in Bezug auf den Umfang der Kontrolle als auch in Bezug auf die Bedingungen der Unparteilichkeit und Unabhängigkeit des mit dieser Kontrolle beauftragten Organs entschieden hat, zu bestimmen.

B.69.5. Um bis zu diesem Eingreifen des Gesetzgebers die Mitteilung der PNR-Daten für die nachträgliche Überprüfung zu ermöglichen, ist davon auszugehen, dass die Datenschutzbehörde - die gemäß Artikel 4 § 2 Absatz 2 des Gesetzes vom 3. Dezember 2017 « zur Schaffung der Datenschutzbehörde » eine Restzuständigkeit bei der Verarbeitung von personenbezogenen Daten besitzt - eine « unabhängige Verwaltungsstelle » darstellt, die den vom Gerichtshof der Europäischen Union festgelegten Anforderungen an die Unparteilichkeit und Unabhängigkeit genügt.

Vor jeder Zurverfügungstellung von PNR-Daten für eine nachträgliche Überprüfung ist daher für die Anwendung von Artikel 27 des Gesetzes vom 25. Dezember 2016 vorher die Datenschutzbehörde unter Berücksichtigung des in B.69.1 Erwähnten und gegebenenfalls in Anlehnung an die von Artikel 46*septies* des Strafprozessgesetzbuches vorgesehene Regelung zu befassen.

B.70. Insofern er gegen Artikel 51 des Gesetzes vom 25. Dezember 2016 und gegen Artikel 27 des Gesetzes vom 25. Dezember 2016 gerichtet ist, insofern dieser die Zurverfügungstellung von PNR-Daten zum Zweck einer nachträglichen Überprüfung – außer in hinreichend begründeten Eilfällen – nicht einer vorherigen Kontrolle durch ein Gericht oder eine « unabhängige Verwaltungsstelle » auf einen mit Gründen versehenen Antrag der zuständigen Behörden unterwirft, ist der Klagegrund begründet.

Im Übrigen ist der Klagegrund, vorbehaltlich der in B.63.2.3, B.63.3.2, B.63.4.1, B.69.1 erwähnten Auslegungen und unter Berücksichtigung des in B.61.2.2 Erwähnten, insofern er gegen die Artikel 12 bis 16 und 24 bis 26 und 50 des Gesetzes vom 25. Dezember 2016 gerichtet ist, unbegründet.

5. *Die Aufbewahrungsdauer der PNR-Daten (Artikel* 18*).*

B.71. Die klagende Partei übt Kritik an Artikel 18 des Gesetzes vom 25. Dezember 2016, insofern die Frist von fünf Jahren, während der die PNR-Daten aufbewahrt werden, unverhältnismäßig sei.

B.72.1. Artikel 12 der PNR-Richtlinie mit der Überschrift « Speicherfrist und Depersonalisierung » bestimmt:

« 1. Die Mitgliedstaaten stellen sicher, dass die von den Fluggesellschaften an die PNR-Zentralstelle übermittelten PNR-Daten für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen beziehungsweise von dem er abgegangen ist, in einer bei dieser PNR-Zentralstelle angesiedelten Datenbank vorgehalten werden.

2. Nach Ablauf einer Frist von sechs Monaten ab Übermittlung der PNR-Daten gemäß Absatz 1 werden alle PNR-Daten durch Unkenntlichmachung der folgenden Datenelemente, mit denen die Identität des Fluggasts, auf den sich die PNR-Daten beziehen, unmittelbar festgestellt werden könnte, depersonalisiert:

a) Name(n), auch die Namen und die Zahl der im PNR-Datensatz verzeichneten mitreisenden Personen;

b) Anschrift und Kontaktdaten;

c) alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift, die zur unmittelbaren Feststellung der Identität des Fluggasts, zu dem die PNR-Daten erstellt wurden, oder anderer Personen beitragen könnten;

d) Vielflieger-Eintrag;

e) allgemeine Hinweise, die zur unmittelbaren Feststellung der Identität des Fluggastes beitragen könnten, zu dem die PNR-Daten erstellt wurden, und

f) jedwede erhobenen API-Daten.

3. Nach Ablauf der in Absatz 2 genannten Frist von sechs Monaten ist die Offenlegung der vollständigen PNR-Daten nur zulässig, wenn

a) berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Artikels 6 Absatz 2 Buchstabe b erforderlich ist und

b) dies genehmigt wird durch

i) eine Justizbehörde oder

ii) eine andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind, vorbehaltlich der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten.

4. Die Mitgliedstaaten stellen sicher, dass die PNR-Daten nach Ablauf der Frist nach Absatz 1 dauerhaft gelöscht werden. Diese Verpflichtung lässt Fälle unberührt, in denen bestimmte PNR-Daten an eine zuständige Behörde übermittelt wurden und im Zusammenhang mit einem konkreten Fall zum Zwecke der Verhütung, Aufdeckung, Ermittlung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität verwendet werden; in diesem Fall richtet sich die Frist für die Speicherung dieser Daten durch die zuständige Behörde nach nationalem Recht.

5. Die Ergebnisse der Verarbeitung nach Artikel 6 Absatz 2 Buchstabe a werden von der PNR-Zentralstelle nur so lange vorgehalten, wie dies erforderlich ist, um die zuständigen Behörden und die PNR-Zentralstellen anderer Mitgliedstaaten gemäß Artikel 9 Absatz 1 über einen Treffer zu informieren. Fällt die in Artikel 6 Absatz 5 genannte anschließende individuelle nicht-automatisierte Überprüfung eines Treffers bei der automatisierten Verarbeitung negativ aus, so kann dieses Ergebnis dennoch gespeichert werden, um künftige ' falsche ' Treffer zu vermeiden, solange die dazugehörigen Daten nicht gemäß Absatz 4 dieses Artikels gelöscht sind ».

Der Erwägungsgrund 25 der PNR-Richtlinie bestimmt:

« Der Zeitraum, für den die PNR-Daten vorgehalten werden sollen, sollte so lang sein, wie dies für den mit ihnen verfolgten Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten sowie schwerer Kriminalität erforderlich ist und in einem angemessenen Verhältnis dazu stehen. Das Wesen der PNR-Daten und ihr Verwendungszweck bringen es mit sich, dass diese so lange gespeichert werden müssen wie nötig, um sie auswerten und für Ermittlungen nutzen zu können. Um einen unverhältnismäßigen Rückgriff auf die Daten auszuschließen, sollten die PNR-Daten nach der anfänglichen Speicherfrist durch Unkenntlichmachung von Datenelementen depersonalisiert werden. Um das höchste Datenschutzniveau zu gewährleisten, sollte Zugriff auf die vollständigen PNR-Daten, die die unmittelbare Identifizierung der betroffenen Person ermöglichen, nach dieser anfänglichen Frist nur unter eingeschränkten, sehr strengen Bedingungen gewährt werden ».

