ECLI:EU:C:2022:65

CONCLUSIONS DE L'AVOCAT GÉNÉRAL

M. GIOVANNI PITRUZZELLA

présentées le 27 janvier 2022 (1)

Affaire C-817/19

Ligue des droits humains

contre

Conseil des ministres

[demande de décision préjudicielle formée par la Cour constitutionnelle (Belgique)]

« Renvoi préjudiciel – Protection des données à caractère personnel – Traitement des données des dossiers passagers (PNR) – Règlement (UE) 2016/679 – Champ d'application – Directive (UE)

2016/681 – Validité – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et article 52, paragraphe 1 »

Table des matières

I. **Introduction**

1. Par la présente demande de décision préjudicielle, la Cour constitutionnelle (Belgique) pose à la Cour une série de dix questions préjudicielles portant sur l'interprétation du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après le (« RGPD ») (2), ainsi que sur la validité et sur l'interprétation de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (ci-après la « directive PNR ») (3) et de la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (ci-après la « directive API ») (4). Ces questions ont été soulevées dans le cadre d'un recours introduit par l'association sans but lucratif Ligue des droits humains (LDH), visant à l'annulation totale ou partielle de la loi du 25 décembre 2016 relative au traitement des données des passagers (ci-après la « loi PNR ») (5), transposant en droit belge la directive PNR ainsi que la directive API.

2. Les questions que la Cour devra trancher dans la présente affaire s'inscrivent dans le cadre de l'un des principaux dilemmes du constitutionnalisme libéral démocratique contemporain : comment convient-il de définir l'équilibre entre l'individu et la collectivité à l'ère des données, lorsque les technologies numériques ont permis la collecte, la conservation, le traitement et l'analyse d'énormes masses de données à caractère personnel à des fins prédictives ? Les algorithmes, l'analyse des big data et l'intelligence artificielle utilisés par les autorités publiques peuvent servir à promouvoir et à protéger les intérêts fondamentaux de la société, avec une efficacité autrefois inimaginable : de la protection de la santé publique à la durabilité environnementale, de la lutte contre le terrorisme à la prévention de la criminalité, en particulier la criminalité grave. Dans le même temps, la collecte indifférenciée de données à caractère personnel et l'utilisation des technologies numériques par les pouvoirs publics peuvent donner naissance à un panoptique numérique, c'est-à-dire à un pouvoir public qui voit tout sans être vu. Un pouvoir omniscient qui peut contrôler et prévoir les comportements de tout un chacun et prendre les mesures qui s'imposent, jusqu'au résultat paradoxal, imaginé par Steven Spielberg dans le film *Minority Report*, d'ôter la liberté de manière préventive à l'auteur d'un délit qui n'a pas encore été réalisé. Comme on le sait, dans certains pays, la société prime sur l'individu et l'utilisation des données personnelles permet légitimement de réaliser une surveillance de masse efficace visant à protéger des intérêts publics considérés comme fondamentaux. À l'inverse, le constitutionnalisme européen – national et supranational – avec la place centrale accordée à l'individu et à ses libertés, met une barrière importante à l'avènement d'une société de la surveillance de masse, surtout après la reconnaissance des droits fondamentaux à la protection de la vie privée et à la protection des données à caractère personnel. Dans quelle mesure, cependant, cette barrière peut-elle être érigée sans porter gravement atteinte à certains intérêts fondamentaux de la société – tels que ceux précédemment cités à titre d'exemple – qui peuvent pourtant avoir des liens constitutionnels ? Nous sommes au cœur de la question de la relation entre individu et collectivité dans la société numérique. Une question qui nécessite, d'une part, la recherche et la mise en œuvre d'équilibres délicats entre les intérêts de la collectivité et les droits des individus, en partant de l'importance absolue que ces derniers ont dans le patrimoine constitutionnel européen, et d'autre part, la mise en place de garanties contre les abus. Ici aussi, nous sommes dans le cadre de la version contemporaine d'un thème classique du constitutionnalisme, car, comme l'affirmait de manière lapidaire *Le Fédéraliste*, les hommes ne sont pas des anges et c'est pourquoi des mécanismes juridiques sont nécessaires pour limiter et contrôler la puissance publique.

