ARRÊT DE LA COUR (grande chambre)
21 juin 2022 (*)
Table des matières

« Renvoi préjudiciel – Traitement des données à caractère personnel – Données des dossiers passagers (PNR) – Règlement (UE) 2016/679 – Article 2, paragraphe 2, sous d) – Champ d'application – Directive (UE) 2016/681 – Utilisation des données PNR des passagers des vols aériens opérés entre l'Union européenne et des pays tiers – Faculté d'inclure les données des passagers des vols aériens opérés au sein de l'Union – Traitements automatisés de ces données – Délai de conservation – Lutte contre les infractions terroristes et les formes graves de criminalité – Validité – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 21 ainsi qu'article 52, paragraphe 1 – Législation nationale étendant l'application du système PNR à d'autres transports opérés au sein de l'Union – Liberté de circulation au sein de l'Union – Charte des droits fondamentaux – Article 45 »

Dans l'affaire C-817/19,
ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par la Cour constitutionnelle (Belgique), par décision du 17 octobre 2019, parvenue à la Cour le 31 octobre 2019, dans la procédure
Ligue des droits humains
contre
Conseil des ministres,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, MM. A. Arabadjiev, S. Rodin, I. Jarukaitis et N. Jääskinen, présidents de chambre, MM. T. von Danwitz (rapporteur), M. Safjan, F. Biltgen, P. G. Xuereb, N. Piçarra, M^me^ L. S. Rossi, MM. A. Kumin et N. Wahl, juges,
avocat général : M. G. Pitruzzella,
greffier : M^me^ M. Krausenböck, administratrice,
vu la procédure écrite et à la suite de l'audience du 13 juillet 2021,
considérant les observations présentées :

pour la Ligue des droits humains, par M^e^ C. Forget, avocate,

pour le gouvernement belge, par MM. P. Cottin, J.-C. Halleux, M^mes^ C. Pochet et M. Van Regemorter, en qualité d'agents, assistés de M^e^ C. Caillet, advocaat, de M^e^ E. Jacubowitz, avocat, ainsi que de M. G. Ceuppens, M^me^ V. Dethy et M. D. Vertongen,

pour le gouvernement tchèque, par M^me^ T. Machovičová, MM. O. Serdula, M. Smolek et J. Vláčil, en qualité d'agents,

pour le gouvernement danois, par MM. M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen et M^me^ M. Søndahl Wolff, en qualité d'agents,

pour le gouvernement allemand, par MM. D. Klebs et J. Möller, en qualité d'agents,

pour le gouvernement estonien, par M^me^ N. Grünberg, en qualité d'agent,

pour l'Irlande, par M^me^ M. Browne, M. A. Joyce et M^me^ J. Quaney, en qualité d'agents, assistés de M. D. Fennelly, BL,

pour le gouvernement espagnol, par M. L. Aguilera Ruiz, en qualité d'agent,

pour le gouvernement français, par M. D. Dubois, M^me^ E. de Moustier et M. T. Stehelin, en qualité d'agents,

pour le gouvernement chypriote, par M^me^ E. Neofytou, en qualité d'agent,

pour le gouvernement letton, par M. E. Bārdiņš, M^mes^ K. Pommere et V. Soņeca, en qualité d'agents,

pour le gouvernement néerlandais, par M^mes^ M. K. Bulterman, A. Hanje, M. J. Langer et M^me^ C. S. Schillemans, en qualité d'agents,

pour le gouvernement autrichien, par MM. G. Kunnert, A. Posch et M^me^ J. Schmoll, en qualité d'agents,

pour le gouvernement polonais, par M. B. Majczyna, en qualité d'agent,

pour le gouvernement slovaque, par M^me^ B. Ricziová, en qualité d'agent,

pour le gouvernement finlandais, par M^mes^ A. Laine et H. Leppo, en qualité d'agents,

pour le Parlement européen, par M^mes^ O. Hrstková Šolcová et P. López-Carceller, en qualité d'agents,

pour le Conseil de l'Union européenne, par M. J. Lotarski, M^me^ N. Rouam, MM. E. Sitbon et C. Zadra, en qualité d'agents,

pour la Commission européenne, par MM. D. Nardi et M. Wasmeier, en qualité d'agents,

pour le Contrôleur européen de la protection des données, par M. P. Angelov, M^mes^ A. Buchta, F. Coudert et C.-A. Marnier, en qualité d'agents,

pour l'Agence des droits fondamentaux de l'Union européenne, par M^me^ L. López, MM. T. Molnar, M. Nespor et M. O'Flaherty, en qualité d'agents,
ayant entendu l'avocat général en ses conclusions à l'audience du 27 janvier 2022,
rend le présent

Arrêt

La demande de décision préjudicielle porte, en substance :

sur l'interprétation de l'article 2, paragraphe 2, sous d), et de 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) (JO 2016, L 119, p. 1, ci-après le « RGPD »), de la directive 2004/82/CE du Conseil, du 29 avril 2004, concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO 2004, L 261, p. 24, ci-après la « directive API »), ainsi que de 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 (JO 2010, L 283, p. 1) ;

sur l'interprétation et la validité, au regard des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), de l'article 3, point 4, des articles 6 et 12 ainsi que de l'annexe I de 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 (JO 2016, L 119, p. 132, ci-après la « directive PNR »), ainsi que

sur l'interprétation et la validité, au regard de l'article 3, paragraphe 2, TUE et de l'article 45 de la Charte, de la directive API.

Cette demande a été présentée dans le cadre d'un litige opposant la Ligue des droits humains au Conseil des ministres (Belgique) au sujet de la légalité de la loi du 25 décembre 2016, relative au traitement des données des passagers.

I. Le cadre juridique

A. Le droit de l'Union

1. La directive 95/46/CE

La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31), a été abrogée, avec effet au 25 mai 2018, par le RGPD. L'article 3, paragraphe 2, de cette directive disposait :

« La présente directive ne s'applique pas au traitement de données à caractère personnel :

mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »

2. La directive API

Les considérants 1, 7, 9 et 12 de la directive API prévoient :

Pour lutter efficacement contre l'immigration clandestine et améliorer les contrôles aux frontières, il est essentiel que tous les États membres se dotent d'un dispositif fixant les obligations des transporteurs aériens qui acheminent des passagers sur le territoire des États membres. Il convient également, pour tendre vers cet objectif avec une plus grande efficacité, d'harmoniser autant que possible les sanctions pécuniaires prévues par les États membres en cas de violation des obligations qui incombent aux transporteurs, en tenant compte des différences entre les systèmes et pratiques juridiques des États membres.

[...]

Les obligations qui doivent être imposées aux transporteurs en vertu de la présente directive sont complémentaires de celles établies en application des dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 signée en 1990, complétées par la directive 2001/51/CE du Conseil, [du 28 juin 2001, visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985 (JO 2001, L 187, p. 45),] étant donné que ces deux types d'obligations concourent à la réalisation du même objectif, à savoir la maîtrise des flux migratoires et la lutte contre l'immigration clandestine.

Pour lutter plus efficacement contre l'immigration clandestine et pour tendre vers cet objectif avec une plus grande efficacité, il est indispensable, sans préjudice des dispositions de la directive [95/46], de tenir compte, dès que l'occasion se présente, de toute innovation technologique, surtout pour ce qui est de l'intégration et de l'utilisation des caractéristiques biométriques dans les informations qu'il incombe aux transporteurs de transmettre.