B.72.2. Artikel 18 des Gesetzes vom 25. Dezember 2016 sieht vor, dass die Passagierdaten höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt werden und dass sie am Ende dieser Frist vernichtet werden.

Gemäß Artikel 21 § 1 des Gesetzes vom 25. Dezember 2016 stellt die PNR-Zentralstelle sicher, dass die Passagierdaten am Ende des in Artikel 18 erwähnten Zeitraums dauerhaft aus ihrer Datenbank gelöscht werden.

B.72.3. In den Vorarbeiten zum Gesetz vom 25. Dezember 2016 heißt es:

« 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. À 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, SS. 25-26).

B.72.4.1. Die in Artikel 18 des Gesetzes vom 25. Dezember 2016 vorgesehene Frist von fünf Jahren ist jedoch in Verbindung mit den Artikeln 19 ff. desselben Gesetzes zu betrachten, die ebenfalls die Modalitäten zur Aufbewahrung der Daten regeln.

B.72.4.2. Artikel 19 des Gesetzes vom 25. Dezember 2016 bestimmt:

« Nach Ablauf einer sechsmonatigen Frist ab der Speicherung der Passagierdaten in der Passagierdatenbank werden alle Passagierdaten durch Unkenntlichmachung folgender Datenelemente, mit denen die Identität des Passagiers, auf den sich die Daten beziehen, unmittelbar festgestellt werden könnte, depersonalisiert:

1. Name(n), auch die Namen anderer Passagiere, sowie Anzahl der mitreisenden Personen,

2. Anschrift und Kontaktangaben,

3. alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift, die zur unmittelbaren Feststellung der Identität des Passagiers oder jeglicher anderen Person beitragen könnten,

4. Informationen in Bezug auf Vielreisende,

5. allgemeine Hinweise, die zur unmittelbaren Feststellung der Identität des Passagiers beitragen könnten,

6. alle in Artikel 9 § 1 Nr. 18 erwähnten Daten ».

Diese Bestimmung ist in Verbindung mit Artikel 4 Nr. 14 des Gesetzes vom 25. Dezember 2016 zu betrachten, der die « Depersonalisierung durch Unkenntlichmachung von Datenelementen » als « die in Artikel 19 erwähnte Vorgehensweise, mit der diejenigen Datenelemente, mit denen die Identität der betreffenden Person unmittelbar festgestellt werden könnte, für einen Nutzer unsichtbar gemacht werden », definiert.

B.72.4.3. Wie in B.64.1 und B.65.5 erwähnt wurde, sieht Artikel 20 des Gesetzes vom 25. Dezember 2016 vor, dass nach Ablauf des in Artikel 19 erwähnten sechsmonatigen Zeitraums die Mitteilung der vollständigen Passagierdaten nur für die durch Artikel 27 vorgeschriebene Datenverarbeitung zugelassen ist, und auch nur unter den in dieser Bestimmung festgelegten Bedingungen.

Außerdem wird das in Artikel 24 erwähnte Ergebnis der Verarbeitung von der PNR-Zentralstelle nur solange aufbewahrt, wie dies erforderlich ist, um die zuständigen Behörden und gemäß Artikel 36 die PNR-Zentralstellen anderer Mitgliedstaaten der Europäischen Union über einen Treffer zu informieren (Artikel 21 § 3 Absatz 1).

B.72.4.4. Artikel 22 des Gesetzes vom 25. Dezember 2016 gewährleistet, dass der leitende Beamte und der Datenschutzbeauftragte nur Zugriff auf alle im Rahmen der Ausführung ihrer Aufträge relevanten Daten haben.

Schließlich wird die Datenverarbeitung protokolliert und hängt sie in direktem Zusammenhang mit den in Artikel 8 vorgesehenen Zwecken (Artikel 23 § 1). Die PNR-Zentralstelle sorgt für die Protokollierung, indem sie alle ihrer Zuständigkeit unterliegenden Verarbeitungssysteme und -verfahren während fünf Jahren dokumentiert (Artikel 23 § 2 Absatz 1).

B.73.1. Auf die Frage des Verfassungsgerichtshofes zur Aufbewahrungsdauer der PNR-Daten hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 erkannt:

« 249. Nach Art. 12 Abs. 1 und 4 dieser Richtlinie werden von der PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der betreffende Flug angekommen bzw. von dem er abgegangen ist, die von den Fluggesellschaften übermittelten PNR-Daten für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an diese Stelle in einer Datenbank vorgehalten und nach Ablauf dieses Zeitraums von fünf Jahren dauerhaft gelöscht.

250. Im 25. Erwägungsgrund der PNR-Richtlinie heißt es: ‘ Der Zeitraum, für den die PNR-Daten vorgehalten werden sollen, sollte so lang sein, wie dies für den mit ihnen verfolgten Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten sowie schwerer Kriminalität erforderlich ist, und in einem angemessenen Verhältnis dazu stehen. ’

251. Folglich ist die Speicherung von PNR-Daten nach Art. 12 Abs. 1 der PNR-Richtlinie nicht gerechtfertigt, wenn kein objektiver Zusammenhang zwischen dieser Speicherung und den mit der Richtlinie verfolgten Zielen der Bekämpfung terroristischer Straftaten und schwerer Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit der Beförderung von Fluggästen besteht.

252. Insoweit ist, wie sich aus dem 25. Erwägungsgrund der PNR-Richtlinie ergibt, zwischen der ursprünglichen Speicherfrist von sechs Monaten (Art. 12 Abs. 2 der Richtlinie) und dem Folgezeitraum (Art. 12 Abs. 3 der Richtlinie) zu unterscheiden.

253. Bei der Auslegung von Art. 12 Abs. 1 der PNR-Richtlinie sind die Bestimmungen in dessen Abs. 2 und 3 zu berücksichtigen, die die Speicherung der vorgehaltenen PNR-Daten und den Zugriff auf sie nach Ablauf der ursprünglichen Speicherfrist von sechs Monaten regeln. Wie aus dem 25. Erwägungsgrund der Richtlinie hervorgeht, kommt in diesen Bestimmungen zum einen das Ziel zum Ausdruck, sicherzustellen, dass die PNR-Daten ‘ so lange gespeichert werden ... wie nötig, um sie auswerten und für [die bereits während der ursprünglichen Speicherfrist von sechs Monaten durchführbaren] Ermittlungen nutzen zu können ’. Zum anderen sollen sie nach den Ausführungen im 25. Erwägungsgrund durch die Unkenntlichmachung der Daten ‘ einen unverhältnismäßigen Rückgriff ’ auf diese ausschließen und ‘ das höchste Datenschutzniveau ... gewährleisten ’, indem der Zugriff auf die Daten in einer Form, die eine unmittelbare Identifizierung der betroffenen Person ermöglicht, ‘ nach dieser anfänglichen Frist nur unter eingeschränkten, sehr strengen Bedingungen ’ gewährt wird; damit wird der Tatsache Rechnung getragen, dass der mit der Speicherung der PNR-Daten verbundene Eingriff umso schwerwiegender ist, je länger die Speicherung dauert.

