Version anonymisée

Affaire C-215/20

Renvoi préjudiciel

Date de dépôt :

19 mai 2020

Juridiction de renvoi :

Verwaltungsgericht Wiesbaden (Allemagne)

Date de la décision de renvoi :

13 mai 2020

Partie requérante :

JV

Partie défenderesse :

Bundesrepublik Deutschland

[OMISSIS]

VERWALTUNGSGERICHT WIESBADEN

DÉCISION

Dans la procédure administrative contentieuse opposant

JV,

[OMISSIS] Berlin,

partie requérante,

[OMISSIS]

à

la Bundesrepublik Deutschland (République fédérale d'Allemagne), représentée par le Bundeskriminalamt (Office fédéral de police criminelle), Wiesbaden, [OMISSIS],

partie défenderesse,

[OMISSIS]

ayant pour objet : le droit à la protection des données à caractère personnelles, **[Or. 2]**

le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden, Allemagne) – 6e chambre – [OMISSIS]

[OMISSIS]

a ainsi statué le 13 mai 2020 :

I. Il est sursis à statuer.

II. La Cour de justice de l'Union européenne est saisie à titre préjudiciel, conformément à l'article 267 TFUE, des questions suivantes :

1. La directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, concernant 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 »), en vertu de laquelle les transporteurs aériens transfèrent des dossiers de données volumineux concernant tous les passagers aériens, sans exception, à des unités d'information passagers mises en place par les États membres, où les données sont utilisées sans motif particulier à des fins de recoupement automatisé avec des bases de données et des critères préétablis et sont ensuite conservées pendant cinq ans, est-elle compatible avec la Charte des droits fondamentaux de l'Union européenne, en particulier avec les articles 7, 8 et 52 de celle-ci, compte tenu de l'objectif poursuivi par cette directive et des exigences de précision et de proportionnalité ?

2. Notamment :

a) L'article 3, point 9, de la directive PNR, lu en combinaison avec l'annexe II de ladite directive, en ce qu'il précise que la notion de « formes graves de criminalité » au sens de la directive PNR désigne les infractions [Or. 3] énumérées à l'annexe II de ladite directive et 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, est-il compatible, du point de vue de la précision

suffisante et de l'exigence de proportionnalité, avec les articles 7 et 8 de la charte ?

b) Les dossiers passagers à transférer (ci-après les « données PNR ») sont-ils définis de manière suffisamment précise pour pouvoir justifier une atteinte aux articles 7 et 8 de la charte dans la mesure où il est nécessaire de transmettre les noms (article 8, paragraphe 1, première phrase, lu en combinaison avec l'annexe I, point 4, de la directive PNR), les informations grands voyageurs (article 8, paragraphe 1, première phrase, lu en combinaison avec l'annexe I, point 8, de la directive PNR) et de remplir un champ libre avec des indications générales (article 8, paragraphe 1, première phrase, lu en combinaison avec l'annexe I, point 12, de la directive PNR) ?

c) Est-il compatible avec les articles 7 et 8 de la charte et avec l'objectif de la directive PNR, que soient également collectées, outre les données des passagers aériens, les données de tiers, tels que l'agence de voyages ou l'agent de voyage (annexe I, point 9, de la directive PNR), les personnes accompagnant des mineurs (annexe I, point 12, de la directive PNR) et les personnes voyageant avec le passager (annexe I, point 17, de la directive PNR) ?

d) La directive PNR est-elle compatible avec les articles 7, 8 et 24 de la charte en ce que des données PNR de voyageurs aériens mineurs sont transférées, traitées et stockées ?

e) L'article 8, paragraphe 2, de la directive PNR, lu en combinaison avec l'annexe I, point 18, de ladite directive, disposant que les transporteurs aériens transfèrent les données API aux autorités compétentes des États membres, même lorsque ces données sont identiques aux données PNR, est-il compatible avec les articles 8 et 52 de la charte ?

f) L'article 6, paragraphe 4, de la directive PNR constitue-t-il en tant que base juridique permettant de déterminer les critères de comparaison des données des dossiers (« critères préétablis ») [Or. 4] un fondement légitime prévu par la loi suffisant au sens des articles 8, paragraphe 2, et 52 de la charte, ainsi que de l'article 16, paragraphe 2, TFUE ?

g) L'article 12 de la directive PNR limite-t-il encore l'atteinte à l'article 7 et à l'article 8 de la charte à ce qui est strictement nécessaire lorsque les données transférées sont conservées par les autorités compétentes des États membres pendant cinq ans ?

h) La dépersonnalisation prévue à l'article 12, paragraphe 2, de la directive PNR réduit-elle les données à caractère personnelles à ce qui

est nécessaire au sens des articles 8 et 52 de la charte, lorsqu'il ne s'agit que d'une pseudonymisation réversible à tout moment ?

i) Convient-il d'interpréter les articles 7 et 8 et 47 de la charte en ce sens qu'ils requièrent que les passagers dont les données sont dé-dépersonnalisées dans le cadre du traitement des données des passagers aériens (article 12, paragraphe 3, de la directive PNR) en soient informés et que la possibilité d'un contrôle juridictionnel leur soit ainsi ouverte ?

3. **L'article 11 de la directive PNR, en ce qu'il permet le transfert de données PNR vers des pays tiers qui ne disposent pas d'un niveau adéquat de protection des données, est-il compatible avec les articles 7 et 8 de la charte ?**

4. **L'article 6, paragraphe 4, quatrième phrase, de la directive PNR offre-t-il une protection suffisante contre le traitement de catégories particulières de données à caractère personnel, au sens de l'article 9 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 (JO 2016, L 119, p. 1 ; ci-après le « règlement général sur la protection des données »), et de l'article 10 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, [Or. 5] L 119, p. 89) si, dans le champ libre « Remarques générales » (annexe I, point 12, de la directive PNR), il est possible de transmettre, par exemple, des souhaits alimentaires, permettant de tirer des conclusions sur de telles catégories particulières de données à caractère personnel ?**

5. **Est-il compatible avec l'article 13 du règlement général sur la protection des données que, sur leur site Internet, les transporteurs aériens renvoient les passagers uniquement à la loi nationale de transposition (en l'occurrence : la loi sur le traitement des données des dossiers passagers, Fluggasdatengesetz du 6 juin 2017, BGBl. I, p. 1484, ci-après le FlugDaG ») ?**

CONSIDÉRANT CE QUI SUIT :

I.

1 L'affaire a pour objet un recours contre L'État fédéral (Bundesrepublik Deutschland), représenté par le Bundeskriminalamt. Le 28 avril 2019, le requérant a voyagé, avec le transporteur aérien Lufthansa, de Francfort-sur-le-Main, Allemagne à Bogota, Colombie, et le 7 mai 2019, il est rentré de Rio de Janeiro, Brésil à Francfort-sur-le-Main. Pour ces vols, il demande la radiation de ses données conservées par la défenderesse.

2 Le FlugDaG est entré en vigueur le 10 juin 2017. La loi vise à transposer la directive PNR. Cette directive régit de manière contraignante le transfert des données PNR en cas de vols des États membres de l'Union européenne vers des pays tiers et de pays tiers vers des États membres de l'Union européenne, ainsi que le traitement de ces données. Aux termes de son article 1er, paragraphe 2, la directive PNR a pour objet la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que les enquêtes et les poursuites en la matière. Elle impose aux États membres l'obligation de mettre en place des « unités d'information passagers » (UIP) **[Or. 6]** (article 4, paragraphe 1, de la directive PNR), qui sont responsables, afin d'atteindre l'objectif de la directive, de la collecte des données PNR auprès des transporteurs aériens, de la conservation, du traitement et du transfert de ces données aux unités d'informations passagers, ainsi que du partage des données PNR elles-mêmes ainsi que des résultats de leur traitement. En vertu de l'article 8 de la directive PNR, lu en combinaison avec l'annexe I de ladite directive, les États membres doivent imposer à toutes les compagnies aériennes de transférer un dossier de données PNR déterminé aux centres des PNR de l'État membre sur le territoire duquel les vols concernés sont arrivés ou dont ils proviennent. En vertu de l'article 9 de la directive PNR, les États membres peuvent demander et transférer entre eux les données PNR. Dans les conditions prévues à l'article 11 de la directive PNR, le transfert des données PNR vers des pays tiers est également possible. Conformément à l'article 12, paragraphe 2, de la directive PNR, les données enregistrées des passagers aériens devant être conservées pendant cinq ans doivent être « dépersonnalisées » à l'issue d'une période de six mois, c'est-à-dire que les éléments de données permettant d'identifier directement le passager doivent être occultés. Toutefois, une dé-dépersonnalisation de ces éléments de données est possible dans les conditions prévues à l'article 12, paragraphe 3, de la directive PNR. L'article 6 de la directive PNR régit le traitement des données qui doit notamment être effectué en procédant au rapprochement automatisé de celles-ci avec les bases de données et les « critères préétablis ». La directive PNR contient, pour les législateurs nationaux, une clause d'ouverture permettant également de couvrir les vols à l'intérieur de l'État membre de l'Union ou entre États membres de l'Union européenne. Le FlugDaG transpose cette directive en droit allemand. Il étend, ainsi que l'admet expressément l'article 2, paragraphe 1, de la directive PNR, l'obligation de notification à tous les vols civils atterrissant en Allemagne et atterrissant dans un autre pays ou en provenance d'un autre pays et à destination de l'Allemagne, y compris donc également aux vols à l'intérieur des États membres de l'Union européenne, article 2, paragraphe 3, du FlugDaG.

II.

3 La **charte des droits fondamentaux** de l'Union européenne (JO 2016, C 202, p. 389) dispose : **[Or. 7]**

4 **Article 7** de la charte – Respect de la vie privée et familiale

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

5 **Article 8** de la charte – Protection des données à caractère personnel

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

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

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

6 **Article 24** de la charte – Droits de l'enfant

1. Les enfants ont droit à la protection et aux soins nécessaires à leur bien-être. Ils peuvent exprimer leur opinion librement. Celle-ci est prise en considération pour les sujets qui les concernent, en fonction de leur âge et de leur maturité.

2. Dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale.

[…]

7 **Article 47** de la charte - Droit à un recours effectif et à accéder à un tribunal impartial

1) Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article.

2) Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter.

[…]

8 **Article 52** de la charte - Portée et interprétation des droits et des principes

1) Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et **[Or. 8]** *répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.*

[…]

9 L'**article 16 du traité sur le fonctionnement de l'Union européenne – TFUE –** (dans la version rectifiée du 7 juin 2016, JO 2016, C 202, p. 1) est libellé comme suit :

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

2) Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes. Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne.

10 La **directive PNR** (JO 2016, L 119, p. 132) dispose :

11 **Article 1er** de la directive PNR – Objet et champ d'application

1) La présente directive concerne :

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

b) 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).

12 **Article 2** de la directive PNR – Application de la présente directive aux vols intra-UE

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.* **[Or. 9]**

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.*

13 **Article 3** de la directive PNR – Définitions

Aux fins de la présente directive, on entend par :

1. *« 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 ;*

[…]

4. *« 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 ;*

[…]

9. *"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 ;*

10. *« 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.*

14 **Article 4** de la directive PNR – Unité d'informations passagers

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 :

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

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

[…]

4) Deux États membres ou plus (ci-après dénommés "États membres participants") peuvent mettre en place ou désigner une autorité unique en tant qu'UIP. Cette UIP est établie dans l'un des États membres participants et est considérée comme l'UIP nationale de tous les États membres participants. Ces derniers conviennent conjointement des modalités de fonctionnement de l'UIP et respectent les exigences prévues dans la présente directive.

[…]

15 **Article 5** de la directive PNR – Délégué à la protection des données au sein de l'UIP

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.

16 **Article 6** de la directive PNR – Traitement des données PNR

1) Les données PNR transférées par les transporteurs aériens sont recueillies par l'UIP de l'État membre concerné comme prévu à l'article 8. Lorsque les données PNR transférées par les transporteurs aériens comportent des

données autres que celles énumérées à l'annexe I, l'UIP efface ces données immédiatement et de façon définitive dès leur réception.

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

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

b) *répondre, au cas par cas, aux demandes dûment motivées fondées sur des motifs suffisants des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection* **[Or. 11]** *d'infractions terroristes ou de formes graves de criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière, et visant à communiquer aux autorités compétentes ou, le cas échéant, à Europol le résultat de ce traitement ; et*

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

3) *Lorsqu'ils réalisent l'évaluation visée au paragraphe 2, point a), l'UIP peut :*

a) *confronter les données PNR aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière, y compris les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données ; ou*

b) *traiter les données PNR au regard de critères préétablis.*

4) *L'évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci effectuée au titre du paragraphe 3, point b), au regard de critères préétablis est réalisée de façon non discriminatoire. Ces critères préétablis doivent être ciblés, proportionnés et spécifiques. Les États membres veillent à ce que ces critères soient fixés et réexaminés à intervalles réguliers par les UIP en coopération avec les autorités*

compétentes visées à l'article 7. Lesdits critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

5) Les États membres s'assurent que toute concordance positive obtenue à la suite du traitement automatisé des données PNR effectué au titre du paragraphe 2, point a), est réexaminée individuellement par des moyens non automatisés, afin de vérifier si l'autorité compétente visée à l'article 7 doit prendre des mesures en vertu du droit national.

[…]

17 **Article 8** de la directive PNR – Obligations imposées aux transporteurs aériens concernant les transferts de données

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 **[Or. 12]** *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 informations préalables sur les passagers (ci-après dénommées « 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.

[…]

18 **Article 9** de la directive PNR – Échange d'informations entre États membres

1) Les États membres veillent à ce que, en ce qui concerne les personnes identifiées par une UIP conformément à l'article 6, paragraphe 2, toutes les

données PNR pertinentes et nécessaires ou le résultat du traitement de ces données soient transmis par ladite UIP aux UIP correspondantes des autres États membres. Les UIP des États membres destinataires transmettent les informations reçues à leurs autorités compétentes, conformément à l'article 6, paragraphe 6.

2) *L'UIP d'un État membre a le droit de demander, si nécessaire, à l'UIP de tout autre État membre de lui communiquer des données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par le masquage d'éléments des données au titre de l'article 12, paragraphe 2, ainsi que, si nécessaire, le résultat de tout traitement de ces données, si celui-ci a déjà été réalisé en vertu de l'article 6, paragraphe 2, point a). Cette demande est dûment motivée. Elle peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas précis de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière. Les UIP transmettent dès que possible les informations demandées. Si les données demandées ont été dépersonnalisées par le masquage d'éléments des données conformément à l'article 12, paragraphe 2, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que cela est nécessaire aux fins visées à l'article 6, paragraphe 2, point b), et uniquement si elle y est autorisée par une autorité visée à l'article 12, paragraphe 3, point b).* **[Or. 13]**

[…]

19 **Article 11** de la directive PNR – Transfert de données vers des pays tiers

1) *Un État membre peut transférer à un pays tiers des données PNR et le résultat du traitement de ces données, qui sont conservés par l'UIP conformément à l'article 12, uniquement au cas par cas et si :*

a) *les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI sont remplies ;*

b) *le transfert est nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2 ;*

c) *le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2, et uniquement avec l'accord exprès dudit État membre ; et*

d) *les mêmes conditions que celles prévues à l'article 9, paragraphe 2, sont remplies.*

2) Nonobstant l'article 13, paragraphe 2, de la décision-cadre 2008/977/JAI, les transferts de données PNR sans l'accord préalable de l'État membre dont les données ont été obtenues, ne sont autorisés que dans des circonstances exceptionnelles et uniquement si :

a) ces transferts sont essentiels pour répondre à une menace précise et réelle liée à une infraction terroriste ou à une forme grave de criminalité dans un État membre ou un pays tiers, et

b) l'accord préalable ne peut pas être obtenu en temps utile.

L'autorité chargée de donner son accord est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

[…]

20 **Article 12** de la directive PNR – Période de conservation et dépersonnalisation des données

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 pouvant servir à identifier directement le passager auquel se rapportent les données PNR :

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR ;

b) *l'adresse et les coordonnées ;* **[Or. 14]**

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne ;

d) les informations "grands voyageurs" ;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte ; et

f) toute donnée API qui a été recueillie.

3) *À l'expiration de la période de six mois visée au paragraphe 2, la communication de l'intégralité des données PNR n'est autorisée que :*

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

b) *lorsqu'elle a été approuvée par :*

i) *une autorité judiciaire ; ou*

ii) *une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post.*

4) *Les États membres veillent à ce que les données PNR soient effacées de manière définitive à l'issue de la période visée au paragraphe 1. Cette obligation s'applique sans préjudice des cas où des données PNR spécifiques ont été transférées à une autorité compétente et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière, auquel cas la conservation de ces données par l'autorité compétente est régie par le droit national.*

5) *Le résultat du traitement visé à l'article 6, paragraphe 2, point a), n'est conservé par l'UIP que le temps nécessaire pour informer les autorités compétentes et, conformément à l'article 9, paragraphe 1, pour informer les UIP des autres États membres de l'existence d'une concordance positive. Lorsque, à la suite du réexamen individuel par des moyens non automatisés visé à l'article 6, paragraphe 5, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées au titre du paragraphe 4 du présent article, de manière à éviter de futures "fausses" concordances positives.*

21 **Article 13** de la directive PNR – Protection des données à caractère personnel

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/JAI. Lesdits articles sont par conséquent applicables.* **[Or. 15]**

2) *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/JAI 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/CE du Parlement européen et du Conseil 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.*

[…]

22 **Annexe I** de la directive PNR – Données des dossiers, telles qu'elles sont recueillies par les transporteurs aériens

1. *Code du dossier passager (PNR)*
2. *Date de réservation/d'émission du billet*
3. *Date(s) prévue(s) du voyage*
4. *nom(s) ;*
5. *Adresse et contact (numéro de téléphone, adresse électronique)*
6. *Moyens de paiement, y compris l'adresse de facturation*
7. *Itinéraire complet pour le PNR concerné*
8. *Informations "grands voyageurs"*
9. *agence de voyage/agent de voyage ;*
10. *Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation*
11. *Indications concernant la scission/division du PNR*
12. *Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur,*

le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée)

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

14. *informations relatives au siège, y compris le numéro du siège occupé* ; **[Or. 16]**

15. *Partage de codes*

16. *Bagages*

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

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

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

23 **Annexe II** de la directive PNR - Liste des infractions visées à l'article 3, point 9)

[…]

6. *la corruption.*

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

[…]

9. *Cybercriminalité*

10. *crimes contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées ;*

[…]

24 La **directive (UE) 2016/680** (JO 2016, L 119, p. 89) dispose :

25 **Article 1er** de la directive (UE) 2016/680 – Objet et objectifs

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.

[…]

26 **Article 3** de la directive (UE) 2016/680 – Définitions

Aux fins de la présente directive, on entend par :

[…]

5. « pseudonymisation » : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles **[Or. 17]** *afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ;*

[…]

27 **Article 4** de la directive (UE) 2016/680 – Principes relatifs au traitement des données à caractère personnel

1) Les États membres prévoient que les données à caractère personnel sont :

a) traitées de manière licite et loyale ;

b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ».