La directive [95/46] s'applique en ce qui concerne le traitement des données à caractère personnel par les autorités des États membres. Cela signifie que, s'il est vrai que le traitement des données transmises concernant les passagers, effectué aux fins des contrôles aux frontières, serait légitime également dans le but de permettre l'utilisation de ces données comme élément de preuve dans des procédures visant à l'application des lois et des règlements sur l'entrée et l'immigration, notamment des dispositions relatives à la protection de l'ordre public et de la sécurité nationale, tout autre traitement de ces données qui serait incompatible avec ces objectifs irait, en revanche, à l'encontre du principe énoncé à l'article 6, paragraphe 1, point b), de la directive [95/46]. Les États membres devraient prévoir un régime de sanctions qui s'appliquerait en cas d'utilisation incompatible avec les objectifs visés par la présente directive. »

L'article 1er de la directive API, intitulé « Objectif », prévoit :

« La présente directive vise à améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine, au moyen de la transmission préalable aux autorités nationales compétentes, par les transporteurs, de données relatives aux passagers. »

L'article 2 de cette directive, intitulé « Définitions », énonce :

fins de la présente directive, on entend par :

"transporteur", toute personne physique ou morale qui assure, à titre professionnel, le transport de personnes par voie aérienne ;

"frontières extérieures", les frontières extérieures des États membres avec des pays tiers ;

"contrôle frontalier", un contrôle effectué à la frontière exclusivement lorsqu'il y a intention de franchir cette frontière, indépendamment de toute autre considération ;

"point de passage frontalier", tout point de passage autorisé par les autorités compétentes pour le franchissement des frontières extérieures ;

"données à caractère personnel", "traitement de données à caractère personnel" et "fichier de données à caractère personnel", ce que l'on entend par ces termes à l'article 2 de la directive [95/46]. »

L'article 3 de ladite directive**,** intitulé « Transmission de données », dispose, à ses paragraphes 1 et 2 :

« 1. Les États membres prennent 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.
Parmi ces renseignements figurent :
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. »

L'article 6 de la directive API, intitulé « Traitement des données », énonce :
« 1. Les données relatives aux personnes visées à l'article 3, paragraphe 1, sont transmises aux autorités chargées d'effectuer le contrôle des personnes aux frontières extérieures par lesquelles le passager entrera sur le territoire d'un État membre, afin de faciliter l'exécution de ce contrôle dans le but de lutter plus efficacement contre l'immigration clandestine.
Les États membres veillent à ce que ces données soient recueillies par les transporteurs et transmises par voie électronique ou, en cas d'échec, par tout autre moyen approprié aux autorités chargées d'effectuer les contrôles au point de passage frontalier autorisé par lequel le passager entrera sur le territoire d'un État membre. Les autorités chargées d'effectuer le contrôle des personnes aux frontières extérieures conservent les données dans un fichier temporaire.
Une fois que les passagers sont entrés, les autorités visées à l'alinéa précédent effacent les données dans les vingt-quatre heures qui suivent la transmission, à moins qu'elles ne soient nécessaires ultérieurement pour permettre aux autorités chargées d'effectuer les contrôles sur les personnes aux frontières extérieures d'exercer leurs pouvoirs réglementaires conformément au droit national et sous réserve des dispositions relatives à la protection des données figurant dans la directive [95/46].
Les États membres prennent les mesures nécessaires afin d'établir l'obligation, pour les transporteurs, d'effacer, dans les vingt-quatre heures suivant l'arrivée du moyen de transport visé à l'article 3, paragraphe 1, les données à caractère personnel qu'ils ont recueillies et transmises aux autorités chargées du contrôle aux frontières aux fins de la présente directive.
Conformément à leur droit interne et sous réserve des dispositions relatives à la protection des données figurant dans la directive [95/46], les États membres peuvent également faire usage des données à caractère personnel visées à l'article 3, paragraphe 1, pour répondre aux besoins des services répressifs.
2. Les États membres prennent les mesures nécessaires afin d'établir l'obligation, pour les transporteurs, d'informer les passagers conformément aux dispositions de la directive [95/46]. Cette obligation porte également sur les informations visées à l'article 10, point c), et à l'article 11, paragraphe 1, point c), de ladite directive. »

3. La directive 2010/65

La directive 2010/65 est abrogée, en vertu de l'article 25 du règlement (UE) 2019/1239 du Parlement européen et du Conseil, du 20 juin 2019, établissant un système de guichet unique maritime européen et abrogeant la directive 2010/65 (JO 2019, L 198, p. 64), à compter du 15 août 2025.

Le considérant 2 de cette directive énonce :
« Dans le but de faciliter les transports maritimes et de réduire la charge administrative pesant sur les compagnies maritimes, il est nécessaire de simplifier et d'harmoniser autant que possible les formalités déclaratives prévues par les actes juridiques de l'Union et par les États membres. [...] »

L'article 1er de ladite directive, intitulé « Objet et champ d'application », dispose, à ses paragraphes 1 et 2 :
« 1. La présente 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.
2. La présente directive s'applique aux formalités déclaratives applicables aux transports maritimes pour les navires à l'entrée ou à la sortie des ports situés dans les États membres. »

Aux termes de l'article 8 de la même directive, intitulé « Confidentialité » :
« 1. Les États membres, conformément aux actes juridiques applicables de l'Union ou au droit des États membres, prennent les mesures nécessaires pour garantir la confidentialité des renseignements à caractère commercial, ou autres renseignements de nature confidentielle, échangés au titre de la présente directive.
2. Les États membres veillent en particulier à assurer la protection des données à caractère commercial collectées au titre de la présente directive. Concernant les données à caractère personnel, les États membres s'assurent du respect de la directive [95/46]. Les institutions et organes de l'Union [européenne] veillent à se conformer au règlement (CE) no 45/2001 [du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO 2001, L 8, p. 1)]. »

4. Le RGPD

Le considérant 19 du RGPD énonce :
« 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[, 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 (JO 2016, L 119, p. 89)]. Les États membres peuvent confier à des autorités compétentes au sens de la [directive 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.
[...] »

L'article 2 de ce règlement, intitulé « Champ d'application matériel », dispose, à ses paragraphes 1 et 2 :
« 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 :
dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ;
par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ;
[...]
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. »

L'article 4 dudit règlement, intitulé « Définitions », prévoit :
« Aux fins du présent règlement, on entend par :
"données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable [...] ;
"traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

L'article 23 du RGPD, intitulé « Limitations », 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 :
la sécurité nationale ;
la défense nationale ;
la sécurité publique ;
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 ;

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) ;
2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant :
aux finalités du traitement ou des catégories de traitement ;
aux catégories de données à caractère personnel ;
à l'étendue des limitations introduites ;
aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
à la détermination du responsable du traitement ou des catégories de responsables du traitement ;
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 ;
aux risques pour les droits et libertés des personnes concernées ; et
au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation. »

L'article 94 de ce règlement, intitulé « Abrogation de la directive [95/46] », prévoit :
« 1. La directive [95/46] est abrogée avec effet au 25 mai 2018.
2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive [95/46] s'entendent comme faites au comité européen de la protection des données institué par le présent règlement. »

5. La directive 2016/680

La directive 2016/680 a, conformément à son article 59, abrogé et remplacé, à compter du 6 mai 2018, la décision-cadre 2008/977/JAI du Conseil, du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO 2008, L 350, p. 60).

Aux termes des considérants 9 à 11 de la directive 2016/680 :

Sur cette base, le [RGPD] définit des règles générales visant à protéger les personnes physiques à l'égard du traitement des données à caractère personnel et à garantir la libre circulation des données dans l'Union.

Dans la déclaration n° 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée à l'acte final de la Conférence intergouvernementale qui a adopté le traité de Lisbonne, la conférence a reconnu que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 [TFUE] pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines.

Il convient dès lors que ces domaines soient régis par une directive qui fixe les 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 la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, en respectant la nature spécifique de ces activités. 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 [RGPD] s'applique. Par conséquent, le [RGPD] 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 [RGPD] 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. »

L'article 1er de cette directive, intitulé « Objet et objectifs », qui correspond en substance à l'article 1er de la décision-cadre 2008/977, prévoit, à son paragraphe 1 :

« 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 3 de ladite directive, intitulé « Définitions », dispose :

« Aux fins de la présente directive, on entend par :

[...]

7. "autorité compétente" :

toute autorité publique compétente pour 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 ; ou

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 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 ;

[...] »

6. La directive PNR

Les considérants 4 à 12, 15, 19, 20, 22, 25, 27, 28, 33, 36 et 37 de la directive PNR énoncent :

La directive [API] régit la transmission aux autorités nationales compétentes, par les transporteurs aériens, d'informations préalables relatives aux passagers (ci-après dénommées "données API"), en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration illégale.

Les objectifs de la présente directive sont, entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes.

L'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire 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, et donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels.

L'évaluation 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 avant cette évaluation et qui devraient être soumises à un examen plus approfondi par les autorités compétentes. 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. Par ailleurs, les critères d'évaluation devraient être définis d'une manière qui réduise au minimum le nombre d'identifications erronées de personnes innocentes par le système.

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.

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.

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, il est essentiel que tous les États membres adoptent des dispositions obligeant les transporteurs aériens qui assurent des vols extra-UE à transférer les données PNR qu'ils recueillent, y compris les données API. Les États membres devraient également avoir la possibilité d'étendre cette obligation aux transporteurs aériens qui assurent des vols intra-UE. Ces dispositions devraient s'entendre sans préjudice de la directive [API].