254. Die Unterscheidung zwischen der ursprünglichen Speicherfrist von sechs Monaten (Art. 12 Abs. 2 der PNR-Richtlinie) und dem Folgezeitraum (Art. 12 Abs. 3 der Richtlinie) gilt aber auch für die nötige Beachtung der oben in Rn. 251 genannten Anforderung.

255. Während des ursprünglichen Zeitraums von sechs Monaten ist somit – angesichts der Ziele der PNR-Richtlinie und der Erfordernisse der Ermittlungs- und Verfolgungsmaßnahmen im Bereich terroristischer Straftaten und schwerer Kriminalität – davon auszugehen, dass die Speicherung der PNR-Daten aller Fluggäste, für die das durch die Richtlinie geschaffene System gilt, grundsätzlich auch dann nicht die Grenzen des absolut Notwendigen überschreitet, wenn es keine Anhaltspunkte für ihre Beteiligung an terroristischen Straftaten oder schwerer Kriminalität gibt, da sie es ermöglicht, die nötigen Recherchen zur Ermittlung von Personen anzustellen, die nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein.

256. Hinsichtlich des von Art. 12 Abs. 3 der PNR-Richtlinie erfassten Folgezeitraums steht die Speicherung der PNR-Daten aller Fluggäste, für die das durch die Richtlinie geschaffene System gilt - abgesehen davon, dass ihr aufgrund der großen Menge an Daten, die kontinuierlich gespeichert werden können, Risiken unverhältnismäßiger Nutzung und des Missbrauchs innewohnen (vgl. entsprechend Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 119) -, dagegen im Widerspruch zu dem im 25. Erwägungsgrund der Richtlinie aufgestellten Erfordernis, wonach der Zeitraum, in dem die PNR-Daten vorgehalten werden, nur so lang sein sollte, wie es für den mit ihnen verfolgten Zweck erforderlich ist, und in einem angemessenen Verhältnis dazu stehen sollte, da der Unionsgesetzgeber das höchste Datenschutzniveau für PNR-Daten schaffen wollte, die eine unmittelbare Identifizierung der betroffenen Personen ermöglichen.

257. Im Fall von Fluggästen, bei denen weder die Vorabüberprüfung nach Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie noch etwaige Überprüfungen während der in Art. 12 Abs. 2 dieser Richtlinie genannten Frist von sechs Monaten oder irgendein anderer Umstand objektive Anhaltspunkte geliefert haben, die eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit ihrer Flugreise belegen können, ist nämlich unter solchen Umständen kein auch nur mittelbarer Zusammenhang zwischen den PNR-Daten dieser Fluggäste und dem mit der Richtlinie verfolgten Ziel ersichtlich, der die Speicherung der Daten rechtfertigen würde (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 204 und 205).

258. Die kontinuierliche Speicherung der PNR-Daten sämtlicher Fluggäste nach dem ursprünglichen Zeitraum von sechs Monaten beschränkt sich somit nicht auf das absolut Notwendige (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 206).

259. Gibt es in besonderen Fällen objektive Anhaltspunkte - wie bei den PNR-Daten der Fluggäste, die zu einem überprüften Treffer geführt haben - dafür, dass von bestimmten Fluggästen eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität ausgehen könnte, erscheint eine Speicherung ihrer PNR-Daten über den ursprünglichen Zeitraum hinaus jedoch zulässig (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 207 und die dort angeführte Rechtsprechung).

260. Das Vorliegen dieser objektiven Anhaltspunkte wäre nämlich geeignet, einen Zusammenhang mit den Zielen herzustellen, die mit den Verarbeitungen gemäß der PNR-Richtlinie verfolgt werden, so dass die Speicherung der PNR-Daten dieser Fluggäste während des nach der Richtlinie maximal zulässigen Zeitraums von fünf Jahren gerechtfertigt wäre.

261. Da die im Ausgangsverfahren in Rede stehenden Rechtsvorschriften offenbar eine allgemeine Speicherfrist der PNR-Daten von fünf Jahren vorsehen, die unterschiedslos für alle Fluggäste gilt, einschließlich derjenigen, bei denen weder die Vorabüberprüfung nach Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie noch etwaige Überprüfungen während des ursprünglichen Zeitraums von sechs Monaten oder irgendein anderer Umstand objektive Anhaltspunkte geliefert haben, die eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität belegen können, verstoßen diese Rechtsvorschriften im Licht der Art. 7 und 8 sowie von Art. 52 Abs. 1 der Charta gegen Art. 12 Abs. 1 der Richtlinie, es sei denn, sie können in einer mit diesen Bestimmungen vereinbaren Weise ausgelegt werden; dies zu prüfen ist Sache des vorlegenden Gerichts.

262. In Anbetracht der vorstehenden Erwägungen ist auf die achte Frage zu antworten, dass Art. 12 Abs. 1 der PNR-Richtlinie in Verbindung mit den Art. 7 und 8 sowie mit Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er nationalen Rechtsvorschriften entgegensteht, die eine allgemeine Speicherfrist der PNR-Daten von fünf Jahren vorsehen, die unterschiedslos für alle Fluggäste gilt, einschließlich derjenigen, bei denen weder die Vorabüberprüfung nach Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie noch etwaige Überprüfungen während des in Art. 12 Abs. 2 der Richtlinie genannten Zeitraums von sechs Monaten oder irgendein anderer Umstand objektive Anhaltspunkte geliefert haben, die eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität mit einem - zumindest mittelbaren - objektiven Zusammenhang mit der Reise der Fluggäste belegen können ».

B.73.2. Aus diesem Urteil geht hervor, dass in Bezug auf die Aufbewahrungsdauer der PNR-Daten zwischen der ursprünglichen Speicherfrist von sechs Monaten (Artikel 12 Absatz 2 der Richtlinie) und dem Folgezeitraum (Artikel 12 Absatz 3 der Richtlinie) zu unterscheiden ist (Randnr. 252): Zwar überschreitet die Speicherung der PNR-Daten aller Passagiere, für die das durch die Richtlinie geschaffene System gilt, während der ursprünglichen Frist von sechs Monaten grundsätzlich auch dann nicht die Grenzen des absolut Notwendigen, wenn es keine Anhaltspunkte für ihre Beteiligung an terroristischen Straftaten oder schwerer Kriminalität gibt, da sie es ermöglicht, die nötigen Recherchen zur Ermittlung von Personen anzustellen, die nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein (Randnr. 255), aber die Speicherung der PNR-Daten aller Passagiere, für die das durch die Richtlinie geschaffene System gilt, über diese ursprüngliche Frist von sechs Monaten hinaus, überschreitet die Grenzen des absolut Notwendigen, insbesondere aufgrund der großen Menge an Daten, die kontinuierlich gespeichert werden können, der Risiken unverhältnismäßiger Nutzung und des Missbrauchs (Randnr. 256).