[…]

28 **Article 6** de la directive (UE) 2016/680 – Distinction entre différentes catégories de personnes concernées

Les États membres prévoient que le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que :

a) les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;

b) les personnes reconnues coupables d'une infraction pénale ;

c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ; et

d) les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, **[Or. 18]** *ou des contacts ou des associés de l'une des personnes visées aux points a) et b).*

29 **Article 10** directive (UE) 2016/680 – Traitement portant sur des catégories particulières de données à caractère personnel

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ;

b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

30 **Article 20** de la directive (UE) 2016/680 – Protection des données dès la conception et protection des données par défaut

1) Les États membres prévoient que, compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant lors de la détermination des moyens du traitement que lors du traitement proprement dit, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires, afin de répondre aux exigences de la présente directive et de protéger les droits des personnes concernées.

2) Les États membres prévoient que le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. **[Or. 19]**

31 **Article 35** de la directive (UE) 2016/680 – Principes généraux applicables aux transferts de données à caractère personnel

1) Les États membres prévoient qu'un transfert, par des autorités compétentes, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après leur transfert vers un pays tiers ou à une organisation internationale, y compris des transferts ultérieurs vers un autre pays tiers ou à une autre organisation internationale, n'a lieu, sous réserve du respect des dispositions nationales adoptées en application d'autres dispositions de la présente directive, que lorsque les conditions définies dans le présent chapitre sont respectées, à savoir :

a) le transfert est nécessaire aux fins énoncées à l'article 1er, paragraphe 1 ;

b) les données à caractère personnel sont transférées à un responsable du traitement dans un pays tiers ou à une organisation internationale qui est une autorité compétente aux fins visées à l'article 1er, paragraphe 1 ;

c) en cas de transmission ou de mise à disposition de données à caractère personnel provenant d'un autre État membre, celui-ci a préalablement autorisé ce transfert conformément à son droit national ;

d) la Commission a adopté une décision d'adéquation en application de l'article 36, ou, en l'absence d'une telle décision, des garanties appropriées ont été prévues ou existent en application de l'article 37 ou, en l'absence de décision d'adéquation au titre de l'article 36 et de garanties appropriées conformément à l'article 37, des dérogations pour des situations particulières s'appliquent en vertu de l'article 38 ; et ».

e) en cas de transfert ultérieur vers un autre pays tiers ou à une autre organisation internationale, l'autorité compétente qui a procédé au transfert initial ou une autre autorité compétente du même État membre autorise le transfert ultérieur, après avoir dûment pris en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données à caractère personnel ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données à caractère personnel sont transférées ultérieurement.

2) Les États membres prévoient que les transferts effectués sans l'autorisation préalable d'un autre État membre prévue au paragraphe 1, point c), sont autorisés uniquement lorsque le transfert de données à caractère personnel est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile. L'autorité à laquelle il revient d'accorder l'autorisation préalable est informée sans retard. **[Or. 20]**

3) Toutes les dispositions du présent chapitre sont appliquées de manière que le niveau de protection des personnes physiques assuré par la présente directive ne soit pas compromis.

32 **Article 36** de la directive (UE) 2016/680 – Transferts sur la base d'une décision d'adéquation

1) Les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir

lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

[…]

33 **Article 37** de la directive (UE) 2016/680 – Transferts moyennant des garanties appropriées

1) En l'absence de décision en vertu de l'article 36, paragraphe 3, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque :

a) des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ; ou

b) le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.

[…]

34 **Article 38** de la directive (UE) 2016/680 – Dérogations pour des situations particulières

1) En l'absence de décision d'adéquation en vertu de l'article 36 ou de garanties appropriées en vertu de l'article 37, les États membres prévoient qu'un transfert ou une catégorie de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à condition que le transfert soit nécessaire :

a) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;

b) à la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit de l'État membre transférant les données à caractère personnel le prévoit ;

c) pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ;

d) dans des cas particuliers, aux fins énoncées à l'article 1er, paragraphe 1 ; ou **[Or. 21]**

e) dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les fins énoncées à l'article 1er, paragraphe 1.

2) Les données à caractère personnel ne sont pas transférées si l'autorité compétente qui transfère les données estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert visé au paragraphe 1, points d) et e).

[…]

35 **Article 59** de la directive (UE) 2016/680 – Abrogation de la décision-cadre 2008/977/JAI

1) La décision-cadre 2008/977/JAI est abrogée à compter du 6 mai 2018.

2) Les références faites à la décision abrogée visée au paragraphe 1 s'entendent comme faites à la présente directive.

36 Le **règlement général sur la protection des données** (JO 2016, L 119, p.1) dispose :

37 **Article 4** du règlement général sur la protection des données – Définitions

Aux fins du présent règlement, on entend par :

1. « données à caractère personnel » toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ; 8)

[…]

38 **Article 9** du règlement général sur la protection des données – Traitement portant sur des catégories particulières de données à caractère personnel

1) Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

[…]

[Or. 22]

39 **Article 13** du règlement général sur la protection des données - Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée

1) Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

b) le cas échéant, les coordonnées du délégué à la protection des données ;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

e) le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel ;

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;

2) En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à

la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;

c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

d) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ; **[Or. 23]**

f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

3) Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

4) Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations.

40 Le **FlugDaG** (BGBl. I, p. 1484), dispose :

41 **Article 2** du FlugDaG – Transfert des données par les transporteurs aériens

[…]

2) Les données des dossiers passagers sont les suivantes :

1. Nom de famille, nom de naissance, prénom et titre académique du passager ;

[…]

9. autres indications relatives au nom ;

[…]

3) Les données des passagers sont transmises pour tous les vols de ligne, de charters et de taxis qui n'ont pas une finalité militaire et qui :

a) partent de la République fédérale d'Allemagne et atterrissent dans un autre État, ou

b) partent d'un autre État et atterrissent ou font escale en République fédérale d'Allemagne.

42 **Article 17** du FlugDaG – Compétence juridictionnelle, procédure

La juridiction compétente pour statuer en vertu de la présente loi est l'Amtsgericht dans le ressort duquel le Bundeskriminalamt a son siège. Les dispositions de la loi sur la procédure en matière familiale et de juridiction gracieuse s'appliquent mutatis mutandis à la procédure. **[Or. 24]**

III.

43 La juridiction de céans est compétente pour statuer sur la procédure administrative et, partant, pour la présente demande de décision préjudicielle adressée à la Cour. Cette conclusion n'est pas remise en cause, notamment, par l'article 17 du FlugDaG, selon lequel les décisions judiciaires relèvent de la compétence de l'Amtsgericht dans le ressort duquel le Bundeskriminalamt a son siège. En effet, les « décisions prises en vertu de la présente loi » ne sont que celles visées à l'article 5, paragraphe 2, du FlugDaG. En l'espèce, il s'agit de rendre non pas « une décision au titre de la présente loi » mais une décision sur celle-ci.

44 En l'espèce, la question déterminante pour la solution du litige est de savoir si la directive PNR ou des parties de celle-ci violent la charte des droits fondamentaux. Dans un tel cas, le FlugDaG ne serait pas applicable en tant que loi de transposition, de sorte que le traitement de données dans son ensemble serait illicite et que le droit à la radiation serait ouvert.

Sur la première question

45 Les différents traitements de données PNR prévus par la directive et par la loi de transposition empiètent sur le champ de protection du droit fondamental au respect de la vie privée garanti à l'article 7 de la charte. En effet, ce droit se rapporte à toute information concernant une personne physique identifiée ou identifiable (voir arrêt du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 52) et, partant, également aux informations visées à l'annexe I de la directive PNR relatives aux personnes concernées par le traitement des données. En outre, les traitements des données PNR prévus par la directive PNR relèvent également de l'article 8 de la Charte en raison du fait qu'ils constituent des traitements des 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 avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 123).

46 En effet, selon la jurisprudence de la Cour, la communication de données à caractère personnel à un tiers, telle qu'une autorité publique, constitue une ingérence dans le droit fondamental consacré à l'article 7 de la Charte, quelle que soit l'utilisation ultérieure **[Or. 25]** 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 (voir avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 124). Cela vaut également pour l'article 8 de la charte, pour ce qui concerne le traitement de données à caractère personnel (voir avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 126).

47 Certes, les droits consacrés aux articles 7 et 8 de la charte n'apparaissent pas comme des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 136). Une limitation de ces droits, susceptible de réaliser des objectifs d'intérêt général, dont fait partie la lutte contre les infractions terroristes et les formes graves (voir avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 149), est parfaitement recevable. Toutefois, les atteintes portées aux droits fondamentaux doivent être appropriées et nécessaires à la réalisation de ces objectifs et ne pas s'avérer démesurées au sens strict. Par ailleurs, conformément à l'article 52, paragraphe 1, de la charte, toute limitation de l'exercice des droits et libertés fondamentaux de l'Union doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui (voir avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 138).

48 Le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union **soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause** et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 46). S'agissant du droit fondamental au respect de la vie privée, il convient, selon la jurisprudence de la Cour, d'exiger que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent **[Or. 26] dans les limites du strict nécessaire** (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 52).

49 Pour satisfaire à cette exigence, la réglementation contenant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la

mesure en cause et imposer des exigences minimales. Les personnes dont les données ont été transférées doivent disposer 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. Tel est notamment le cas s'agissant de la protection de la catégorie particulière des données à caractère personnel sensibles (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 54 et suiv.). Il y a lieu de douter sérieusement que la directive PNR soit conforme en tous points à ces exigences.