Le traitement des données à caractère personnel devrait être proportionné aux objectifs de sécurité spécifiques poursuivis par la présente directive.

La définition des infractions terroristes appliquée dans le cadre de la présente directive devrait être la même que celle figurant dans la décision-cadre 2002/475/JAI du Conseil[, du 13 juin 2002, relative à la lutte contre le terrorisme (JO 2002, L 164, p. 3)]. La définition des formes graves de criminalité devrait englober les catégories d'infractions énumérées à l'annexe II de la présente directive.

Une liste des données PNR à transmettre à une [unité d'information passagers désignée (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], la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après dénommée "convention n^{o} 108") et la convention [européenne] de sauvegarde des droits de l'homme et des libertés fondamentales[, signée à Rome le 4 novembre 1950 (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.

Chaque État membre devrait être responsable de l'évaluation des menaces potentielles liées aux infractions terroristes et aux formes graves de criminalité.

En tenant pleinement compte du droit à la protection des données à caractère personnel et du droit à la non-discrimination, aucune décision qui produit des effets juridiques préjudiciables à une personne ou l'affecte de manière significative ne devrait être prise sur la seule base du traitement automatisé des données PNR. Par ailleurs, conformément aux articles 8 et 21 de la Charte, aucune décision de cette nature ne devrait introduire de discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. La Commission [européenne] devrait également prendre en compte ces principes lors du réexamen de l'application de la présente directive.

En tenant pleinement compte des principes mis en évidence par la récente jurisprudence pertinente de la Cour de justice de l'Union européenne, l'application de la présente directive devrait garantir le plein respect des droits fondamentaux et du droit au respect de la vie privée ainsi que du principe de proportionnalité. Elle devrait aussi véritablement remplir les objectifs de nécessité et de proportionnalité afin de répondre aux intérêts généraux reconnus par l'Union et à la nécessité de protéger les droits et libertés d'autrui dans la lutte contre les infractions terroristes et les formes graves de criminalité. L'application de la présente directive devrait être dûment justifiée et les garanties nécessaires devraient être mises en place afin d'assurer la légalité de tout stockage, de toute analyse, de tout transfert ou de toute utilisation des données 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. 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.

Dans chaque État membre, le traitement de données PNR effectué par l'UIP et par les autorités compétentes devrait être soumis à une norme de protection des données à caractère personnel du droit national conforme à la décision-cadre [2008/977] et aux exigences spécifiques de protection des données énoncées dans la présente directive. Les références à la décision-cadre [2008/977] devraient s'entendre comme des références faites à la législation actuellement en vigueur ainsi qu'à la législation qui la remplacera.

Compte tenu du droit à la protection des données à caractère personnel, il convient que les droits des personnes concernées en ce qui concerne le traitement de leurs données PNR, tels que les droits d'accès, de rectification, d'effacement et de limitation, ainsi que le droit à réparation et le droit à un recours juridictionnel, soient conformes à la décision-cadre [2008/977] et au niveau de protection élevé conféré par la Charte et la CEDH.

La présente directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne, sous réserve que ce droit national respecte le droit de l'Union.

La présente directive respecte les droits fondamentaux et les principes énoncés dans la Charte, en particulier le droit à la protection des données à caractère personnel, le droit au respect de la vie privée et le droit à la non-discrimination consacrés par ses articles 8, 7 et 21 ; elle devrait dès lors être mise en œuvre en conséquence. La présente directive est compatible avec les principes de la protection des données et ses dispositions sont conformes à la décision-cadre [2008/977]. En outre, afin de respecter le principe de proportionnalité, la présente directive prévoit, pour des points spécifiques, des règles de protection des données plus strictes que celles prévues dans la décision-cadre [2008/977].

Le champ d'application de la présente directive est aussi limité que possible dès lors que : il prévoit que la conservation des données PNR dans les UIP est autorisée pendant une période n'excédant pas cinq ans au terme de laquelle les données devraient être effacées ; il prévoit que les données sont dépersonnalisées par le masquage d'éléments des données après une période initiale de six mois ; et il interdit la collecte et l'utilisation des données sensibles. Pour garantir l'efficacité et un niveau élevé de protection des données, les États membres sont tenus de veiller à ce qu'une autorité de contrôle nationale indépendante et, notamment, un délégué à la protection des données soient chargés de fournir des conseils et de surveiller la manière dont les données PNR sont traitées. Tout traitement de données PNR devrait être consigné ou faire l'objet d'une trace documentaire à des fins de vérification de sa licéité et d'autocontrôle et pour garantir de manière adéquate l'intégrité des données et la sécurité du traitement. Les États membres devraient également veiller à ce que les passagers reçoivent des informations claires et précises sur la collecte des données PNR et sur leurs droits. »

L'article 1er de la directive PNR, intitulé « Objet et champ d'application », énonce :

« 1. La présente directive prévoit :

le transfert, par les transporteurs aériens, de données des dossiers des passagers (PNR) de vols extra-UE ;

le traitement des données visées au point a), notamment leur collecte, leur utilisation et leur conservation par les États membres et leur échange entre les États membres.

2. 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 2 de cette directive, intitulé « Application de la présente directive aux vols intra-UE », est libellé comme suit :

« 1. Si un État membre décide d'appliquer la présente directive aux vols intra-UE, il le notifie à la Commission par écrit. Un État membre peut adresser ou révoquer une telle notification à tout moment. La Commission publie cette notification et la révocation éventuelle de celle-ci au *Journal officiel de l'Union européenne*.

2. Lorsqu'une notification visée au paragraphe 1 est adressée, toutes les dispositions de la présente 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.

3. Un État membre peut décider d'appliquer la présente directive uniquement à certains vols intra-UE. Lorsqu'il prend une telle décision, l'État membre sélectionne les vols qu'il juge nécessaires afin de poursuivre les objectifs de la présente directive. L'État membre peut décider à tout moment de modifier la sélection des vols intra-UE. »

L'article 3 de ladite directive, intitulé « Définitions », dispose :

Aux fins de la présente directive, on entend par :

"transporteur aérien", une entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de passagers ;

"vol extra-UE", tout vol, régulier ou non, effectué par un transporteur aérien en provenance d'un pays tiers et devant atterrir sur le territoire d'un État membre ou en provenance du territoire d'un État membre et devant atterrir dans un pays tiers, y compris, dans les deux cas, les vols comportant d'éventuelles escales sur le territoire d'États membres ou de pays tiers ;

" vol intra-UE ", tout vol, régulier ou non, effectué par un transporteur aérien en provenance du territoire d'un État membre et devant atterrir sur le territoire d'un ou de plusieurs États membres, sans escale sur le territoire d'un pays tiers ;

"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 un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers ;

"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 ;

"système de réservation", le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations ;

"méthode push", la méthode par laquelle les transporteurs aériens transfèrent les données PNR énumérées à l'annexe I vers la base de données de l'autorité requérante ;

"infractions terroristes", les infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre [2002/475] ;

"formes graves de criminalité", 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 ;

"dépersonnaliser par le masquage d'éléments des données", rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée. »

L'article 4 de la directive PNR, intitulé « Unité d'informations passagers », énonce, à ses paragraphes 1 à 3 :

« 1. 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.

2. L'UIP est chargée :

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 ;

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.

3. Les membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes. Les États membres dotent les UIP des ressources adéquates pour l'accomplissement de leurs missions. »

L'article 5 de cette directive, intitulé « Délégué à la protection des données au sein de l'UIP », est libellé comme suit :

« 1. L'UIP nomme un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes.

2. Les États membres dotent les délégués à la protection des données des moyens pour accomplir leurs missions et obligations, conformément au présent article, de manière effective et en toute indépendance.

3. Les États membres veillent à ce que la personne concernée ait le droit de s'adresser au délégué à la protection des données, en sa qualité de point de contact unique, pour toutes les questions relatives au traitement des données PNR la concernant. »

L'article 6 de ladite directive, intitulé « Traitement des données 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 :

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 ;

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

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 :

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

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.

[...]