Im Fall von Passagieren, bei denen weder die Vorabüberprüfung nach Artikel 6 Absatz 2 Buchstabe *a)* der PNR-Richtlinie noch etwaige Überprüfungen während der in Artikel 12 Absatz 2 dieser Richtlinie genannten Frist von sechs Monaten oder irgendein anderer Umstand objektive Anhaltspunkte geliefert haben, die eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit ihrer Reise belegen können, ist nämlich unter solchen Umständen kein auch nur mittelbarer Zusammenhang zwischen den PNR-Daten dieser Passagiere und dem mit der Richtlinie verfolgten Ziel ersichtlich, der die Speicherung der Daten rechtfertigen würde (Randnr. 257).

Der Gerichtshof der Europäischen Union überlässt es dem vorlegenden Gericht zu prüfen, ob das Gesetz vom 25. Dezember 2016 so ausgelegt werden kann, dass es den Anforderungen der Artikel 7 und 8 der Charta der Grundrechte in Verbindung mit Artikel 52 Absatz 1 der Charta entspricht (Randnr. 261).

B.74.1. Wie in B.72.2 erwähnt, sieht Artikel 18 des Gesetzes vom 25. Dezember 2016 vor, dass die Passagierdaten höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt werden und dass sie am Ende dieser Frist vernichtet werden.

Diese Bestimmung beschränkt sich darauf, eine maximale Aufbewahrungsdauer festzulegen, ohne die Daten zu nennen, die während dieser maximalen Dauer gespeichert werden sollen.

Artikel 18 des Gesetzes vom 25. Dezember 2016 kann deshalb dahin ausgelegt werden, dass nach der ursprünglichen Frist von sechs Monaten ab der Erfassung der Passagierdaten in der Passagierdatenbank nur die Daten von Personen während einer Dauer von fünf Jahren in der Passagierdatenbank aufbewahrt werden, für die entweder die Vorabüberprüfung nach Artikel 6 Absatz 2 Buchstabe *a)* der PNR-Richtlinie oder etwaige Überprüfungen während der in Artikel 12 Absatz 2 dieser Richtlinie genannten Frist von sechs Monaten oder irgendein anderer Umstand objektive Anhaltspunkte geliefert haben, die eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Reise dieser Passagiere belegen können.

Die Daten, bei denen diese Auslegung nicht eingehalten werden kann, müssen vernichtet werden.

B.74.2. In der in B.74.1 erwähnten Auslegung überschreitet Artikel 18 des Gesetzes vom 25. Dezember 2016 nicht die Anforderungen des absolut Notwendigen.

B.75. Vorbehaltlich der in B.74.1 erwähnten Auslegung, ist der Klagegrund, insofern er gegen Artikel 18 des Gesetzes vom 25. Dezember 2016 gerichtet ist, unbegründet.

In Bezug auf den zweiten Klagegrund

B.76. Der zweite, hilfsweise vorgebrachte Klagegrund ist aus einem Verstoß abgeleitet gegen Artikel 22 der Verfassung in Verbindung mit Artikel 3 Absatz 2 des Vertrags über die Europäische Union und Artikel 45 der Charta der Grundrechte der Europäischen Union. Dieser Klagegrund richtet sich gegen Artikel 3 § 1, Artikel 8 § 2 und Kapitel 11, das die Artikel 28 bis 31 umfasst, des Gesetzes vom 25. Dezember 2016.

Die klagende Partei ist der Ansicht, dass mit den angefochtenen Bestimmungen durch die Ausweitung des PNR-Systems auf Flüge innerhalb der EU mittelbar wieder Grenzkontrollen eingeführt würden, die gegen die Freizügigkeit verstoßen würden.

B.77.1. Artikel 3 § 1 des Gesetzes vom 25. Dezember 2016 bestimmt:

« Vorliegendes Gesetz bestimmt die Verpflichtungen der Beförderungsunternehmen und Reiseunternehmen in Bezug auf die Übermittlung von Daten zu Passagieren, die in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet befördert werden ».

B.77.2. In Bezug auf den Anwendungsbereich des Gesetzes vom 25. Dezember 2016 heißt es in den Vorarbeiten:

« 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 » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-2069/001, S. 7).

B.77.3. Wie bereits erwähnt, ist die Ausweitung des PNR-Systems auf EU-Flüge nach dem Erwägungsgrund 10 der PNR-Richtlinie zulässig. Artikel 2 der PNR-Richtlinie regelt das Verfahren, um den Anwendungsbereich auszudehnen.

In seinem Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 hat der Gerichtshof der Europäischen Union diesbezüglich darauf hingewiesen, dass die Ausdehnung des « PNR »-Systems auf EU-Flüge eine Befugnis der Mitgliedstaaten darstellt, die Anwendung des durch diese Richtlinie geschaffenen Systems auf EU-Flüge auszudehnen (Randnr. 162) und die Kommission hat, wie in B.36.4.1 erwähnt, festgestellt, dass alle Mitgliedstaaten mit einer Ausnahme von dieser Befugnis Gebrauch gemacht haben.

B.77.4. Bezüglich der Umsetzung dieser Befugnis hat der Gerichtshof der Europäischen Union in seinem Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 erkannt:

« 274. Zunächst ist in Art. 45 der Charta die Freizügigkeit verankert, die im Übrigen eine der Grundfreiheiten des Binnenmarkts darstellt (vgl. in diesem Sinne Urteil vom 22. Juni 2021, *Ordre des barreaux francophones et germanophone u. a.* [Präventive Maßnahmen im Hinblick auf eine Ausweisung], C-718/19, EU:C:2021:505, Rn. 54).

275. Dieser Artikel gewährleistet in Abs. 1 das Recht jedes Unionsbürgers, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten. Dieses Recht, entspricht nach den Erläuterungen zur Charta der Grundrechte (*ABl.* 2007, C 303, S. 17) dem in Art. 20 Abs. 2 Unterabs. 1 Buchst. a AEUV garantierten Recht und wird gemäß Art. 20 Abs. 2 Unterabs. 2 AEUV und Art. 52 Abs. 2 der Charta unter den Bedingungen und innerhalb der Grenzen ausgeübt, die in den Verträgen und durch die in Anwendung der Verträge erlassenen Maßnahmen festgelegt sind.

276. Sodann bietet die Union nach Art. 3 Abs. 2 EUV ihren Bürgerinnen und Bürgern einen Raum der Freiheit, der Sicherheit und des Rechts ohne Binnengrenzen, in dem der freie Personenverkehr gewährleistet ist, in Verbindung mit dem Erlass geeigneter Maßnahmen u. a. in Bezug auf die Kontrollen an den Außengrenzen sowie die Verhütung und Bekämpfung der Kriminalität. Desgleichen stellt die Union nach Art. 67 Abs. 2 AEUV sicher, dass Personen an den Binnengrenzen nicht kontrolliert werden, und entwickelt eine gemeinsame Politik u. a. im Bereich der Kontrollen an den Außengrenzen.