50 En vertu des dispositions de la directive PNR, les transporteurs aériens sont tenus de transmettre, pour chaque vol individuel, les données PNR de tous les passagers, sans exception, aux centres des PNR des États membres auprès desquels ces données sont traitées et stockées de manière automatisée et durable. Un motif particulier, comme des indices concrets de l'existence d'un lien avec le terrorisme international ou la criminalité organisée, n'est pas nécessaire pour cela. Cela conduit à traiter et à stocker des centaines de billions de données sur de courtes périodes. Partant, la « conservation des données des dossiers passagers » concerne de manière évidente les droits fondamentaux d'une très grande partie de l'ensemble de la population européenne (voir le seul trafic touristique antérieur à la « crise du Coronavirus » ; déjà 226 764 086 passagers transportés par des transporteurs aériens en Allemagne en 2019, 47 millions de vols dans le monde en 2019 ; dans l'Union européenne, 928 634 652 passagers en 2019, chaque vol conduisant à une collecte de données, pour 513,5 millions d'habitants de l'Union européenne en 2019, https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table ?lang=de, au 1er mai 2020). **[Or. 27]**

51 Les données à transférer, définies à l'article 8, paragraphe 1, phrase 1, lu en combinaison avec l'annexe I de la directive PNR, sont très nombreuses et comprennent, outre le nom et l'adresse des passagers ainsi que leur itinéraire complet, des informations relatives à leurs bagages, aux personnes voyageant avec eux, à tous types d'informations relatives aux paiements ainsi qu'à des « remarques générales » non définies. L'ensemble de ces données permet de tirer des conclusions très précises sur la vie privée et professionnelle des personnes concernées. Il en ressort, en effet, qui a voyagé quand pour aller où et en compagnie de qui, le moyen de paiement utilisé à cette fin et les coordonnées de contact indiquées, et si la personne concernée a voyagé avec des bagages légers ou lourds. D'autres données, dont la quantité est parfaitement indéterminable (voir ci-après), peuvent encore figurer dans le champ libre « Remarques générales ».

52 La juridiction de renvoi estime que le traitement et la conservation des données PNR sont comparables à ceux des données dans le domaine des télécommunications. S'agissant de celle-ci, la Cour a précisé à juste titre qu'ils

constituaient une ingérence d'une grande ampleur et d'une gravité particulière dans les articles 7 et 8 de la charte. En effet, une conservation massive, sans réserve, d'une grande quantité de données permettant de tirer des conclusions sur la vie privée et professionnelle des personnes concernées est susceptible de générer chez elles un sentiment de surveillance constante (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 37).

53 Dans son premier arrêt sur la conservation des données, la Cour a jugé celle-ci contraire aux droits fondamentaux, notamment parce que des données relatives à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves doivent également être conservées (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 58). Tel est également le cas du traitement et de la conservation des données PNR, ce qui démontre que les dispositions de la directive PNR dépassent les limites de ce qui est nécessaire pour atteindre les objectifs de ladite directive et sont donc disproportionnés au sens de la jurisprudence de la Cour européenne. Il convient d'ajouter que, à la différence des données relatives au trafic de télécommunications, dans le cadre de la conservation des données, les données PNR sont non seulement enregistrée sans motif particulier, mais aussi traitées ultérieurement, c'est-à-dire par recoupement automatisé avec des bases de données et des « critères préétablis ». **[Or. 28]**

Sur la deuxième question, sous a), relative aux « formes graves de criminalité »

54 Il convient également de s'interroger sur le caractère précis et proportionné de la collecte et du traitement de dossiers de données volumineux au regard des infractions que cette pratique vise à combattre. L'objectif déclaré de la directive PNR est la prévention, la détection, la recherche et la poursuite d'infractions terroristes et de formes graves de criminalité. L'article 3, point 9, de la directive PNR définit les « formes graves de criminalité » comme les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre. L'annexe II de la directive PNR contient une liste de 26 infractions pénales au sens de l'article 3, point 9, de la directive PNR. Tel est le cas, par exemple, de la corruption (point 6), de la fraude (point 7), des infractions informatiques/ de la cybercriminalité (point 9) ainsi que des infractions pénales contre l'environnement (point 10).

55 Tout d'abord, c'est le caractère précis des dispositions qui est en cause en l'espèce. Ainsi, le droit pénal allemand ne connaît pas de délit de « corruption ». En effet, la corruption constitue un terme générique pour un grand nombre d'infractions envisageables. Pour les autorités nationales, il n'y a donc pas de définition claire et univoque des infractions précisément visées par cette disposition. Il en va de même des notions de « fraude », de « cybercriminalité » et

de « infractions contre l'environnement ». Tous ces termes peuvent recouvrir une pluralité d'infractions plus ou moins concrètes.

56 Cela et la référence faite, à l'article 3, point 9, de la directive PNR, à la peine encourue par chaque État membre conduisent à une utilisation divergente des données PNR dans différents États membres de l'Union, dès lors que cela laisse droit pénal de chaque État membre le soin de recenser ou même de ne pas appréhender certaines infractions en tant que « forme grave de criminalité » au sens de ladite directive, en fonction des sanctions pénales prévues par le code pénal national.

57 Est également douteuse, du point de vue du caractère proportionné de la disposition, la « limite minimale » de la peine encourue, d'une durée maximale de trois ans de privation de liberté, fixée à l'article 3, point 9, de la directive PNR. En effet, cette disposition va très loin. **[Or. 29]**

58 Conformément au droit pénal allemand, cela vise un nombre considérable d'infractions dont la qualification en tant que « forme grave de criminalité » paraît très contestable. Ainsi, en vertu de l'article 263 du Strafgesetzbuch (code pénal allemand), la peine encourue est fixée à cinq ans d'emprisonnement pour une fraude ordinaire. Il en va de même, par exemple, du recel (article 259 du code pénal), de la fraude informatique (article 263a du code pénal) ou de l'abus de confiance (article 266 du code pénal). Toutes ces infractions sont susceptibles d'être rattachées à la liste des faits criminels figurant à l'annexe II de la directive PNR et, en particulier, au point 6 de celle-ci, à savoir le point « infractions frauduleuses ». Or, de telles infractions relèvent de la criminalité courante et peuvent se produire également et précisément dans des cas de moindre gravité. Partant, si elles relèvent de la directive PNR, cela n'a rien à voir avec la lutte contre le terrorisme et la prévention et la répression de formes graves de criminalité et il faudrait y renoncer, dans ce contexte, les formes graves de criminalité devant avoir un poids comparable à celui du terrorisme.

59 La juridiction de céans doute sérieusement qu'il soit encore possible de considérer comme appropriée une collecte, à l'exception de la réservation d'un voyage en avion, d'un nombre aussi élevé de données en vue de la poursuite de telles infractions relativement mineures et non spécifiques. La juridiction de renvoi a l'impression que la directive vise moins à lutter contre le terrorisme et les formes graves de criminalité, que, plutôt, à pouvoir poursuivre, en tant que « prises accessoires », un grand nombre d'infractions de gravité moyenne ou mineure (voir également la directive (UE) 2015/849, telle que modifiée par la directive (UE) 2018/843 du Parlement européen et du Conseil, du 30 mai 2018, modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et modifiant les directives 2009/138/CE et 2013/36/UE, dont la mise en œuvre conduit en pratique à la détection d'infractions fiscales, comme la fraude à l'impôt sur les successions, et non pas, justement, à celle du financement du terrorisme ; [OMISSIS]. **[Or. 30]**

60 À l'article 3 de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières du 14 juillet 2012 (JO 2012, L 186, p. 4, tel que rectifié au JO 2012, L 302, p. 14)), le législateur a au moins prévu une dispositions selon laquelle, outre les crimes terroristes, seules les formes graves de criminalité transnationale dont l'objet d'une prévention d'une détection, d'enquête ou de poursuites. La directive PNR n'a même prévu une telle limitation, même si le même problème de concrétisation des différentes infractions se pose. Cela suscite l'impression que le but de la formulation de la directive est d'être très large, à dessein. Cela paraît extrêmement discutable compte tenu de l'atteinte aux droits fondamentaux et de la jurisprudence de la Cour européenne qui exige, dans son interprétation, que cette atteinte se limite au strict nécessaire.

Deuxième question, sous b) : définition suffisamment précise des données PNR

61 Certaines formulations des données PNR que, d'après la liste de l'annexe I de la directive PNR, les transporteurs aériens doivent transférer aux UIP des États membres, n'ont pas la précision suffisante requise par la jurisprudence constante de la Cour qui exige des règles claires et précises quant à la portée et à l'application des mesures concernées (voir seulement avis 1/15, du 26 juillet 2017, EU:C:2017:592, point 141).

62 On ne voit pas clairement ce qu'il faut entendre par « nom(s) » à transférer (annexe I, point 4, de la directive PNR). Cela est bien mis en évidence par l'article 2, points 1 et 9, du FlugDaG, qui prévoit que le nom de famille, le nom de naissance, les prénoms et un éventuel titre académique ainsi que d'autres noms doivent être communiqués. Dans le langage courant, lorsque l'on demande le nom, habituellement, on ne mentionne pas en plus le nom de naissance. Ainsi, il n'est pas certain que celui-ci relève du ou des « nom(s) » visés à l'annexe I, point 4, de la directive PNR. La question se pose également de savoir si un titre académique doit être considéré comme un élément du nom au sens de la directive. **[Or. 31]**

63 En ce qui concerne le transfert et le traitement des données relatives aux informations « grands voyageurs » (annexe I, point 8, de la directive PNR), la disposition manque également de précision. En effet, on ne voit pas clairement ce qu'il faut entendre par là. En particulier, on ne voit pas si cela vise uniquement la participation à des programmes de primes de fidélisation en tant que tels ou également des informations concrètes relatives aux vols et aux réservations de la personne participant à un tel programme.

64 La formulation « Remarques générales, notamment », figurant à l'annexe I, point 12, de la directive PNR est rédigée en termes très larges et incompréhensibles. Ainsi qu'il ressort du terme « *notamment* », il s'agit d'une énumération seulement indicative et non exhaustive. En outre, en remplissant ce

champ libre, il est possible de communiquer également des informations qui n'ont aucun rapport avec les fins de la collecte des données des passagers aériens (voir, déjà, avis 1/15, du 27 juillet 2017, EU:C:2017:592, point 160). Cette formulation pourrait également permettre, notamment, de transmettre des informations que la directive PNR ne cherche pas à autoriser, à savoir, notamment, des données sensibles qui, selon le considérant 15, ne doivent pas être collectées au titre de la directive PNR (voir également, à cet égard, les considérations relatives à la quatrième question).