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[, du 29 avril 2004, relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n^{o} 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO 2004, L 158, p. 77)]. En outre, lorsque des évaluations sont réalisées pour des vols intra-UE entre des États membres auxquels s'applique le règlement (CE) n^{o} 562/2006 du Parlement européen et du Conseil[, du 15 mars 2006, établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO 2006, L 105, p. 1)], les conséquences de ces évaluations doivent respecter ledit règlement. »

Aux termes de l'article 7 de la directive PNR, intitulé « Autorités compétentes » :

« 1. Chaque État membre arrête une liste des autorités compétentes habilitées à demander aux UIP ou à recevoir de celles-ci des données PNR ou le résultat du traitement de telles données en vue de procéder à un examen plus approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière.

2. Les autorités visées au paragraphe 1 sont des autorités compétentes en matière de prévention ou de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes ou de poursuites en la matière.

[...]

4. Les données PNR et le résultat du traitement de ces données reçus par l'UIP ne peuvent faire l'objet d'un traitement ultérieur par les autorités compétentes des États membres 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.

5. Le paragraphe 4 s'applique sans préjudice des compétences des autorités répressives ou judiciaires nationales, lorsque d'autres infractions, ou des indices d'autres infractions, sont détectés dans le cadre d'actions répressives menées à la suite de ce traitement.

6. Les autorités compétentes ne peuvent prendre 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. Ces décisions ne peuvent pas être fondées 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. »

L'article 8 de cette directive, intitulé « Obligations imposées aux transporteurs aériens concernant les transferts de données », prévoit, à ses paragraphes 1 à 3 :

« 1. Les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent, par la "méthode push", les données PNR énumérées à l'annexe I, pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités, vers la base de données de l'UIP de l'État membre sur le territoire duquel le vol atterrira ou du territoire duquel il décollera. Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR de tous les passagers du vol incombe au transporteur aérien qui assure le vol. Lorsqu'un vol extra-UE comporte une ou plusieurs escales dans des aéroports des États membres, les transporteurs aériens transfèrent les données PNR de tous les passagers aux UIP de tous les États membres concernés. Il en est de même lorsqu'un vol intra-UE comporte une ou plusieurs escales dans les aéroports de différents États membres, mais uniquement en ce qui concerne les États membres qui recueillent les données PNR des vols intra-UE.

2. Dans l'hypothèse où les transporteurs aériens ont recueilli des [données API] énumérées à l'annexe I, point 18, mais ne les conservent pas par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent également ces données, par la "méthode push", à l'UIP des États membres visés au paragraphe 1. Dans le cas d'un tel transfert, toutes les dispositions de la présente directive s'appliquent à ces données API.

3. Les transporteurs aériens transfèrent les données PNR par voie électronique au moyen de protocoles communs et de formats de données reconnus à adopter en conformité avec la procédure d'examen visée à l'article 17, paragraphe 2, ou, en cas de défaillance technique, par tout autre moyen approprié garantissant un niveau de sécurité des données approprié :

24 à 48 heures avant l'heure de départ programmée du vol ; et

immédiatement après la clôture du vol, c'est-à-dire dès que les passagers ont embarqué à bord de l'aéronef prêt à partir et qu'ils ne peuvent plus embarquer ou débarquer. »

L'article 12 de ladite directive, 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 :

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 ;

l'adresse et les coordonnées ;

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 ;

les informations "grands voyageurs" ;

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

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 :

lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b) ; et

lorsqu'elle a été approuvée par :

une autorité judiciaire ; ou

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. »

L'article 13 de la directive PNR, intitulé « Protection des données à caractère personnel », énonce, à ses paragraphes 1 à 5 :

« 1. Chaque État membre veille à ce que, pour tout traitement de données à caractère personnel effectué au titre de la présente directive, chaque passager dispose du même droit à la protection de ses données à caractère personnel, des mêmes droits d'accès, de rectification, d'effacement et de limitation, et droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union et le droit national et en application des articles 17, 18, 19 et 20 de la décision-cadre [2008/977]. Lesdits articles sont par conséquent applicables.

2. Chaque État membre veille à ce que les dispositions adoptées en droit national en application des articles 21 et 22 de la décision-cadre [2008/977] concernant la confidentialité du traitement et la sécurité des données s'appliquent également à tous les traitements de données à caractère personnel effectués en vertu de la présente directive.

3. La présente directive est sans préjudice de l'applicabilité de la directive [95/46] au traitement des données à caractère personnel par les transporteurs aériens, en particulier en ce qui concerne leurs obligations de prendre des mesures techniques et organisationnelles appropriées pour protéger la sécurité et la confidentialité des données à caractère personnel.

4. Les États membres interdisent 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. Dans l'hypothèse où l'UIP reçoit des données PNR révélant de telles informations, elle les efface immédiatement.

5. Les États membres veillent à ce que l'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous leur responsabilité. Cette documentation comprend au minimum :

le nom et les coordonnées de l'organisation et du personnel chargés du traitement des données PNR au sein de l'UIP et les différents niveaux d'autorisation d'accès ;

les demandes formulées par les autorités compétentes et les UIP d'autres États membres ;

toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci. »

Selon l'article 15 de cette directive, intitulé « Autorité de contrôle nationale » :

« 1. Chaque État membre prévoit que l'autorité de contrôle nationale visée à l'article 25 de la décision-cadre [2008/977] est chargée de fournir des conseils sur l'application, sur son territoire, des dispositions adoptées par

les États membres en vertu de la présente directive et de surveiller l'application de celles-ci. L'article 25 de ladite décision-cadre s'applique.

2. Ces autorités de contrôle nationales exercent les activités au titre du paragraphe 1 en ayant en vue la protection des droits fondamentaux en matière de traitement des données à caractère personnel.

3. Chaque autorité de contrôle nationale :

traite les réclamations introduites par toute personne concernée, enquête sur l'affaire et informe la personne concernée de l'état d'avancement du dossier et de l'issue de la réclamation dans un délai raisonnable ;

vérifie la licéité du traitement des données, effectue des enquêtes, des inspections et des audits conformément au droit national, de sa propre initiative ou en se fondant sur une réclamation visée au point a).

4. Chaque autorité de contrôle nationale conseille, sur demande, toute personne concernée quant à l'exercice des droits que lui confèrent les dispositions adoptées en vertu de la présente directive. »

L'article 19 de ladite directive, intitulé « Réexamen », prévoit :

« 1. Sur la base des informations communiquées par les États membres, y compris les informations statistiques visées à l'article 20, paragraphe 2, la Commission procède, au plus tard le 25 mai 2020, au réexamen de tous les éléments de la présente directive et communique et présente un rapport au Parlement européen et au Conseil [de l'Union européenne].

2. Dans le cadre de son réexamen, la Commission accorde 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 ;

à la durée de la période de conservation des données ;

à l'efficacité de l'échange d'informations entre les États membres ; et

à la qualité des évaluations, y compris en ce qui concerne les informations statistiques recueillies en vertu de l'article 20.

3. Le rapport visé au paragraphe 1 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. 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. Le rapport 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.

4. Le cas échéant, au vu du réexamen effectué au titre du présent article, la Commission soumet une proposition législative au Parlement européen et au Conseil en vue de modifier la présente directive. »

L'article 21 de la même directive, intitulé « Rapports avec d'autres instruments », énonce, à son paragraphe 2 :

« La présente directive s'applique sans préjudice de l'applicabilité de la directive [95/46] au traitement des données à caractère personnel par les transporteurs aériens. »

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

Code repère du dossier passager

Date de réservation/d'émission du billet

Date(s) prévue(s) du voyage

Nom(s)

Adresse et coordonnées (numéro de téléphone, adresse électronique)

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

Itinéraire complet pour le PNR concerné

Informations "grands voyageurs"

Agence de voyages/agent de voyages

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

Indications concernant la scission/division du PNR

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)

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

Numéro du siège et autres informations concernant le siège

Informations sur le partage de code

Toutes les informations relatives aux bagages

Nombre et autres noms de voyageurs figurant dans le PNR

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)

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

L'annexe II de cette directive, intitulée « Liste des infractions visées à l'article 3, point 9) », est libellée comme suit :

Participation à une organisation criminelle

Traite des êtres humains

Exploitation sexuelle des enfants et pédopornographie
Trafic de stupéfiants et de substances psychotropes
Trafic d'armes, de munitions et d'explosifs
Corruption
Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union
Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro
Cybercriminalité
Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées
Aide à l'entrée et au séjour irréguliers
Meurtre, coups et blessures graves
Trafic d'organes et de tissus humains
Enlèvement, séquestration et prise d'otage
Vol organisé ou vol à main armée
Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art
Contrefaçon et piratage de produits
Falsification de documents administratifs et trafic de faux
Trafic de substances hormonales et d'autres facteurs de croissance
Trafic de matières nucléaires et radioactives
Viol
Infractions graves relevant de la Cour pénale internationale
Détournement d'avion/de navire
Sabotage
Trafic de véhicules volés
Espionnage industriel. »

7. La décision-cadre 2002/475

L'article 1er de la décision-cadre 2002/475 définissait la notion d'« infraction terroriste » en énumérant une série d'actes intentionnels, visés aux points a) à i) de ce même article, commis dans le but de « gravement intimider une population », « contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque » ou « gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou une organisation internationale ». Les articles 2 et 3 de cette décision-cadre définissaient, respectivement, les notions d'« infractions relatives à un groupe terroriste » et d'« infractions liées aux activités terroristes ». L'article 4 de ladite décision-cadre régissait les incriminations d'incitation et de complicité à commettre ces infractions ainsi que de tentative de les commettre.