277. Nach ständiger Rechtsprechung des Gerichtshofs stellt eine nationale Regelung, durch die bestimmte Angehörige eines Mitgliedstaats allein deswegen benachteiligt werden, weil sie von ihrer Freiheit, sich in einen anderen Mitgliedstaat zu begeben und sich dort aufzuhalten, Gebrauch gemacht haben, eine Beschränkung der Freiheiten dar, die Art. 45 Abs. 1 der Charta jedem Unionsbürger zuerkennt (vgl. in diesem Sinne, zu Art. 21 Abs. 1 AEUV, Urteile vom 8. Juni 2017, *Freitag*, C-541/15, EU:C:2017:432, Rn. 35 und die dort angeführte Rechtsprechung, sowie vom 19. November 2020, *ZW*, C-454/19, EU:C:2020:947, Rn. 30)..

278. Nationale Rechtsvorschriften wie die im Ausgangsverfahren in Rede stehenden, mit denen das in der PNR-Richtlinie vorgesehene System nicht nur auf Drittstaatsflüge, sondern gemäß Art. 2 Abs. 1 der Richtlinie auch auf EU-Flüge sowie, über den Inhalt dieser Bestimmung hinaus, auf Beförderungen mit anderen Mitteln innerhalb der Union angewandt wird, haben zur Folge, dass die PNR-Daten aller mit diesen Mitteln innerhalb der Union beförderten Personen systematisch und kontinuierlich übermittelt und verarbeitet werden.

279. Wie oben in den Rn. 98 bis 111 festgestellt, führen die Übermittlung und Verarbeitung der Daten der Fluggäste von Drittstaatsflügen und von EU-Flügen aufgrund des durch die PNR-Richtlinie geschaffenen Systems zu fraglos schwerwiegenden Eingriffen in die in den Art. 7 und 8 der Charta verankerten Grundrechte der betroffenen Personen. Die Schwere eines solchen Eingriffs erhöht sich noch, wenn die Anwendung dieses Systems auf andere Beförderungsmittel innerhalb der Union ausgedehnt wird. Solche Eingriffe sind aus den in den genannten Randnummern dargelegten Gründen zudem geeignet, die Staatsangehörigen der Mitgliedstaaten, die solche Rechtsvorschriften vorsehen, und allgemein die Unionsbürger, die diese Beförderungsmittel für Reisen innerhalb der Union aus den oder in die betreffenden Mitgliedstaaten nutzen, zu benachteiligen und infolgedessen davon abzuhalten, von ihrer Freizügigkeit im Sinne von Art. 45 der Charta Gebrauch zu machen, so dass die betreffenden Rechtsvorschriften zu einer Beschränkung dieser Grundfreiheit führen.

280. Nach ständiger Rechtsprechung kann eine Beschränkung der Freizügigkeit nur gerechtfertigt sein, wenn sie auf objektiven Erwägungen beruht und in angemessenem Verhältnis zu dem mit dem nationalen Recht in legitimer Weise verfolgten Ziel steht. Eine Maßnahme ist verhältnismäßig, wenn sie zur Erreichung des verfolgten Ziels geeignet ist und nicht über das hinausgeht, was dafür notwendig ist (vgl. in diesem Sinne Urteil vom 5. Juni 2018, *Coman u. a.*, C-673/16, EU:C:2018:385, Rn. 41 und die dort angeführte Rechtsprechung).

281. Hinzuzufügen ist, dass eine nationale Maßnahme, die geeignet ist, die Ausübung der Freizügigkeit zu behindern, nur dann gerechtfertigt sein kann, wenn sie mit den durch die Charta verbürgten Grundrechten vereinbar ist, deren Beachtung der Gerichtshof sichert (Urteil vom 14. Dezember 2021, *Stolichna obshtina, rayon ' Pancharevo '*, C-490/20, EU:C:2021:1008, Rn. 58 und die dort angeführte Rechtsprechung).

282. Insbesondere kann nach der oben in den Rn. 115 und 116 angeführten Rechtsprechung eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne dem Umstand Rechnung zu tragen, dass sie mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen wird. Insoweit ist die Möglichkeit für die Mitgliedstaaten, eine Einschränkung des durch Art. 45 Abs. 1 der Charta garantierten Grundrechts zu rechtfertigen, zu beurteilen, indem die Schwere des mit einer solchen Einschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die mit ihr verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht.

283. Wie oben in Rn. 122 ausgeführt, ist das mit der PNR-Richtlinie verfolgte Ziel der Bekämpfung terroristischer Straftaten und schwerer Kriminalität unzweifelhaft eine dem Gemeinwohl dienende Zielsetzung der Union.

284. In Bezug auf die Frage, ob nationale Rechtsvorschriften, die zur Umsetzung der PNR-Richtlinie erlassen wurden und mit denen das in dieser Richtlinie vorgesehene System auf EU-Flüge und andere Beförderungsmittel innerhalb der Union ausgedehnt wird, zur Erreichung des verfolgten Ziels geeignet sind, geht aus den dem Gerichtshof vorliegenden Akten hervor, dass die Heranziehung der PNR-Daten es gestattet, Personen zu ermitteln, die nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die genauer überprüft werden sollten, so dass solche Rechtsvorschriften zur Erreichung des angestrebten Ziels der Bekämpfung terroristischer Straftaten und schwerer Kriminalität geeignet erscheinen.

285. Was die Erforderlichkeit solcher Rechtsvorschriften betrifft, muss sich die Ausübung der in Art. 2 Abs. 1 der PNR-Richtlinie vorgesehenen Befugnis durch die Mitgliedstaaten im Licht der Art. 7 und 8 der Charta auf das in Anbetracht der oben in den Rn. 163 bis 174 genannten Anforderungen zur Erreichung dieses Ziels absolut Notwendige beschränken.

286. Diese Anforderungen gelten erst recht, wenn das in der PNR-Richtlinie vorgesehene System auf andere Beförderungsmittel innerhalb der Union angewandt wird ».

B.77.5. Wie der Verfassungsgerichtshof in B.40 geurteilt hat, rechtfertigt die tatsächliche terroristische Bedrohung angesichts insbesondere der geografischen Lage des Landes, die Anwendung des PNR-Systems auf verschiedene Beförderungsmittel innerhalb der Grenzen der Union.

Aus denselben Gründen ist anzunehmen, dass die Einschränkung der Freizügigkeit, die das Gesetz vom 25. Dezember 2016 mit sich bringen würde, durch den Umstand gerechtfertigt ist, dass das auf EU-Flüge angewandte und auf andere Beförderungsmittel ausgedehnte PNR-System dem Ziel der Bekämpfung terroristischer Straftaten und schwerer Kriminalität dient, das die PNR-Richtlinie verfolgt und das zweifellos ein Allgemeininteresse der Union ist, und dass dieses PNR-System nicht die Grenzen des absolut Notwendigen überschreitet.

B.77.6. Insofern der Klagegrund gegen Artikel 3 § 1 des Gesetzes vom 25. Dezember 2016 gerichtet ist, ist er unbegründet.