Sur la deuxième question, sous c) : tiers concernés

65 Aux termes de son article 1er, paragraphe 1, la directive PNR régit le transfert, par les transporteurs aériens, de données des dossiers des passagers (PNR) de vols extra-UE et le traitement de ces données par les États membres. Est un « passager », toute personne, y compris une personne en correspondance ou en transit, 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. Or, à l'annexe I de la directive PNR, sont mentionnées plusieurs données à transférer dans le cadre du traitement des données des dossiers passagers qui ne sont pas celle de « passagers » ainsi définis. Dans cette mesure, les dispositions de la directive PNR sont intrinsèquement contradictoires.

66 Ainsi, cela contredit l'article 3, point 4, de la directive PNR lorsque l'annexe I, point 9, de ladite directive prévoit la collecte, dans le cadre du traitement des données des dossiers passagers, des informations relatives à l'agence de voyages **[Or. 32]** et à l'agent de voyage. Selon le point 12 de l'annexe I de la directive PNR, dans le champ libre « Remarques générales », il convient de fournir notamment des informations sur les accompagnateurs des mineurs au départ et à l'arrivée, ainsi que sur l'agent accompagnateur à l'aéroport.

67 Toutes ces données ne relèvent manifestement pas de la catégorie des passagers aériens définie à l'article 3, point 4, de la directive PNR. Il n'en demeure pas moins que, en contradiction directe avec le libellé de la définition donnée dans la directive PNR, en vertu de ladite directive (en l'occurrence l'annexe I), les transporteurs aériens doivent transférer ces données aux UIP des États membres, où celles-ci doivent être conservées. À cet égard, la juridiction de céans considère que toutes ces dispositions ne se limitent pas au strict nécessaire au sens de la jurisprudence de la Cour (voir seulement avis 1/15, du 27 juillet 2017, EU:C:2017:592, point 141). En outre, pour l'ensemble des tiers intéressés, se pose la question de la manière dont ils doivent être informés du traitement de leurs données à caractère personnel en vertu de l'article 14 du règlement général sur la protection des données.

68 Conformément à l'annexe I, point 17, de la directive PNR, il convient également de transférer et de traiter les données PNR des personnes voyageant avec les

passagers aériens. En ce qui concerne les personnes voyageant avec le passager, cela conduit à une double collecte des données, puisque ceux-ci sont, en tout état de cause, déjà concernés, en tant que passagers aériens, par le traitement des données des dossiers passagers. Partant, il y a là une violation grave du principe de minimisation des données (voir article 5, paragraphe 1, sous c), du règlement général sur la protection des données).

Sur la deuxième question, sous d) : mineurs

69 En vertu de la directive PNR, les transporteurs aériens sont tenus de transférer les données PNR de tous les passagers, sans exception, aux UIP respectives des États membres, de sorte que les passagers aériens mineurs sont également concernés. L'annexe I, point 12, de la directive PNR, qui prévoit la communication des « informations générales, y compris toutes les données disponibles, concernant les mineurs non accompagnés âgés de moins de 18 ans, tels que le nom et le sexe du mineur », le souligne encore une fois.

70 Le traitement de données relatives à des mineurs peut, d'une part, être effectué dans le but d'agir à titre préventif et/ou répressif contre les mineurs (présumés) impliqués dans le **[Or. 33]** terrorisme ou les formes graves de criminalité et, d'autre part, pour des raisons de protection des mineurs, telles que la détection ou la poursuite du trafic d'enfants. Ces deux objectifs distincts nécessitent des régimes différenciés. L'article 6 de la directive (UE) 2016/680 le précise. Cette disposition indique qu'il convient, dans la mesure du possible, d'opérer une distinction claire entre les données à caractère personnel de différentes catégories. Ces catégories distinctes incluent, en particulier, les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale (Art. 6, sous a), de la directive (UE) 2016/680) et les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale (article 6, sous c), de la directive (UE) 2016/680 ; voir, également, considérant 31 de la directive (UE) 2016/680).

71 Toutefois, dans la mesure où les données sont collectées et traitées à des fins répressives ou préventives à l'encontre des mineurs, il faudrait tenir compte du fait que, en tout état de cause, des poursuites pénales ne peuvent être engagées, sur la base des informations tirées du traitement des données des dossiers passagers, que pour les jeunes qui ont déjà commis des infractions. À cet égard, la directive PNR va au-delà des limites du strict nécessaire dans la mesure où elle ne comporte pas de limitation, par exemple, aux données des mineurs ayant fait l'objet de poursuites pénales.

72 En ce qui concerne la collecte et le traitement des données PNR aux fins de la protection des mineurs, il convient de tenir compte du fait que les enfants et les jeunes sont particulièrement vulnérables. Cela est illustré par l'article 24 de la charte, qui leur accorde une protection particulière en leur conférant des droits

fondamentaux propres. Ce besoin particulier de protection vaut également pour le traitement de leurs données à caractère personnel. Dans la mesure où la collecte et le traitement des données PNR des passagers aériens mineurs visent à prévenir et à poursuivre la criminalité contre les mineurs concernés, dirigée contre les enfants, les dispositions de la directive PNR ne paraissent pas appropriées à cette fin. Le traitement des données des données PNR est conçu pour détecter ou reconnaître des personnes suspectes. À cet effet, les données PNR sont recoupées de manière automatisée avec les bases de données et les critères préétablis afin pouvoir **identifier les personnes suspectes**, voir article 6, paragraphe 2, de la directive PNR. Or, dans le contexte de la protection des mineurs contre le trafic d'enfants, les données des mineurs ne sont justement pas des données de suspects, mais, au contraire, des données de personnes qui ont besoin de protection. Dès lors, elles devraient également être traitées différemment. Partant, il n'est justement pas nécessaire de procéder à des comparaisons **[Or. 34]** avec des critères préétablis. À cet égard, il apparaît que la directive PNR ne prévoit pas de règles suffisamment différenciées en ce qui concerne la gestion des données PNR des passagers aériens mineurs.

Sur la deuxième question, sous e) : données API

73 L'article 8, paragraphe 2, de ladite directive prévoit que dans l'hypothèse où les transporteurs aériens ont recueilli des informations préalables sur les passagers (ci-après dénommées « 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 à l'UIP, 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. À cet égard, il existe de nombreux chevauchements entre les données API et les données PNR à transférer de toute façon, telles que les dates prévues du voyage (annexe I, point 3, de la directive PNR), le nom (annexe I, point 4, de la directive PNR) ou l'itinéraire complet (annexe I, point 7, de la directive PNR).

74 Ce double ou multiple traitement des données des passagers aériens est en contradiction avec le principe de minimisation des données consacré, notamment, par la directive (UE) 2016/680. Celui-ci ressort, tout d'abord, de l'article 4, paragraphe 1, sous c), de la directive (UE) 2016/680, lequel prévoit que les données à caractère personnel ne sont pas excessives au regard des finalités pour lesquelles elles sont traitées. L'article 20, paragraphe 1, de la directive (UE) 2016/680 concrétise ce principe en ce sens que les États membres prévoient que le responsable du traitement prend des mesures destinées à mettre en œuvre efficacement les principes relatifs à la protection des données, par exemple la minimisation des données. En outre, l'article 20, paragraphe 2, de la directive

(UE) 2016/680 prévoit que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

75 Un double traitement de certaines données dont le contenu est identique, à savoir tant des données PNR que des données API, est inconciliable avec le principe de minimisation des données et, partant, n'est pas **[Or. 35]** nécessaire. On ne voit aucune raison impérieuse justifiant une telle démarche. Dès lors, selon la juridiction de céans, en raison de la double collecte et du double traitement de ces données, l'atteinte aux articles 7 et 8 de la charte qu'impliquent le transfert de ces données aux UIP des États membres et leur utilisation ne se limite pas au strict nécessaire.

Sur la deuxième question 2, sous f), base juridique des critères préétablis

76 En vertu de l'article 6, paragraphe 3, sous b), de la directive PNR, les dossiers de données transmis par les transporteurs aériens aux UIP des États membres doivent répondre à des critères préétablis. L'article 6, paragraphe 4, deuxième et quatrième phrases, de la directive PNR dispose que les critères préétablis doivent être ciblés, proportionnés et déterminés et que ces critères ne doivent pas reposer sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'affiliation à un syndicat, l'état de santé, la vie sexuelle ou l'orientation sexuelle d'une personne. Conformément à l'article 6, paragraphe 4, première phrase, de la directive PNR, il incombe aux UIP respective des États membres de fixer les critères préétablis.

77 Ainsi, l'ensemble de la conception du recoupement avec des critères préétablis est entièrement confiée au pouvoir exécutif de chaque État membre. Cela a nécessairement pour conséquence de conduire les États membres à utiliser des critères préétablis différents et, partant, à soumettre les passagers, selon la destination du voyage, à des critères préétablis qui peuvent aboutir à des résultats totalement différents.

78 Il convient de se demander si une telle situation est compatible avec l'article 8, paragraphe 2, et l'article 52 de la charte, ainsi qu'avec l'article 16, paragraphe 2, TFUE. Conformément à l'article 8, paragraphe 2, de la charte, ces données doivent être traitées loyalement, **à des fins déterminées** et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Selon l'article 52, paragraphe 1, de la charte, toute limitation de l'exercice des droits et libertés reconnus par celle-ci doit être prévue par la loi. Conformément à l'article 16, paragraphe 2, TFUE, le Parlement européen et le Conseil, statuant **conformément à la procédure législative ordinaire**, adoptent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les **[Or. 36]** institutions, organes et organismes de l'Union ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union.