La décision-cadre 2002/475 a été abrogée par 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), dont les articles 3 à 14 comportent des définitions analogues.

B. Le droit belge

1. La Constitution

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. »

2. La loi du 25 décembre 2016

L'article 2 de la loi du 25 décembre 2016, relative au traitement des données des passagers (*Moniteur belge* du 25 janvier 2017, p. 12905, ci-après la « loi du 25 décembre 2016 »), est libellé comme suit :

« La présente loi et les arrêtés royaux, qui seront pris en exécution de la présente loi, transposent la [directive API] et la [directive PNR]. La présente loi et l'arrêté royal concernant le secteur maritime transposent partiellement la directive [2010/65]. »

L'article 3 de cette loi dispose :

« § 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. »

L'article 4 de ladite loi prévoit :

« Pour l'application de la présente loi et de ses arrêtés d'exécution, l'on entend par :
[...]

"les services compétents" : les services visés à l'article 14, § 1er, 2° ;

"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 ;

"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 ;

[...] »

L'article 8 de la loi du 25 décembre 2016 énonce :

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

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 90ter, § 2, [...] 7°, [...] 8°, [...] 11°, [...] 14°, [...] 17°, 18°, 19°, et § 3, du Code d'instruction criminelle ;

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, 199bis, 207, 213, 375 et 505 du Code pénal ;

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 ;

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. »

Aux termes de l'article 14, § 1er, de cette loi :

« L'UIP est composée :

[...]

2° de membres détachés issus des services compétents suivants :

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

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

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

L'article 24 de ladite loi, qui figure dans la section 1re, intitulée « Le traitement des données de passagers dans le cadre de l'évaluation préalable des passagers », du chapitre 10 de la même loi, relatif au traitement des données, est ainsi libellé :

« § 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 :

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.

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. »

Le chapitre 11 de la loi du 25 décembre 2016, intitulé « Le traitement des données des passagers en vue de l'amélioration du contrôle aux frontières et de la lutte contre l'immigration illégale », comprend les articles 28 à 31 de celle-ci.

L'article 28 de cette loi dispose :

« § 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. »

Aux termes de l'article 29 de ladite loi :

« § 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 :

les passagers qui envisagent d'entrer ou sont entrés sur le territoire par les frontières extérieures de la Belgique ;
les passagers qui envisagent de quitter ou ont quitté le territoire par les frontières extérieures de la Belgique ;
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.

[...] »

La loi du 25 décembre 2016 a été rendue applicable aux compagnies aériennes, aux transporteurs assurant un service international de transport de voyageurs (transporteurs HST) et aux intermédiaires de voyage ayant un contrat avec ces transporteurs (distributeurs de tickets HST), ainsi qu'aux transporteurs par bus, respectivement, par l'arrêté royal du 18 juillet 2017 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les compagnies aériennes (*Moniteur belge* du 28 juillet 2017, p. 75934), par l'arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs HST et distributeurs de tickets HST (*Moniteur belge* du 12 février 2019, p. 13018), et par l'arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs par bus (*Moniteur belge* du 12 février 2019, p. 13023).

II. Le litige au principal et les questions préjudicielles

Par requête du 24 juillet 2017, la Ligue des droits humains a saisi la Cour constitutionnelle (Belgique) d'un recours tendant à l'annulation totale ou partielle de la loi du 25 décembre 2016.

La juridiction de renvoi expose que cette loi transpose, en droit interne, la directive PNR et la directive API ainsi que, partiellement, la directive 2010/65. Il ressortirait des travaux préparatoires de ladite loi que celle-ci 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 [Service public fédéral intérieur (Belgique)] ». Le législateur national aurait également précisé que les finalités de la loi du 25 décembre 2016 relèvent de trois catégories, à savoir, premièrement, la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, deuxièmement, les missions des services de renseignement et de sécurité et, troisièmement, l'amélioration des contrôles aux frontières extérieures et la lutte contre l'immigration illégale.

À l'appui de son recours, la Ligue des droits humains soulève deux moyens tirés, le premier, d'une violation de l'article 22 de la Constitution, lu en combinaison avec l'article 23 du RGPD, les articles 7, 8 et l'article 52, paragraphe 1, de la Charte ainsi que l'article 8 de la CEDH et, le second, invoqué à titre subsidiaire, d'une violation de cet article 22, lu en combinaison avec l'article 3, paragraphe 2, TUE et l'article 45 de la Charte.

Par son premier moyen, la Ligue des droits humains fait valoir, en substance, que cette loi implique une ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel, qui n'est pas conforme à l'article 52, paragraphe 1, de la Charte, et notamment au principe de proportionnalité. En effet, le champ d'application de ladite loi et la définition des données collectées, susceptibles de révéler des informations sensibles, seraient trop larges. De même, la notion de « passager », au sens de la même loi, permettrait un traitement automatisé systématique, non ciblé, des données de tous les passagers. En outre, la nature et les modalités de la méthode de *prescreening* ainsi que les bases de données avec lesquelles sont confrontées ces données, une fois transmises, ne seraient pas déterminées de manière suffisamment claire. Par ailleurs, la loi du 25 décembre 2016 poursuivrait des finalités autres que celles de la directive PNR. Enfin, le délai de cinq ans prévu par cette loi pour la conservation desdites données serait disproportionné.

Par son second moyen, visant l'article 3, paragraphe 1, l'article 8, paragraphe 2, et les articles 28 à 31 de la loi du 25 décembre 2016, la Ligue des droits humains fait valoir que, en étendant le système prévu par la directive PNR aux transports intra-UE, ces dispositions ont pour effet de rétablir indirectement des contrôles aux frontières intérieures contraires à la liberté de circulation des personnes. En effet, dès lors qu'une personne se trouve sur le territoire belge, que ce soit à son arrivée, à son départ ou pour une escale, ses données seraient automatiquement collectées.

Le Conseil des ministres conteste cette argumentation. Il considère, en particulier, que le premier moyen est irrecevable en ce qu'il vise le RGPD, lequel ne serait pas applicable à la loi du 25 décembre 2016. Par ailleurs, le traitement des données prévu par cette loi, conformément à la directive PNR, constituerait un outil essentiel dans le cadre, notamment, de la lutte contre le terrorisme et la grande criminalité, et les mesures résultant de ladite loi seraient nécessaires pour atteindre les buts poursuivis et proportionnées.

S'agissant du premier moyen, la juridiction de renvoi s'interroge, tout d'abord, sur l'applicabilité de la protection prévue par le RGPD aux traitements des données instaurés par la loi du 25 décembre 2016, laquelle vise à mettre en œuvre, principalement, la directive PNR. Cette juridiction relève, ensuite, en se référant à la jurisprudence issue de l'avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592), que la définition des données PNR, figurant à l'article 3, point 5, ainsi qu'à l'annexe I de cette directive, pourrait, d'une part, n'être pas suffisamment claire et précise, en raison du caractère non exhaustif de la description de certaines de ces données contenue dans ces dispositions et, d'autre part, aboutir indirectement à la révélation de données sensibles. En outre, la définition

de la notion de « passager » figurant à l'article 3, point 4, de ladite directive pourrait avoir pour conséquence que la collecte, le transfert, le traitement et la conservation des données PNR constituent des obligations générales et indifférenciées, s'appliquant à toute personne transportée ou devant être transportée et inscrite sur la liste des passagers, indépendamment de l'existence de motifs sérieux de croire que cette personne a commis ou est sur le point de commettre une infraction ou bien encore a été reconnue coupable d'une infraction.