B.78.1. Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016 gestattet es, die PNR-Daten unter den in Kapitel 11 (Artikel 28 bis 31) des Gesetzes vom 25. Dezember 2016 vorgesehenen Bedingungen zu verarbeiten, um die Personenkontrollen an den Außengrenzen zu verbessern und insbesondere um die illegale Einwanderung zu bekämpfen.

B.78.2.1. Auf die Frage des Verfassungsgerichtshofes zum Anwendungsbereich der « API »-Richtlinie hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 erkannt:

« 263. Mit Buchst. a seiner neunten Frage möchte das vorlegende Gericht wissen, ob die API-Richtlinie gemessen an Art. 3 Abs. 2 EUV und Art. 45 der Charta gültig ist, ausgehend von der Prämisse, dass die mit dieser Richtlinie eingeführten Verpflichtungen für EU-Flüge gelten.

264. Wie der Generalanwalt in Nr. 277 seiner Schlussanträge ausgeführt hat und wie der Rat, die Kommission und mehrere Regierungen dargelegt haben, ist diese Prämisse falsch.

265. Art. 3 Abs. 1 der API-Richtlinie sieht nämlich vor, dass die Mitgliedstaaten die erforderlichen Schritte unternehmen müssen, um die Beförderungsunternehmen zu verpflichten, auf Anfrage der mit der Durchführung der Personenkontrollen an den Außengrenzen beauftragten Behörden bei Abschluss des Check-in die Angaben über die Personen zu übermitteln, die sie zu einer zugelassenen Grenzübergangsstelle befördern werden, über die diese Personen in das Hoheitsgebiet eines Mitgliedstaats einreisen werden. Diese Daten werden nach Art. 6 Abs. 1 der Richtlinie an die mit der Durchführung von Kontrollen an den Außengrenzen, über die die beförderte Person in dieses Hoheitsgebiet einreisen wird, beauftragten Behörden übermittelt und werden unter den in dieser Bestimmung vorgesehenen Bedingungen verarbeitet.

266. Aus diesen Bestimmungen geht im Licht der Definitionen der Begriffe ‘ Beförderungsunternehmen ’, ‘ Außengrenzen ’ und ‘ Grenzübergangsstelle ’ in Art. 2 Buchst. a, b und d der API-Richtlinie klar hervor, dass die Richtlinie die Luftfahrtunternehmen zur Übermittlung der in ihrem Art. 3 Abs. 2 genannten Daten an die mit der Durchführung von Kontrollen an den Außengrenzen, über die die beförderte Person in dieses Hoheitsgebiet einreisen wird, beauftragten Behörden nur für Flüge verpflichtet, bei denen die Fluggäste zu einem für das Überschreiten der Außengrenzen der Mitgliedstaaten zu Drittstaaten zugelassenen Übergang befördert werden, und nur für die Verarbeitung der diese Flüge betreffenden Daten.

267. Dagegen erlegt die Richtlinie keine Verpflichtung in Bezug auf Fluggastdatensätze bei Flügen auf, die nur Binnengrenzen zwischen den Mitgliedstaaten überschreiten.

268. Hinzuzufügen ist, dass dadurch, dass die PNR-Richtlinie, wie aus ihrem neunten Erwägungsgrund und ihrem Art. 8 Abs. 2 hervorgeht, die von Art. 3 Abs. 2 der API-Richtlinie erfassten, im Einklang mit dieser Richtlinie erhobenen und von bestimmten Fluggesellschaften vorgehaltenen Daten in die PNR-Daten einbezieht und dass die PNR-Richtlinie den Mitgliedstaaten in ihrem Art. 2 die Befugnis einräumt, sie auf die von den Mitgliedstaaten festgelegten EU-Flüge anzuwenden, weder die Tragweite der Bestimmungen der API-Richtlinie noch die sich aus ihr ergebenden Beschränkungen geändert werden.

269. Nach alledem ist auf Buchst. a der neunten Frage zu antworten, dass die API-Richtlinie dahin auszulegen ist, dass sie nicht für EU-Flüge gilt ».

B.78.2.2. Aus dem Vorstehenden geht hervor, dass der Gerichtshof der Europäischen Union bestätigt, dass dadurch, dass die PNR-Richtlinie die API-Daten in die PNR-Daten einbezieht, weder die Tragweite der Bestimmungen der API-Richtlinie noch die sich aus ihr ergebenden Beschränkungen geändert werden; diese ist dahin auszulegen, dass sie nicht für EU-Flüge gilt [...]. Wie in B.54.2 erwähnt, urteilt der Gerichtshof der Europäischen Union nämlich, dass die Verarbeitung von API-Daten nur Passagiere betreffen darf, die die Außengrenzen der Union zu Drittstaaten überschreiten, da sie ansonsten die gleiche Wirkung wie Kontrollen an den Außengrenzen zu Drittstaaten hätte (Randnr. 290).

B.78.3. Es ist außerdem die Randnummer 235 des vorerwähnten Urteils in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 zu berücksichtigen, mit der der Gerichtshof der Europäischen Union erkennt, dass « aus dem abschließenden Charakter der in Art. 1 Abs. 2 der PNR-Richtlinie genannten Ziele [folgt], dass die PNR-Daten auch nicht in einer einheitlichen Datenbank gespeichert werden dürfen, die zur Verfolgung sowohl dieser als auch anderer Ziele konsultiert werden kann. Die Speicherung dieser Daten in einer solchen Datenbank brächte nämlich die Gefahr einer Verwendung der Daten zu anderen als den in Art. 1 Abs. 2 genannten Zwecken mit sich ».

Wie in B.54.2 erwähnt, hat der Gerichtshof der Europäischen Union im Übrigen mit dem Argument der Unvereinbarkeit einer einheitlichen Datenbank mit den Anforderungen des absolut Notwendigen geurteilt, dass die Verarbeitung von PNR-Daten zu anderen als den von der PNR-Richtlinie vorgesehenen Zwecken, insbesondere zur Verbesserung der Grenzkontrollen und zur Bekämpfung illegaler Einwanderung, die abschließende Beschaffenheit der Aufzählung der mit der Verarbeitung der PNR-Daten verfolgten Ziele missachtet (Randnr. 288), die die Mitgliedstaaten daran hindert, eine einheitliche Datenbank zu errichten, die sowohl die gemäß der PNR-Richtlinie erhobenen PNR-Daten enthält als auch die in Artikel 3 Absatz 2 der API-Richtlinie genannten Daten, insbesondere wenn diese Datenbank nicht nur zur Verfolgung der in Artikel 1 Absatz 2 der PNR-Richtlinie genannten Zwecke konsultiert werden kann, sondern auch zur Verfolgung anderer Zwecke (Randnr. 289).

B.78.4. Hinsichtlich der Existenz einer einheitlichen Datenbank, die sowohl die PNR-Daten als auch die API-Daten enthält, ist es nicht möglich, den Anwendungsbereich der Artikel 28 bis 31 des Gesetzes vom 25. Dezember 2016 in einer Weise auszulegen, die mit dem Unionsrecht vereinbar wäre.