79 Ainsi le principe de légalité s'applique pour justifier les atteintes aux droits fondamentaux de l'Union en général et, en particulier, à l'article 8 de la charte. Pour satisfaire à cette exigence, il ne faut pas seulement qu'il existe une quelconque disposition législative, il faut aussi que celle-ci soit suffisamment précise (voir seulement, arrêt de la Cour du 21. Décembre 2016, AGET Iraklis, C-201/15, ECLI:EU:C:2016:972, point 99). Le justiciable doit pouvoir prévoir les conséquences de la loi, étant entendu qu'une réglementation ouverte doit être acceptée lorsqu'une réglementation plus précise n'est pas possible pour l'objet de celle-ci (arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, ECLI:EU:C:2003:294, point 77).

80 L'article 6, paragraphe 4, de la directive PNR ne répond pas à ces exigences. L'article 6, paragraphe 4, deuxième phrase, de la directive PNR, est composé de mots imprécis qui feignent une concrétisation des critères qui, en réalité, n'existe pas. Les mots, finalité, précision et proportionnalité ne permettent pas de tirer des conclusions tangibles aux fins de l'élaboration des critères préétablis. On ne sait absolument pas comment les « algorithmes » à développer peuvent exclure de manière fiable une discrimination, expressément interdite aussi par l'article 13, paragraphe 4, de la directive PNR. L'article 6, paragraphe 4, première phrase, de la directive PNR laisse entièrement aux seuls États membres le soin de prendre la décision essentielle et de principe quant aux données utilisées pour établir les critères de recoupement automatisée. Or, cela n'est pas strictement nécessaire eu égard à l'objet de la directive. Le législateur de l'Union aurait très bien pu indiquer certaines données ou critères à utiliser ou non lors de l'élaboration des critères préétablis. À cet égard, ni la criminalité et le terrorisme qui affectent les différents États membres ni les critères permettant d'identifier les suspects ne se distinguent d'un État membre à l'autre. Il en est ainsi, notamment, dans la mesure où les données PNR ont nécessairement un certain caractère intra-UE et international, ne serait-ce qu'en raison du déplacement transfrontalier des personnes concernées. **[Or. 37]**

81 En tant que seul mécanisme de contrôle de la proportionnalité des critères préétablis adoptés par les États membres, l'article 6, paragraphe 7, lu en combinaison avec l'article 5 de la directive PNR prévoit, que le contrôleur de la protection des données de l'UIP a accès à ceux-ci. Toutefois, conformément à l'article 5, paragraphe 1, de la directive PNR, le contrôleur de la protection des données est nommé et, généralement, employé par l'UIP, de sorte que son indépendance n'est pas garantie d'emblée (voir, s'agissant de l'indépendance de l'Autorité, arrêt du 9 mars 2010, Commission/Allemagne, C-518/07, ainsi qu'arrêt du 16 octobre 2012, Commission/Autriche, C-614/10, EU:C:2012:631). Ainsi, l'accès du contrôleur des données ne constitue pas une garantie suffisante de la proportionnalité des critères utilisés par chaque État membre ou par leurs UIP. En l'occurrence, selon la juridiction de céans, une disposition figurant dans la directive PNR elle-même est nécessaire et possible compte tenu de l'objet de ladite directive.

Sur la deuxième question, sous g : durée de conservation

82 En vertu de l'article 12, paragraphe 1, de la directive PNR, les données PNR collectées par les transporteurs aériens et traitées par les UIP des États membres sont conservées pour une période de cinq ans. Selon le considérant 25 de la directive PNR, l'essence même des données PNR et le but du traitement de celles-ci, impliquent que ces données doivent être conservées aussi longtemps que nécessaire. Or, il n'y est justement pas expliqué pourquoi il doit en être ainsi et pourquoi une durée de conservation de cinq ans serait nécessaire.

83 Rien n'explique ni ne justifie pourquoi des durées de conservation aussi longues sont nécessaires. Après que les passagers aériens ont été évalués avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, conformément à l'article 6, paragraphe 4, première phrase, de la directive PNR, sans résultat positif ou autres anomalies, il n'existe aucun indice objectif permettant de considérer qu'ils puissent avoir un lien, même indirect, avec des infractions terroristes ou des formes graves de criminalité. Ainsi, le lien suffisant entre la conservation des données et les objectifs poursuivis par la directive PNR fait défaut. Ce n'est qu'en cas d'indices concrets de danger **[Or. 38]** présenté par certains passagers aériens qu'un stockage durable apparaît approprié (voir, en ce sens, arrêt du 20 juin 1999, Allemagne/Commission, précité, point 42, et avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, points 204 et suivants). En revanche, la **simple possibilité théorique** que les données puissent, un jour, être pertinentes à des fins de sécurité ne devrait pas suffire à justifier l'atteinte grave, sans motif particulier, aux droits fondamentaux que constitue la conservation de données à caractère personnel pendant des années.

84 La durée de conservation longue n'est pas non plus nécessaire et, partant, elle est disproportionnée, dans la mesure où les objectifs de conservation des données des dossiers passagers peuvent être atteints par des mesures moins contraignantes.

85 Ainsi, d'une manière générale, la durée de conservation doit être réduite. La Cour a déjà constaté, dans le contexte de la conservation des données, une autre forme de conservation d'une grande quantité de données à caractère personnel sans motif particulier, qu'une directive qui prévoit une durée de conservation pouvant aller jusqu'à 24 mois ne limite pas l'ingérence au strict nécessaire (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, ECLI : EU : 2014 : 238, point 63). Si une durée de conservation des données de 24 mois est déjà trop longue, une durée de cinq ans, comme en l'espèce, l'est à plus forte raison.

86 Dans la mesure où une durée de conservation plus longue serait objectivement justifiée, il serait possible de prévoir que, lorsque le recoupement automatisé n'a pas produit de « résultat positif » et qu'il n'y a pas eu de vérification individuelle à cet égard, il convient d'effacer ou, à tout le moins, d'anonymiser immédiatement les données PNR. Or, la directive PNR ne prévoit pas une telle différenciation. Pourtant, dès son premier arrêt sur la conservation des données, la Cour a souligné l'importance de la distinction entre différentes catégories de données en fonction

de leur utilité éventuelle au regard de l'objectif poursuivi ou selon les personnes concernées (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 63). En l'absence d'une telle distinction, la durée de conservation de cinq ans prévue par la directive PNR dépasse la limite de ce qui peut être considéré comme strictement nécessaire pour atteindre les objectifs de ladite directive. La « dépersonnalisation » ne remet pas en cause cette conclusion. **[Or. 39]**

Sur la deuxième question, sous h) : dépersonnalisation

87 Selon le considérant 25 de la directive PNR, la « dépersonnalisation » vise à garantir un niveau élevé de protection des données. Cela paraît extrêmement douteux. La « dépersonnalisation » des données à effectuer après six mois, ainsi désignée à l'article 12, paragraphe 2, de la directive PNR, ne change rien au caractère disproportionné de la durée de conservation.

88 Tout d'abord, force est de constater à cet égard que le terme « dépersonnalisation » est incompatible avec l'économie de la directive et trompeur. Il s'agit simplement d'une pseudonymisation des données au sens de l'article 3, point 5, de la directive (UE) 2016/680 et de son annexe I. Cette dernière se distingue d'une anonymisation en ce que, contrairement à celle-ci, l'impossibilité de rattacher les données à une personne donnée n'est pas permanente et définitive, et une dé-dépersonnalisation reste possible (voir article 12, paragraphe 3, de la directive PNR), c'est-à-dire qu'un rattachement direct à une personne peut facilement être rétabli. La raison pour laquelle la notion de pseudonymisation, telle qu'elle est également utilisée dans la directive (UE) 2016/680, n'est pas utilisée n'est donc pas claire. Or, du fait de son caractère réversible, une pseudonymisation réduit nettement moins l'intensité de l'atteinte aux droits fondamentaux qu'une véritable anonymisation.

89 En outre, il convient de prendre en compte l'article 4, paragraphe 1, sous e), de la directive (UE) 2016/680. Selon cette disposition, les données à caractère personnel ne doivent pas être conservées sous une forme permettant l'identification de la personne concernée pendant une durée n'excédant pas celle nécessaire aux fins pour lesquelles elles sont traitées. Dans le cas de la dite « dépersonnalisation » prévue à l'article 12, paragraphe 2, de la directive PNR, une identification de la personne concernée reste possible pendant toute la durée de conservation de cinq ans, ainsi qu'en atteste l'article 12, paragraphe 3, de la directive PNR, qui régit la (la) divulgation (s) au-delà de six mois. Or, il n'apparaît pas que cela soit indispensable aux fins de la directive PNR et n'a pas été motivé par le législateur de l'Union. Comme nous l'avons déjà indiqué, lorsque les données des personnes concernées n'ont présenté aucune anomalie lors du recoupement automatisé des bases de données et des critères préétablis, la possibilité que leurs données deviennent un jour pertinentes à des fins de sécurité est purement théorique. Or, une telle possibilité théorique n'est pas suffisante pour

justifier de conserver les **[Or. 40]** données d'une manière permettant l'identification des personnes concernées, pendant des années.

Sur la deuxième question, sous i) : information après une dé-dépersonnalisation

90 Il n'existe pas, dans la directive PNR, de disposition prévoyant que les personnes concernées soient informées lorsque leurs données, stockées par les UIP des États membres, sont personnalisées conformément à l'article 12, paragraphe 3, de ladite directive. Il est seulement prévu que la dé-dépersonnalisation doit être approuvée par une « autorité judiciaire » ou autre (article 12, paragraphe 3, sous b), de la directive PNR).