Ladite juridiction fait encore observer que les données PNR, conformément aux dispositions de la directive PNR, font systématiquement l'objet d'une évaluation préalable impliquant un croisement avec des bases de données ou des critères préétablis, en vue d'établir des correspondances. Or, le Comité consultatif de la convention n° 108 du Conseil de l'Europe aurait indiqué, dans son avis du 19 août 2016 sur les implications en matière de protection des données du traitement des données passagers [T-PD(2016)18rev], que les traitements des données à caractère personnel concernent tous les passagers et pas seulement les individus ciblés, soupçonnés d'être impliqués dans une infraction pénale ou de constituer une menace immédiate pour la sécurité nationale ou l'ordre public, et que les données PNR peuvent non seulement être comparées *(data matching)* à des bases de données mais également être traitées par exploration *(data mining)* au moyen de sélecteurs ou d'algorithmes prédictifs, dans le but d'identifier quiconque pourrait être impliqué ou s'engager dans des activités criminelles, une telle évaluation des passagers par mise en correspondance de données pouvant soulever des questions de prévisibilité, en particulier lorsqu'elle est effectuée sur la base d'algorithmes prédictifs utilisant des critères dynamiques pouvant évoluer en permanence selon leurs capacités d'auto-apprentissage. Dans ce contexte, la juridiction de renvoi estime que, si les critères préétablis servant à déterminer des profils à risque doivent être spécifiques, fiables et non discriminatoires, conformément à l'avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592), il semble techniquement impossible de définir davantage ces critères.

Quant au délai de conservation de cinq ans et à l'accès aux données prévus à l'article 12 de la directive PNR, cette juridiction relève que la Commission de la protection de la vie privée (Belgique), dans son avis d'initiative n° 01/2010 du 13 janvier 2010 relatif au projet de loi portant assentiment à l'accord PNR UE-États-Unis d'Amérique, a estimé que, lorsque le délai de conservation est long et que les données sont stockées massivement, le risque de profilage des personnes concernées augmente, tout comme celui de détournement de l'utilisation de ces données pour des finalités autres que celles prévues initialement. Il ressortirait, en outre, de l'avis du 19 août 2016 du Comité consultatif de la convention n° 108 du Conseil de l'Europe que des données masquées permettent encore d'identifier les personnes et restent ainsi des données à caractère personnel et que leur conservation doit être limitée dans le temps pour prévenir une surveillance permanente généralisée.

Dans ces conditions, eu égard à la jurisprudence issue notamment de l'avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592), la juridiction de renvoi se demande si le système de collecte, de transfert, de traitement et de conservation des données PNR établi par la directive PNR peut être considéré comme respectant les limites du strict nécessaire. Cette juridiction considère qu'il convient également de déterminer si cette directive s'oppose à une législation nationale autorisant le traitement des données PNR pour une finalité autre que celles prévues par ladite directive et si une communication de l'intégralité de ces données après leur dépersonnalisation, en vertu de l'article 12 de la même directive, pourrait être approuvée par une autorité nationale telle que l'UIP créée par la loi du 25 décembre 2016.

S'agissant du second moyen, la juridiction de renvoi indique que l'article 3, paragraphe 1, de cette 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 ». Cette juridiction ajoute, concernant le champ d'application de ladite loi, que le législateur national a décidé de « l'inclusion intra-UE dans la collecte des données » afin d'obtenir « un tableau plus complet des déplacements des passagers qui constituent une menace potentielle pour la sécurité intracommunautaire et nationale », ce que prévoit l'article 2 de la directive PNR, lu en combinaison avec le considérant 10 de celle-ci, pour les vols à l'intérieur de l'Union. Ladite juridiction précise encore que la Commission de la protection de la vie privée, dans son avis n° 55/2015 du 16 décembre 2015 sur l'avant-projet de loi à l'origine de la loi du 25 décembre 2016, s'est interrogée sur un éventuel conflit entre le système PNR belge et le principe de la libre circulation des personnes, dans la mesure où ce système inclut les transports effectués au sein de l'Union.

C'est dans ces conditions que la Cour constitutionnelle a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

L'article 23 du [RGPD], lu en combinaison avec l'article 2, paragraphe 2, sous d), de ce règlement, doit-il être interprété comme s'appliquant à une législation nationale telle que la [loi du 25 décembre 2016], qui transpose la [directive PNR], ainsi que la [directive API] et la directive [2010/65] » ?

L'annexe I de la [directive PNR] est-elle compatible avec les articles 7, 8 et 52, paragraphe 1, de la [Charte], en ce que les données qu'elle énumère sont très larges – notamment les données visées au point 18 de l'annexe I de [cette directive], qui dépassent les données visées à l'article 3, paragraphe 2, de la [directive API] – et en ce que, prises ensemble, elles pourraient révéler des données sensibles, et violer ainsi les limites du "strict nécessaire" ?

Les points 12 et 18 de l'annexe I de la [directive PNR] sont-ils compatibles avec les articles 7, 8 et 52, paragraphe 1, de la [Charte], 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 ?

L'article 3, point 4, de la [directive PNR] et l'annexe I de la même directive sont-ils compatibles avec les articles 7, 8 et 52, paragraphe 1, de la [Charte], 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 ?

L'article 6 de la [directive PNR], lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la [Charte], 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 ?

L'article 6 de la [directive PNR] est-il compatible avec les articles 7, 8 et 52, paragraphe 1, de la [Charte], 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 ?

La notion d'"autre autorité nationale compétente" visée à l'article 12, paragraphe 3, de la [directive PNR] 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 ?

L'article 12 de la [directive PNR], lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la [Charte], 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 ?

La [directive API] est-elle compatible avec l'article 3, paragraphe 2, [TUE] et avec l'article 45 de la [Charte], en ce que les obligations qu'elle instaure s'appliquent aux vols à l'intérieur de l'Union européenne ?

La [directive API], lue en combinaison avec l'article 3, paragraphe 2, [TUE] et avec l'article 45 de la [Charte], 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 ?

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 PNR], 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] 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 ? »

III. Sur les questions préjudicielles

A. Sur la première question

Par sa première question, la juridiction de renvoi demande, en substance, si 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 PNR, de la directive API et de la directive 2010/65, en particulier au transfert, à la conservation et au traitement des données PNR.

Ainsi qu'il découle de l'article 2, paragraphe 1, du RGPD, ce règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de telles données contenues ou appelées à figurer dans un fichier. La notion de « traitement » est définie de manière large à l'article 4, point 2, dudit règlement comme incluant, notamment, la collecte, l'enregistrement, la conservation, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute forme de mise à disposition, le rapprochement ou l'effacement de telles données ou ensembles de données.

Le gouvernement belge fait cependant valoir que le transfert des données PNR, par des opérateurs économiques, à l'UIP, à des fins de prévention et de détection des infractions pénales, tel que prévu à l'article 1er, paragraphe 1, sous a), à l'article 1er, paragraphe 2, et à l'article 8 de la directive PNR, qui constitue un « traitement » de données à caractère personnel au sens de l'article 4, point 2, du RGPD, tout comme leur recueil préalable, ne relève pas du champ d'application de ce règlement en vertu de l'article 2, paragraphe 2, sous d), dudit règlement, au motif que la jurisprudence issue de l'arrêt du 30 mai 2006, Parlement/Conseil et Commission, C-317/04 et C-318/04, EU:C:2006:346, points 57 à 59), relative à l'article 3, paragraphe 2, premier tiret, de la directive 95/46, serait transposable à cette disposition dudit règlement.

À cet égard, il est vrai que, ainsi que la Cour l'a déjà constaté, l'article 3, paragraphe 2, premier tiret, de la directive 95/46, laquelle a été abrogée et remplacée par le RGPD avec effet au 25 mai 2018, excluait de son champ d'application, de manière générale, les « traitements ayant pour objet la sécurité publique, la défense [et] la sûreté de l'État », sans opérer de distinction en fonction de l'auteur du traitement de données concerné. Ainsi, les traitements effectués par des opérateurs privés découlant d'obligations imposées par les pouvoirs publics pouvaient, le cas échéant, relever de l'exception prévue à cette disposition, compte tenu du fait que la formulation de celle-ci visait l'ensemble des traitements, quel qu'en soit l'auteur, ayant pour objet la sécurité publique, la défense ou la sûreté de l'État (voir, en ce sens, 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 101).