B.78.5. Indem sie im Rahmen des « PNR »-Systems die Verarbeitung der API-Daten, die in Artikel 9 § 1 Nr. 18 des Gesetzes vom 25. Dezember 2016 erwähnt sind, für EU-Flüge zulassen, verstoßen die Artikel 28 bis 31, die das Kapitel 11 des Gesetzes vom 25. Dezember 2016 bilden, gegen die im Klagegrund erwähnten Bestimmungen und sind für nichtig zu erklären. Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016, der untrennbar mit diesen Bestimmungen verbunden ist, ist ebenfalls für nichtig zu erklären.

B.78.6. Es obliegt dem Gesetzgeber, die Erhebung der API-Daten in einer von der PNR-Datenbank getrennten Datenbank und gemäß Bedingungen zu regeln, mit denen die Zwecke, die Einschränkungen und der Anwendungsbereich der Pflichten, die sich aus der API-Richtlinie ergeben, eingehalten werden.

B.79. Der Klagegrund ist begründet, insofern er gegen die Artikel 8 § 2 und 28 bis 31 des Gesetzes vom 25. Dezember 2016 gerichtet ist.

In Bezug auf die Tragweite der Nichtigerklärung

B.80.1. Der Verfassungsgerichtshof hat die Klagegründe für begründet erklärt, insoweit sie sich beziehen auf

- Artikel 8 § 1 Nr. 4 und Artikel 8 § 2 des Gesetzes vom 25. Dezember 2016,

- Artikel 27 des Gesetzes vom 25. Dezember 2016, insofern er die Zurverfügungstellung von PNR-Daten zum Zweck einer nachträglichen Überprüfung - außer in hinreichend begründeten Eilfällen - nicht einer vorherigen Kontrolle durch ein Gericht oder eine « unabhängige Verwaltungsstelle » auf einen mit Gründen versehenen Antrag der zuständigen Behörden unterwirft,

- die Artikel 28 bis 31 des Gesetzes vom 25. Dezember 2016 und

- Artikel 51 des Gesetzes vom 25. Dezember 2016.

B.80.2. Die vorerwähnten Bestimmungen sind folglich in dem Maße für nichtig zu erklären, in dem die Klagegründe begründet sind.

B.81.1. Diese Nichtigerklärung hat zur Folge, dass die Bestimmungen des Gesetzes vom 25. Dezember 2016 oder andere gesetzliche Bestimmungen, die auf die für nichtig erklärten Bestimmungen verweisen, in diesem Maße ihren Gegenstand verlieren.

B.81.2. Diese Nichtigerklärung hat auch zur Folge, dass die Datenverarbeitungen, die auf der Grundlage von für nichtig erklärten Zwecken durchgeführt wurden, oder die Zurverfügungstellungen von Daten, die ohne vorherige Kontrolle durchgeführt wurden, als unrechtmäßig anzusehen sind.

Die Identifizierung von unrechtmäßigen Verarbeitungen ist möglich, da Artikel 23 § 1 des Gesetzes vom 25. Dezember 2016 vorsieht, dass die Datenverarbeitung protokolliert wird, was in Artikel 4 Nr. 11 desselben Gesetzes definiert ist als « de[r] in Artikel 23 § 2 erwähnten Mechanismus, durch den die Rückverfolgbarkeit der durchgeführten Datenverarbeitungen ermöglicht wird, damit es möglich ist, die Person, die Daten abgefragt hat, die abgefragten Daten, den Zeitpunkt und den Zweck dieses Abfragens zu identifizieren ».

Diese Protokollierung ermöglicht es somit, die Verarbeitungen zu identifizieren, die das « absolut Notwendige » überschreiten.

B.81.3. Im Übrigen beeinträchtigt diese teilweise Nichtigerklärung des Gesetzes vom 25. Dezember 2016 nicht die anderen Verarbeitungen von Passagierdaten.

In Bezug auf die Aufrechterhaltung der Folgen

B.82.1. Artikel 8 Absatz 6 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof bestimmt:

« Wenn der Verfassungsgerichtshof es für notwendig erachtet, gibt er im Wege einer allgemeinen Verfügung die Folgen der für nichtig erklärten Bestimmungen an, die als endgültig zu betrachten sind oder für die von ihm festgelegte Frist vorläufig aufrechterhalten werden ».

B.82.2. Der Gerichtshof muss diesbezüglich die Einschränkungen berücksichtigen, die sich aus dem Recht der Europäischen Union bezüglich der Aufrechterhaltung der Folgen innerstaatlicher Normen, die für nichtig zu erklären sind, weil sie im Widerspruch zu diesem Recht stehen, ergeben (EuGH, Große Kammer, 8. September 2010, C-409/06, *Winner Wetten*, ECLI:EU:C:2010:503, Randnrn. 53-69; EuGH, Große Kammer, 28. Februar 2012, C-41/11, *Inter-Environnement Wallonie und Terre wallonne*, ECLI:EU:C:2012:103, Randnrn. 56-63).

In der Regel kann diese Aufrechterhaltung der Folgen nur unter den Bedingungen geschehen, die durch den Europäischen Gerichtshof in der Antwort auf eine Vorabentscheidungsfrage festgelegt werden.

B.83.1. Auf die Frage des Gerichtshofs zu einer etwaigen Aufrechterhaltung der Folgen des angefochtenen Gesetzes hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil in Sachen *Ligue des droits humains gegen Ministerrat* vom 21. Juni 2022 erkannt:

« 293. Der Grundsatz des Vorrangs des Unionsrechts besagt, dass das Unionsrecht dem Recht der Mitgliedstaaten vorgeht. Dieser Grundsatz verpflichtet daher alle mitgliedstaatlichen Stellen, den verschiedenen Bestimmungen des Unionsrechts volle Wirksamkeit zu verschaffen, wobei das Recht der Mitgliedstaaten die diesen Bestimmungen zuerkannte Wirkung im Hoheitsgebiet dieser Staaten nicht beeinträchtigen darf. Nach diesem Grundsatz ist ein nationales Gericht, das im Rahmen seiner Zuständigkeit die Bestimmungen des Unionsrechts anzuwenden hat und nationale Rechtsvorschriften nicht im Einklang mit den Anforderungen des Unionsrechts auslegen kann, verpflichtet, für die volle Wirksamkeit dieser Bestimmungen Sorge zu tragen, indem es erforderlichenfalls jede - auch spätere - entgegenstehende Vorschrift des nationalen Rechts aus eigener Entscheidungsbefugnis unangewendet lässt, ohne dass es die vorherige Beseitigung dieser Vorschrift auf gesetzgeberischem Weg oder durch irgendein anderes verfassungsrechtliches Verfahren beantragen oder abwarten müsste (Urteile vom 15. Juli 1964, *Costa*, 6/64, EU:C:1964:66, S. 1270 und 1271, vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 214 und 215, sowie vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 118).