91 La Cour a déjà relevé dans son avis sur l'accord PNR UE-Canada, que si cet accord envisagé prévoyait que les passagers aériens devaient être informés du traitement général de leurs données le cadre des contrôles de sécurité et des contrôles aux frontières, cette information générale ne leur permettait pas de savoir si leurs données seraient utilisées par les autorités compétentes au-delà de ces contrôles (avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 223). En outre, aux termes de l'avis de la Cour : « dans les hypothèses […] dans lesquelles se présentent des éléments objectifs justifiant une telle utilisation et nécessitant une autorisation préalable d'une autorité judiciaire ou d'une entité administrative indépendante, une information individuelle des passagers aériens s'avère nécessaire. Il en va de même dans les cas où les données PNR des passagers aériens sont communiquées à d'autres autorités publiques ou à des particuliers » (avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 223).

92 La juridiction de céans estime que cette appréciation de la Cour est transposable à la directive PNR et considère, dès lors, qu'il convient d'informer individuellement les intéressés de la dé-dépersonnalisation de leurs données. Si la Cour devait considérer qu'une notification immédiate de la dé-dépersonnalisation aux intéressés pourrait porter une atteinte trop importante à l'objectif poursuivi de prévention, de détection, de recherche et de poursuite d'infractions terroristes et de formes graves de criminalité, la juridiction de céans estimerait qu'une information des intéressés serait nécessaire au plus tard au moment où il n'y aurait plus à craindre **[Or. 41]** que l'objectif de la dé-dépersonnalisation soit mis en péril, par exemple en raison de la clôture des mesures d'enquête.

93 De même, en vertu de l'article 47 de la charte, l'intéressé a le droit d'obtenir un réexamen devant un tribunal indépendant et impartial, établi préalablement par la loi, et non par une « autorité judiciaire ». Or, en l'espèce, tout recours est exclu et toute voie de recours est fermée.

Sur la troisième question : transfert à des États tiers

94 Conformément à l'article 11, paragraphe 1, de la directive PNR, les données PNR et les résultats du traitement de ces données peuvent, en principe, faire l'objet

d'un transfert au cas par cas vers un État tiers si les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI sont remplies, si le transfert est nécessaire aux fins de la directive PNR, si l'État tiers se déclare prêt à transférer ces données vers un autre État tiers uniquement si cela est strictement nécessaire aux fins de la directive PNR et si l'État membre concerné y consent expressément et si les conditions prévues à l'article 9, paragraphe 2, de cette directive sont remplies.

95 L'article 11, paragraphe 2, de la directive PNR comporte une exception à cette exigence en disposant que, nonobstant l'article 13, paragraphe 2, de la décision-cadre 2008/977/JAI (devenu l'article 38 de la directive (UE) 2016/680), les transferts de données PNR vers des pays tiers sans le consentement préalable de l'État membre auprès duquel ces données ont été obtenues ne sont autorisés que dans des circonstances exceptionnelles, à savoir lorsque ce transfert vers l'État tiers est indispensable pour éviter une menace précise et actuelle d'infractions terroristes ou de formes graves de criminalité dans un État membre ou dans un État tiers, et que le consentement préalable ne peut être obtenu en temps utile.

96 Dans la mesure où la communication à des États tiers donne aux autorités publiques de ces derniers, de fait, accès aux données PNR, tous les principes relatifs à l'utilisation de ces données, qui visent à assurer la proportionnalité des atteintes aux droits fondamentaux qui en découlent et à assurer un niveau adéquat de protection des données à caractère personnel, doivent également s'appliquer auxdits États tiers. À cet égard, la Cour a précisé, dans son avis sur l'accord PNR UE-Canada, qu'un transfert de données à caractère personnel depuis l'Union vers un pays tiers ne peut avoir lieu que si ce pays assure un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union. Cela vise à éviter que le niveau de protection prévu par cet accord puisse être contourné par des transferts de données à caractère personnel vers d'autres pays tiers et à garantir la continuité du niveau de protection offert par le droit de l'Union (avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 214). La Cour en a déduit qu'une telle communication nécessite l'existence soit d'un accord entre l'Union et le pays tiers concerné équivalent audit accord, soit d'une décision de la Commission, au titre de l'article 25, paragraphe 6, de la directive 95/46 (devenu l'article 45, paragraphe 3, du règlement général sur la protection des données), constatant que ledit pays tiers assure un niveau de protection adéquat au sens du droit de l'Union et couvrant les autorités vers lesquelles le transfert des données PNR est envisagé (avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 214).

97 L'article 11 de la directive PNR méconnaît ces conditions. L'article 11, paragraphe 1, sous a), de la directive PNR renvoie à l'article 13 de la décision-cadre 2008/977/JAI. Cette décision-cadre a été abrogée par la directive (UE) 2016/680. Les références à la décision-cadre s'entendent désormais comme faites à la directive (UE) 2016/680 (également appelée « directive relative à la sûreté »), voir article 59 de la directive (UE) 2016/680. À l'article 13 de l'ancienne

décision-cadre 2008/977/JI correspondent, en substance, les articles 35 à 38 de la directive (UE) 2016/680.

98 Conformément à l'article 35, paragraphe 1, sous d), de la directive (UE) 2016/680, le transfert de données vers un État tiers est subordonné à la condition que la Commission ait adopté une décision d'adéquation conformément à l'article 36 de la directive (UE) 2016/680 ou, à défaut, qu'il existe des garanties appropriées au sens de l'article 37 de la directive (UE) 2016/680 ou, à défaut, qu'il s'agisse d'une **situation particulière au sens de l'article 38 de la directive (UE) 2016/680**. À cet égard, le renvoi opéré par l'article 11, paragraphe 1, sous a), de la directive PNR à l'article 13 de la décision-cadre 2008/977/JAI et, partant, à l'article 35 de la directive (UE) 2016/680, ne garantit un niveau adéquat de protection des données par l'État tiers, dans la mesure où il permet, en renvoyant à l'article 38 de la directive (UE) 2016/680, de transmettre des données PNR à des pays tiers, même en l'absence d'une décision d'adéquation ou de garanties appropriées. Il en est ainsi en particulier **[Or. 43]** parce que la notion de situation particulière au sens de l'article 38 de la directive (UE) 2016/680 est conçue de manière très large. En effet, cette disposition permet de transférer des données PNR vers des pays tiers sans niveau adéquat de protection des données lorsque cela est nécessaire, au cas par cas, aux fins de l'article 1er, paragraphe 1, de la directive (UE) 2016/680 (prévention, recherche, détection ou poursuites d'infractions pénales ou exécution d'une peine, y compris la protection contre des risques pour la sécurité publique et la prévention de ces derniers) ou en rapport avec ces fins, pour faire valoir, exercer ou défendre des droits en justice.

Sur la quatrième question : souhaits alimentaires dans le champ libre

99 En vertu de l'article 6, paragraphe 4, première phrase, de la directive PNR, les critères sur la base desquels les données PNR sont recoupées de manière automatisée par les UIP des États membres (« critères préétablis ») ne peuvent en aucun cas être fondés sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'affiliation à un syndicat, l'état de santé, la vie sexuelle ou l'orientation sexuelle.

100 Cela correspond, tout d'abord, à la logique de l'article 10 de la directive (UE) 2016/680 et de l'article 9 du règlement général sur la protection des données, qui régissent le traitement de catégories particulières de données à caractère personnel. Sont des catégories particulières de données à caractère personnel, au sens de ces dispositions, notamment celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données génétiques et biométriques permettant d'identifier clairement une personne physique, des données de santé ou des données relatives à la vie sexuelle ou à l'orientation sexuelle. Le traitement de ces données particulièrement sensibles est, en principe, interdit et ne peut se faire que dans des conditions très strictes. En effet, conformément à l'article 10 de la directive (UE) 2016/680, il est autorisé uniquement en cas de nécessité absolue,

sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ; b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; **[Or. 44]** ou c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

101 Or, la directive PNR ne comporte pas de disposition efficace pour répondre à ces exigences strictes. En effet, l'article 6, paragraphe 4, première phrase, de la directive PNR ne contient qu'une déclaration d'intention qui est contrariée, notamment, par le point 12 de l'annexe I de ladite directive. En effet, par le biais du champ libre qui doit être transmis obligatoirement aux UIP dans tous les cas, sans exception, et de manière absolue, des « Remarques générales », peuvent être transmises aux centres des PNR et exploitées par ceux-ci, notamment des données particulièrement sensibles. Ainsi, ce champ libre pourrait permettre de communiquer [OMISSIS] qu'un passager a souhaité un repas kosher ou des plats halal. Or, il est possible de déduire d'une telle information les convictions religieuses de la personne concernée, de sorte qu'il s'agit d'une donnée particulièrement sensible au sens susmentionné.

102 Selon la juridiction de céans, il n'apparaît pas que le transfert de catégories particulières de données à caractère personnel soit strictement nécessaire dans le cadre du traitement des données des dossiers passagers. En vertu de l'annexe I de la directive PNR, un très grand nombre de données à caractère personnel concrètement identifiées doivent déjà être transférées aux UIP des États membres. La possibilité, par le biais d'un champ libre au contenu pratiquement illimité, de communiquer toutes les autres informations possibles, dépasse probablement la limite du strict nécessaire.

Sur la cinquième question : informations fournies par les transporteurs aériens

103 Conformément à l'article 13, paragraphe 3, de la directive PNR, la présente directive est sans préjudice de l'applicabilité de la directive 95/46/CE du Parlement européen et du Conseil 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. De même, l'article 21, paragraphe 2, de la directive PNR précise encore une fois que l'applicabilité de la directive 95/46/CE au traitement des données à caractère personnel par les compagnies aériennes ne doit pas être affectée. **[Or. 45]**

104 La directive 95/46/CE a été remplacée par le 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 (voir article 94, paragraphe 2, du règlement général sur la protection des données, selon

lequel les références à la directive 95/46/CE s'entendent comme faites au présent règlement).