Toutefois, l'article 2, paragraphe 2, sous d), du RGPD opère une telle distinction, puisque, ainsi que l'a relevé M. l'avocat général aux points 41 et 46 de ses conclusions, le libellé de cette disposition met clairement en évidence que deux conditions sont exigées pour qu'un traitement de données relève de l'exception qu'il prévoit. Si 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.

Comme l'a également constaté la Cour, il ressort de l'article 23, paragraphe 1, sous d) et h), du RGPD que les traitements de données à caractère personnel effectués par des particuliers aux fins visées à l'article 2, paragraphe

2, sous d), de ce règlement relèvent du champ d'application de celui-ci (voir, en ce sens, 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 102).

Il s'ensuit que la jurisprudence issue de l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346), invoquée par le gouvernement belge, n'est pas transposable à l'exception au champ d'application du RGPD figurant à son article 2, paragraphe 2, sous d).

En outre, cette exception doit 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.

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].

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].

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.

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.

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] ».

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.

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.

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].

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.

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.

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.

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.

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.

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. Sur les deuxième à quatrième et sixième questions

Par ses deuxième à quatrième et sixième questions, qu'il convient d'examiner conjointement, la juridiction de renvoi interroge la Cour, en substance, sur la validité de la directive PNR au regard des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte. Ces questions portent, notamment, sur :

l'annexe I de cette directive et les données que cette annexe énumère, notamment celles visées à ses points 12 et 18, au regard des exigences de clarté et de précision (deuxième et troisième questions) ;

l'article 3, point 4, de ladite directive et l'annexe I de celle-ci, en ce que le système de collecte, de transfert et de traitement généralisés des données PNR que ces dispositions instituent est susceptible de s'appliquer à toute personne empruntant un vol relevant des dispositions de cette même directive (quatrième question), et

l'article 6 de la directive PNR en ce qu'il prévoit une évaluation préalable, au moyen d'une confrontation des données PNR à des bases de données et/ou de leur traitement au regard de critères préétablis, qui s'applique de manière systématique et généralisée à ces données, indépendamment de tout élément objectif permettant de considérer que les passagers concernés sont susceptibles de présenter un risque pour la sécurité publique (sixième question).

À titre liminaire, il y a lieu de rappeler 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. Ainsi, lorsqu'un texte du droit dérivé de l'Union est susceptible de plus d'une interprétation, il convient de donner la préférence à celle qui rend la disposition conforme au droit primaire plutôt qu'à celle conduisant à constater son incompatibilité avec celui-ci (arrêt du 2 février 2021, Consob, C-481/19, EU:C:2021:84, point 50 et jurisprudence citée).

En outre, il est de jurisprudence constante que, lorsque les dispositions d'une directive laissent aux États membres une marge d'appréciation pour définir des mesures de transposition qui soient adaptées aux différentes situations envisageables, il leur incombe, 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 [voir, en ce sens, arrêts du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 60 et jurisprudence citée, ainsi que du 16 juillet 2020, État belge (Regroupement familial – Enfant mineur), C-133/19, C-136/19 et C-137/19, EU:C:2020:577, point 33 et jurisprudence citée].

S'agissant de la directive PNR, il convient de relever que, notamment, 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, de sorte que, ainsi que l'énonce le considérant 36, cette directive « devrait […] être mise en œuvre en conséquence ».

En particulier, le considérant 22 de la directive PNR souligne que, « [en] tenant pleinement compte des principes mis en évidence par la récente jurisprudence pertinente de la [Cour], l'application de [cette] directive devrait garantir le plein respect des droits fondamentaux et du droit au respect de la vie privée ainsi que du principe de proportionnalité » et « véritablement remplir les objectifs de nécessité et de proportionnalité afin de répondre aux intérêts généraux reconnus par l'Union et à la nécessité de protéger les droits et libertés d'autrui dans la lutte contre les infractions terroristes et les formes graves de criminalité ». Ce considérant ajoute que cette application « devrait être dûment justifiée et les garanties nécessaires devraient être mises en place afin d'assurer la légalité de tout stockage, de toute analyse, de tout transfert ou de toute utilisation des données PNR ».

Par ailleurs, 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 ».

Il convient donc de vérifier si la directive PNR, conformément à ce qu'exigent notamment ses considérants et ses dispositions visés aux points 88 à 90 du présent arrêt, peut être interprétée d'une manière qui assure le plein respect des droits fondamentaux garantis aux articles 7 et 8 de la Charte ainsi que du principe de proportionnalité consacré à l'article 52, paragraphe 1, de celle-ci.

1. Sur les ingérences résultant de la directive PNR dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte

L'article 7 de la Charte garantit à toute personne le droit au respect de sa vie privée et familiale, de son domicile et de ses communications, tandis que l'article 8, paragraphe 1, de la Charte confère explicitement à toute personne le droit à la protection des données à caractère personnel la concernant.

Ainsi qu'il ressort de l'article 3, point 5, de la directive PNR et de l'énumération figurant à l'annexe I de celle-ci, les données PNR visées par cette directive comprennent notamment, outre le nom du ou des passagers aériens, des informations nécessaires à la réservation, telles que les dates prévues du voyage et l'itinéraire de voyage, des informations relatives aux billets, les groupes de personnes enregistrées sous le même numéro de réservation, les coordonnées du ou des passagers, des informations relatives aux modes de paiement ou à la facturation, des informations concernant les bagages ainsi que des remarques générales à l'égard des passagers.

Dès lors que les données PNR comportent ainsi des informations sur des personnes physiques identifiées, à savoir les passagers aériens concernés, les différents traitements dont ces données peuvent faire l'objet affectent le droit fondamental au respect de la vie privée, garanti à l'article 7 de la Charte [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 121 et 122 ainsi que jurisprudence citée].

En outre, les traitements de données PNR tels que ceux visés par la directive PNR relèvent également de l'article 8 de la Charte en raison du fait qu'ils constituent des traitements de données à caractère personnel au sens de cet article et doivent, par suite, nécessairement satisfaire aux exigences de protection des données prévues audit article [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 123 et jurisprudence citée].

Or, il est de jurisprudence constante que la communication de données à caractère personnel à un tiers, tel qu'une autorité publique, constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure des informations communiquées. Il en va de même de la conservation des données à caractère personnel ainsi que de l'accès auxdites données en vue de leur utilisation par les autorités publiques. À cet égard, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée].

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.

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.

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 ».

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].

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.

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 ».

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].

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.

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.

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.

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.

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 ».

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.

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.

Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer 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.

2. Sur la justification des ingérences résultant de la directive PNR

Il y a lieu de rappeler que les droits fondamentaux 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 [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 136 et jurisprudence citée, ainsi que arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 63 et jurisprudence citée].

Aux termes de 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. À cet égard, l'article 8, paragraphe 2, de la Charte précise que 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 ».

Il convient d'ajouter que l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que l'acte qui permet l'ingérence dans ces droits doit définir lui-même la portée de la limitation de l'exercice du droit concerné, étant précisé, d'une part, que cette exigence n'exclut pas que la limitation en cause soit formulée dans des termes suffisamment ouverts pour pouvoir s'adapter à des cas de figure différents ainsi qu'aux changements de situations (voir, en ce sens, arrêt du 26 avril 2022, Pologne/Parlement et Conseil, C-401/19, EU:C:2022:297, points 64 et 74 ainsi que jurisprudence citée) et, d'autre part, que la Cour peut, le cas échéant, préciser, par voie d'interprétation, la portée concrète de la limitation au regard tant des termes mêmes de la réglementation de l'Union en cause que de son économie générale et des objectifs qu'elle poursuit, tels qu'interprétés à la lumière des droits fondamentaux garantis par la Charte.

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. En outre, 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, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140, ainsi que arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 52 et jurisprudence citée].

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 (voir, en ce sens, arrêts du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 55 et jurisprudence citée, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 53 et jurisprudence citée).

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].

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

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.

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

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.

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].

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.

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.

c) Sur le caractère nécessaire des ingérences résultant de la directive PNR

Conformément à la jurisprudence rappelée aux points 115 à 118 du présent arrêt, 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.

1) Sur les données des passagers aériens visées par la directive PNR

Il convient d'apprécier si les rubriques de données figurant dans l'annexe I de la directive PNR définissent de manière claire et précise les données PNR qu'un transporteur aérien est tenu de communiquer à l'UIP.