294. Nur der Gerichtshof kann ausnahmsweise und aus zwingenden Erwägungen der Rechtssicherheit eine vorübergehende Aussetzung der Verdrängungswirkung herbeiführen, die eine unionsrechtliche Vorschrift gegenüber mit ihr unvereinbarem nationalem Recht ausübt. Eine solche zeitliche Beschränkung der Wirkungen einer Auslegung des Unionsrechts durch den Gerichtshof kann nur in dem Urteil vorgenommen werden, in dem über die erbetene Auslegung entschieden wird. Der Vorrang und die einheitliche Anwendung des Unionsrechts würden beeinträchtigt, wenn nationale Gerichte befugt wären, nationalen Bestimmungen, sei es auch nur vorübergehend, Vorrang vor dem Unionsrecht einzuräumen, gegen das sie verstoßen (Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 119 und die dort angeführte Rechtsprechung).

295. Anders als das Fehlen einer das Verfahren betreffenden Verpflichtung wie der vorherigen Umweltverträglichkeitsprüfung eines Projekts, um die es in der Rechtssache ging, in der das Urteil vom 29. Juli 2019, *Inter-Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen* (C-411/17, EU:C:2019:622, Rn. 175, 176, 179 und 181), ergangen ist, in der der Gerichtshof eine vorübergehende Aussetzung der Verdrängungswirkung gebilligt hat, kann ein Verstoß gegen die Bestimmungen der PNR-Richtlinie im Licht der Art. 7, 8 und 45 sowie von Art. 52 Abs. 1 der Charta nicht Gegenstand einer Legalisierung im Wege eines vergleichbaren Verfahrens wie in dieser Rechtssache sein. Würden die Wirkungen nationaler Rechtsvorschriften wie des Gesetzes vom 25. Dezember 2016 aufrechterhalten, würde dies nämlich bedeuten, dass durch die betreffenden Rechtsvorschriften den Luftfahrtunternehmen, anderen Beförderungsunternehmen und Reiseunternehmen weiterhin Verpflichtungen auferlegt würden, die gegen das Unionsrecht verstoßen und mit schwerwiegenden Eingriffen in die Grundrechte der Personen verbunden sind, deren Daten übermittelt, gespeichert und verarbeitet wurden, sowie mit Beschränkungen der Freizügigkeit dieser Personen, die über das erforderliche Maß hinausgehen (vgl. entsprechend Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 122 und die dort angeführte Rechtsprechung).

296. Das vorlegende Gericht darf somit die ihm nach nationalem Recht obliegende Feststellung der Rechtswidrigkeit der im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften nicht in ihren zeitlichen Wirkungen beschränken (vgl. entsprechend Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 123 und die dort angeführte Rechtsprechung).

297. Soweit das vorlegende Gericht schließlich wissen möchte, wie sich die Feststellung einer etwaigen Unvereinbarkeit des Gesetzes vom 25. Dezember 2016 mit den Bestimmungen der PNR-Richtlinie im Licht der Charta auf die Zulässigkeit und die Auswertung der Beweise und Informationen, die mittels der von den betreffenden Beförderungs- und Reiseunternehmen übermittelten Daten erlangt wurden, im Rahmen von Strafverfahren auswirkt, genügt es, auf die dazu ergangene Rechtsprechung des Gerichtshofs zu verweisen, insbesondere auf die in den Rn. 41 bis 44 des Urteils vom 2. März 2021, *Prokuratuur* (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152), angeführten Grundsätze, aus denen sich ergibt, dass diese Zulässigkeit nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten dem nationalen Recht unterliegt, vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität (vgl. entsprechend Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 127).

298. Nach alledem ist auf die zehnte Frage zu antworten, dass das Unionsrecht dahin auszulegen ist, dass es ein nationales Gericht daran hindert, die Wirkungen einer ihm nach nationalem Recht obliegenden Feststellung der Rechtswidrigkeit nationaler Rechtsvorschriften, die - in einer Weise, die im Licht von Art. 3 Abs. 2 EUV, Art. 67 Abs. 2 AEUV sowie der Art. 7, 8 und 45 und von Art. 52 Abs. 1 der Charta mit den Bestimmungen der PNR-Richtlinie unvereinbar ist - den Beförderungsunternehmen des Luft-, Schienen- und Landwegs und den Reiseunternehmen die Übermittlung von PNR-Daten vorschreiben sowie eine Verarbeitung und Speicherung dieser Daten vorsehen, zeitlich zu beschränken. Die Zulässigkeit der in dieser Weise erlangten Beweise unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten dem nationalen Recht, vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität ».

B.83.2. Aus dem vorerwähnten Urteil geht hervor, dass der Gerichtshof die Folgen der für nichtig erklärten Bestimmungen nicht vorläufig aufrechterhalten darf.

Wie in B.81 erwähnt, stellt diese begrenzte Nichtigerklärung nicht die Verarbeitungen in Frage, die gemäß den in den Klagegründen geltend gemachten Verfassungs- und Vertragsbestimmungen durchgeführt wurden.

B.83.3. Es obliegt dem zuständigen Strafrichter, gegebenenfalls gemäß Artikel 32 des einleitenden Titels des Strafprozessgesetzbuches und im Lichte der vom Gerichtshof der Europäischen Union im vorerwähnten Urteil vom 21. Juni 2022 angegebenen Präzisierungen über die Zulässigkeit von Beweisen zu befinden, die bei der Umsetzung der für nichtig erklärten Bestimmungen gesammelt wurden.

Aus diesen Gründen:

Der Gerichtshof

- erklärt Artikel 8 § 1 Nr. 4 und § 2 des Gesetzes vom 25. Dezember 2016 « über die Verarbeitung von Passagierdaten » für nichtig;

- erklärt Artikel 27 des vorerwähnten Gesetzes vom 25. Dezember 2016, insofern er die Zurverfügungstellung von PNR-Daten zum Zweck einer nachträglichen Überprüfung - außer in hinreichend begründeten Eilfällen - nicht einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle auf einen mit Gründen versehenen Antrag der zuständigen Behörden unterwirft, für nichtig;

- erklärt die Artikel 28 bis 31 des vorerwähnten Gesetzes vom 25. Dezember 2016 für nichtig;

- erklärt Artikel 16/3 des Gesetzes vom 30. November 1998 « über die Nachrichten- und Sicherheitsdienste », eingefügt durch Artikel 51 des vorerwähnten Gesetzes vom 25. Dezember 2016, für nichtig;

- weist die Klage vorbehaltlich der in B.33.2 bis B.33.5, B.49, B.63.2.3, B.63.3.2, B.63.4.1, B.69.1 und B.74.1 erwähnten Auslegungen und unter Berücksichtigung des in B.40.3.2, in B.40.3.3 und in B.61.2.2 Erwähnten im Übrigen zurück;

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 12. Oktober 2023.

Der Kanzler, Der Präsident,
F. Meersschaut P. Nihoul