105 En vertu de l'article 13 du règlement général sur la protection des données, lorsque des données à caractère personnel sont collectées, les personnes concernées reçoivent les informations qui y sont mentionnées. En vertu de l'article 4, point 1, du règlement sur les données à caractère personnel, les données à caractère personnel sont toutes les informations relatives à une personne physique identifiée ou identifiable (ci-après la « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. La collecte des données PNR des passagers et des tiers concernés par les transporteurs aériens constitue une collecte de données à caractère personnel en ce sens, de sorte que, en l'espèce, l'article 13 du règlement sur la protection des données personnelles s'applique aux transporteurs aériens.

106 La juridiction de céans estime que, compte tenu de la gravité des atteintes aux droits fondamentaux que comporte le traitement des données PNR, il convient d'appliquer des critères stricts en ce qui concerne les obligations d'information. Il en est ainsi également parce qu'une information seulement insuffisante des passagers aériens, en violation de l'article 13 du règlement général sur la protection des données, serait susceptible d'entraîner une intensification des atteintes aux droits fondamentaux de la part des UIP des États membres, puisque ces dernières prendraient des mesures encore plus lourdes si les personnes concernées n'avaient pas connaissance de leurs pouvoirs.

107 Selon nous, il incombe aux transporteurs aériens d'informer les personnes concernées en vertu des articles 13 et 14 du règlement général sur la protection des données, sous peine d'une lacune qui serait incompatible avec les articles 7 et 8 du même règlement. Ainsi, il apparaît nécessaire que les transporteurs aériens informent expressément les passagers aériens de l'ensemble des données PNR qu'ils ont collectées, de leur communication prévue aux UIP des **[Or. 46]** États membres et du traitement ultérieur des dossiers dans ces États, y compris de la durée de conservation de cinq ans et de leurs droits précis en tant que personnes concernées. En effet, en l'absence de ces informations, les passagers aériens concernés seraient difficilement en mesure d'exercer lesdits droits des personnes concernées. Ces informations portent également sur le personnel de l'aéroport et des agences de voyages.

108 La directive PNR ne comporte pas de dispositions à cet égard. Elle ne contient que des règles relatives aux droits d'accès aux données PNR auprès des UIP.

109 La Cour a déjà précisé, dans son avis sur l'accord PNR UE-Canada, que, afin d'assurer le respect de ces droits, il importe que les passagers aériens soient

informés du transfert de leurs données PNR vers le Canada et de l'utilisation de ces données dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes conduites par les autorités publiques visées par l'accord envisagé. En effet, une telle information s'avère, de fait, nécessaire pour permettre aux passagers aériens d'exercer leurs droits de demander l'accès aux données PNR les concernant et, le cas échéant, la rectification de celles-ci ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la charte, un recours effectif devant un tribunal (avis 1/15, du 26 juillet 2017, ECLI:EU:C:2017:592, point 220).

110 À titre d'exemple de l'information insuffisante fournie aux passagers par les transporteurs aériens, nous mentionnons, en l'espèce, les indications du transporteur aérien utilisé par le requérant. Les informations figurant sur le site Internet de Lufthansa AG (https://www.lufthansa.com/xx/de/informationen-zum-datenschutz, au 11 mai 2020) sont les suivantes :

« Qui est le responsable ?

Deutsche Lufthansa AG […] vous informe ci-dessous du traitement de vos données à caractère personnel dans le cadre de nos offres. Vous pouvez accéder directement à ces offres via lufthansa.com (« Site Web ») et l'application Lufthansa.

Lorsque nous parlons des Lufthansa Group Airlines ci-dessous, nous entendons les compagnies aériennes Lufthansa, SWISS International Airlines AG, Austrian Airlines AG et Eurowings GmbH. Le groupe Lufthansa comprend Lufthansa Group Airlines et les autres sociétés du groupe Lufthansa. ***[Or. 47]***

Qui puis-je contacter ?

Si vous avez d'autres questions sur la protection des données en relation avec notre site Internet ou les services qui y sont proposés, veuillez contacter notre

délégué à la protection des données […]

Deutsche Lufthansa AG

Datenauskunft

Sur la base de quelles autres obligations traiterons-nous vos données ?

Nous traiterons les données relatives aux passagers aériens en vertu des obligations prévues par la loi, conformément à l'article 6, paragraphe 1, première phrase, sous c), du règlement général sur la protection des données :

Dans la mesure où nous sommes légalement tenus de traiter des données à caractère personnel pour satisfaire à des obligations commerciales ou fiscales ou pour satisfaire à des exigences en matière de sécurité (par exemple, article 7 de la

LuftSiG, loi allemande sur la sécurité aérienne). Vous trouvez d'autres informations concernant les délais de conservation sous « Durée du traitement des données ».

Transferts à des ***autorités compétentes pour l'admission sur le territoire*** :

– en vertu des accords PNR conclus UE-États-Unis ou UE-Canada

– en vertu de la loi PNR en Allemagne

– API * (Advance Passenger Information), pour autant que nous sommes tenus de participer à des activités de contrôle dans le domaine du trafic international de voyageurs.

**Les données des zones de lecture automatique du passeport ou de la carte d'identité*

Vous pouvez obtenir des informations complémentaires auprès des autorités compétentes.

[…]

Qui obtient vos données ?

Dans le contexte des traitements de données à effectuer et des différentes bases juridiques indiquées (mise en œuvre du contrat, intérêt légitime, consentement ou en vertu d'obligations légales de traitement), vos données peuvent être transmises aux catégories de destinataires suivantes :

[…]

organismes et administrations publics, par exemple en vertu de règles d'admission sur le territoire ou d'activités de police et d'enquête.

Il peut arriver que des données à caractère personnel soient transférées vers des pays tiers ou des organisations internationales. Votre protection et la protection de vos données à caractère personnel sont prévues dans le cadre de tels transferts, **[Or. 48]** *conformément aux conditions prévues par la loi.*

Lorsque ces transferts ne reposent pas sur une base légale ou sont effectués dans un pays pour lequel il n'existe pas de décision d'adéquation adoptée par la Commission européenne, nous utiliserons les clauses contractuelles types de l'Union européenne.

De quels droits à la protection des données à caractère personnel disposez-vous ?

Pour Lufthansa, il est important de concevoir nos processus de traitement de manière loyale et transparente. C'est pourquoi nous tenons à ce que, outre le

droit d'opposition dans les conditions légales applicables, les personnes concernées puissent exercer les droits suivants :

droit d'accès, article 15 du règlement général sur la protection des données ;

droit de rectification, article 16 du règlement général sur la protection des données ;

droit à l'effacement (« Droit à l'oubli »), article 17 du règlement général sur la protection des données ;

droit à la limitation du traitement, article 18 du règlement général sur la protection des données ;

droit à la portabilité des données, article 20 du règlement général sur la protection des données ;

droit d'opposition, article 21 du règlement général sur la protection des données.

Pour exercer votre droit, vous pouvez vous adresser par courriel à datenauskunft@dlh.de.

Afin de vous identifier, nous vous demandons de préciser vos :

Nom ;;

adresse postale ;

adresse électronique et, de préférence : numéro de client ou code de réservation ou numéro de billet.

Si vous nous envoyez une copie de votre document d'identité, nous vous demandons d'occulter toutes les informations, sauf le nom, le prénom, l'adresse.

Pour pouvoir traiter votre demande et à des fins d'identification, nous vous signalons que vos données personnelles seront traitées conformément à l'article 6, paragraphe 1, sous c), du règlement général sur la protection des données.

En outre, en vertu de l'article 77 du règlement général sur la protection des données, lu en combinaison avec l'article 19 du Bundesdatenschutzgesetz (loi allemande sur la protection des données), vous avez le droit d'introduire un recours auprès d'une autorité de surveillance. L'autorité de surveillance compétente pour la Lufthansa est :

[…] ».

111 Au vu des considérations qui précèdent, ces informations apparaissent insuffisantes et trompeuses. Ainsi, en particulier, l'indication selon laquelle les

données API concerneraient seulement les zones de lecture automatique du passeport ou de la carte d'identité est manifestement incomplète. En effet, conformément à l'annexe I, point 18, de la directive PNR, les données API, dans la mesure où elles sont collectées, y compris, notamment, le numéro de vol, les **[Or. 49]** jours, heures et lieux d'arrivée et de départ, doivent être transmises, c'est-à-dire, en aucun cas uniquement les zones de lecture automatique. Par ailleurs, aucune référence n'est faite à la directive PNR, il est uniquement fait référence au FlugDaG. En outre, il n'y a aucune référence au contenu de la directive PNR ou du FlugDaG. Ainsi, pour les personnes concernées, avant la réservation de vol, il n'y a de transparence ni quant à l'autorité qui est l'UIP de l'État membre et la façon de s'adresser à celle-ci, ni quant à la manière exacte dont les données PNR y sont traitées ou la durée pendant laquelle elles y sont conservées. Partant, l'information que la Lufthansa fournit aux passagers ne paraît pas satisfaire aux exigences de l'article 13 du règlement général sur la protection des données, sans mentionner les autres personnes devant également faire l'objet d'une notification.

112 Il aurait fallu prévoir un dispositif de clarification entre le règlement général sur la protection des données et la directive PNR en ce qui concerne les différentes obligations de la compagnie aérienne, de façon à éviter de brouiller les pistes.

IV.

113 Il résulte de ce qui précède qu'un renvoi préjudiciel à la Cour s'impose.

114 La solution du litige dépend des questions préjudicielles. En effet, si la directive PNR était contraire au droit primaire de l'Union, la transposition en droit national par le FlugDaG serait également illégale. Cette loi ne pourrait alors pas justifier les atteintes aux droits fondamentaux qu'impliquent le traitement des données PNR, de sorte que la juridiction de renvoi ferait usage de sa compétence pour écarter l'application du FlugDaG en raison de violations du droit de l'Union (de rang supérieur).

115 Un renvoi supplémentaire séparé de la juridiction de céans soulèvera, à titre principal, des questions qui découlent de la clause d'ouverture prévue à l'article 2 de la directive PNR.

V.

116 La décision n'est pas susceptible de recours.

[OMISSIS]