À titre liminaire, il y a lieu de rappeler que, ainsi qu'il ressort du considérant 15 de la directive PNR, le législateur de l'Union a entendu que la liste des données PNR à transmettre à une UIP soit 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 ». En particulier, selon ce même considérant, ces données « 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 ». En outre, la directive PNR interdit, à son article 13, paragraphe 4, première phrase, « 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 ».

Par conséquent, 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.

Or, 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. Ainsi que M. l'avocat général l'a relevé au point 165 de ses conclusions, tel est également le cas, nonobstant leur libellé ouvert, des rubriques 10, 13, 14 et 16.

Il y a lieu, en revanche, d'apporter des précisions aux fins de l'interprétation des rubriques 5, 6, 8, 12 et 18.

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.

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].

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.

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) ».

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.

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.

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) ».

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.

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].

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.

2) Sur les finalités des traitements des données PNR

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 ».

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] ».

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.

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 ».

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

4) Sur les passagers aériens et les vols concernés

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.

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.

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.

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].

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.

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.

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.

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.

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.

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.

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.

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.

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).

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).

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).

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.

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.

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.

5) Sur l'évaluation préalable des données PNR au moyen de traitements automatisés

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.

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).*

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.

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.

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.

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^{o} 562/2006. Ainsi, le système établi par la directive PNR ne permet pas aux autorités compétentes de limiter ce droit au-delà de ce qui est prévu par la directive 2004/38 et le règlement n^{o} 562/2006.

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

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 ».

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.

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.

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.

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.

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 ».

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.

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).

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).

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.

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

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.

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.

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.

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.

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.

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 ».

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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].

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].

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.

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.

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.

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].

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.

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).

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).

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.

Eu égard à l'ensemble des considérations qui précèdent, 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.

C. Sur la cinquième question

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.

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.

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.

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 ».

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.

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 ».

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.

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.

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.

D. Sur la septième question

Par sa septième question, la juridiction de renvoi demande, en substance, si 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.

À titre liminaire, il y a lieu de faire observer que le gouvernement belge nourrit des doutes quant à la compétence de la Cour pour répondre à cette question, telle que formulée par la juridiction de renvoi, au motif que cette dernière juridiction est seule compétente pour interpréter les dispositions nationales et, en particulier, apprécier les exigences résultant de la loi du 25 décembre 2016 au regard de l'article 12, paragraphe 3, sous b), de la directive PNR.

À cet égard, il suffit de relever que, par ladite question, la juridiction de renvoi sollicite l'interprétation d'une disposition du droit de l'Union. En outre, si, dans le cadre d'une procédure introduite en vertu de l'article 267 TFUE, l'interprétation des dispositions nationales appartient aux juridictions des États membres et non à la Cour, et s'il n'incombe pas à cette dernière de se prononcer sur la compatibilité de normes de droit interne avec les dispositions du droit de l'Union, la Cour est compétente pour fournir à la juridiction nationale tous les éléments d'interprétation relevant du droit de l'Union qui permettent à celle-ci d'apprécier la compatibilité de telles normes avec la réglementation de l'Union (arrêt du 30 avril 2020, CTT – Correios de Portugal, C-661/18, EU:C:2020:335, point 28 et jurisprudence citée). Il s'ensuit que la Cour est compétente pour répondre à la septième question.

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.

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.

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.

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.

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.

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).

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.

E. Sur la huitième question

Par sa huitième question, la juridiction de renvoi demande, en substance, si l'article 12 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, sans distinguer selon que les passagers concernés présentent ou non un risque en matière d'infractions terroristes ou de formes graves de criminalité.

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.

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 ».

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.

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.

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.

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.

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.

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.

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].

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].

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].

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.

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.

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.

F. Sur la neuvième question, sous a)

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.

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.

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.

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.

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.

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.

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.

G. Sur la neuvième question, sous b)

Si, dans sa neuvième question, sous b), la juridiction de renvoi se réfère à la directive API, lue en combinaison avec l'article 3, paragraphe 2, TUE et l'article 45 de la Charte, il ressort de la demande de décision préjudicielle que cette juridiction s'interroge sur la compatibilité du système de transfert et de traitement des données des passagers mis en place par la loi du 25 décembre 2016 avec la libre circulation des personnes et la suppression des contrôles aux frontières intérieures prévues par le droit de l'Union, en ce que ce système s'applique non seulement aux transports aériens, mais également aux transports ferroviaires, terrestres, voire maritimes, en provenance ou à destination de la Belgique, effectués à l'intérieur de l'Union, sans franchissement de frontières extérieures avec les pays tiers.

Or, ainsi qu'il ressort des points 265 à 269 du présent arrêt, la directive API, qui ne s'applique pas aux vols intra-UE et n'impose pas d'obligation de transfert et de traitement des données des passagers voyageant par voie aérienne ou par un autre mode de transport à l'intérieur de l'Union, sans franchissement des frontières extérieures avec des pays tiers, n'est pas pertinente pour répondre à cette question.

En revanche, et alors que, selon l'article 67, paragraphe 2, TFUE, l'Union assure l'absence de contrôles des personnes aux frontières intérieures, l'article 2 de la directive PNR, sur lequel le législateur belge s'est fondé pour adopter la loi du 25 décembre 2016 en cause au principal, ainsi qu'il ressort de la demande de décision préjudicielle, autorise les États membres à appliquer cette directive aux vols intra-UE.

Dans ces conditions, afin de donner à la juridiction de renvoi une réponse utile, il convient de reformuler la neuvième question, sous b), comme visant, en substance, à savoir si 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 un système de transfert, par les transporteurs et les opérateurs de voyage, ainsi que de traitement, par les autorités compétentes, des données PNR des vols et des transports effectués par d'autres moyens à l'intérieur de l'Union, en provenance ou à destination de l'État membre ayant adopté ladite législation ou bien encore transitant par cet État membre.

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].

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.

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.

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).

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.

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.

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).

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

H. Sur la dixième question

Par sa dixième question, la juridiction de renvoi cherche, en substance, à savoir si le droit de l'Union doit être interprété en ce sens qu'une juridiction nationale peut limiter 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.

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).

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).

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).

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).

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).

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.

IV. Sur les dépens

La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

L'article 2, paragraphe 2, sous d), et 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), 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 2004/82/CE du Conseil, du 29 avril 2004, concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, de 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, et de 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, 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 2004/82 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 2016/681, qui sont effectués par l'unité d'information passagers (UIP) ou par les autorités compétentes aux fins visées à l'article 1er, paragraphe 2, de cette directive.

Dès lors qu'une interprétation de la directive 2016/681 à la lumière des articles 7, 8 et 21 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, assure la conformité de cette directive avec ces articles de la charte des droits fondamentaux, l'examen des deuxième à quatrième et sixième questions préjudicielles n'a révélé aucun élément de nature à affecter la validité de ladite directive.

L'article 6 de la directive 2016/681, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une législation nationale qui autorise le traitement de données des dossiers passagers (données PNR)

recueillies conformément à cette directive à des fins autres que celles expressément visées à l'article 1er, paragraphe 2, de ladite directive.

L'article 12, paragraphe 3, sous b), de la directive 2016/681 doit être interprété en ce sens qu'il s'oppose à une législation nationale selon laquelle l'autorité mise en place en tant qu'unité d'information passagers (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.

L'article 12, paragraphe 1, de la directive 2016/681, lu en combinaison avec les articles 7 et 8 ainsi qu'avec l'article 52, paragraphe 1, de la charte des droits fondamentaux, 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.

La directive 2004/82 doit être interprétée en ce sens qu'elle ne s'applique pas aux vols, réguliers ou non, effectués par un transporteur aérien en provenance du territoire d'un État membre et devant atterrir sur le territoire d'un ou de plusieurs États membres, sans escale sur le territoire d'un pays tiers (vols intra-UE).

Le droit de l'Union, en particulier l'article 2 de la directive 2016/681, 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 des droits fondamentaux, 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 2016/681 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.

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 2016/681, 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 des droits fondamentaux. 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.

Lenaerts Arabadjiev Rodin

Jarukaitis Jääskinen von Danwitz

Safjan Biltgen Xuereb

Piçarra Rossi Kumin

Wahl

Ainsi prononcé en audience publique à Luxembourg, le 21 juin 2022.

Le greffier Le président

A. Calot Escobar K. Lenaerts

---

* Langue de procédure : le français.