3. Telles sont les questions d'ordre général qui s'inscrivent dans le contexte des présentes conclusions, qui ne pourront que se limiter à interpréter le droit de l'Union, à la lumière de la jurisprudence antérieure de la Cour, en employant des techniques bien établies, parmi lesquelles figure celle de l'interprétation conforme. Une technique à laquelle on aura recours souvent, lorsque cela apparaît juridiquement possible, dans les présentes conclusions, dans le but de trouver l'équilibre nécessaire, du point de vue constitutionnel, entre les finalités publiques qui sous-tendent le système de transfert, de collecte et de traitement des données des dossiers passagers (ci-après les « données PNR »), et les droits consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

II. Le cadre juridique

A. Le droit de l'Union

1. *La Charte*

4. Aux termes de l'article 7 de la Charte, « [t]oute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

5. Aux termes de l'article 8 de la Charte :

« 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. Conformément à l'article 52, paragraphe 1, de la Charte « [t]oute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

2. *Le RGPD*

7. L'article 2, paragraphe 2, sous d), du RGPD exclut du champ d'application de ce règlement le traitement de données à caractère personnel effectué « par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces ».

8. Aux termes de l'article 23, paragraphe 1, sous d), du RGPD :

« Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22,

lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :

[...]

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

3. ***La directive PNR***

9. Je ne donnerai ci-après qu'un bref aperçu du fonctionnement du système instauré par la directive PNR. Plus de détails sur le contenu des dispositions de la directive PNR pertinente aux fins de la réponse à donner aux questions préjudicielles seront fournis au cours de l'analyse juridique.

10. Conformément à son article 1er, la directive PNR, adoptée sur la base de l'article 82, paragraphe 1, sous d), TFUE et de l'article 87, paragraphe 2, sous a), TFUE, organise, à l'échelle de l'Union européenne, un système de transfert, par les transporteurs aériens, des données PNR de vols extra-UE (6), ainsi que de collecte, de traitement et de conservations de ces données par les autorités compétentes des États membres à des fins de lutte contre le terrorisme et la criminalité grave.

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

12. L'annexe I de la directive PNR (ci-après l'« annexe I »), énumère les données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens, qui font l'objet de transfert au sens et selon les modalités prévues à l'article 8 de cette directive.

13. L'annexe II de la directive PNR (ci-après l'« annexe II ») contient la liste des infractions qui constituent des « formes graves de criminalité » au sens de l'article 3, point 9, de cette directive.

14. L'article 2 de la directive PNR prévoit la possibilité, pour les États membres, de décider d'appliquer cette directive également aux « vols intra-UE » (7) ou à certains d'entre eux, jugés « nécessaires » afin de poursuivre les objectifs de ladite directive.

15. Aux termes de l'article 4, paragraphe 1, de la directive PNR, « [c]haque 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 [unité d'informations passagers] UIP ». Conformément au paragraphe 2, sous a), de cet article 4, l'UIP est notamment chargée de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, ainsi que du transfert de ces données ou du résultat de leur traitement aux autorités compétentes visées à l'article 7 de la directive PNR. Aux termes du paragraphe 2, de cet article 7, ces autorités sont « des autorités compétentes en matière de prévention ou de détection des

infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes ou de poursuites en la matière » (8).

16. Aux termes de l'article 6, paragraphe 1, seconde phrase, de la directive PNR, « 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 ». Le paragraphe 2 de cet article est rédigé comme suit :

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

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

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

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

17. L'article 12 de la directive PNR contient les dispositions relatives à la conservation des données PNR.

18. L'article 5 de la directive PNR prévoit que chaque 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. En outre, chaque État membre est tenu, conformément à l'article 15 de cette directive, de charger l'autorité nationale de contrôle visée à l'article 25 de la décision-cadre 2008/977/JAI (9), remplacée par la directive (UE) 2016/680, du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après la « directive police ») (10), de surveiller l'application, sur son territoire, des dispositions adoptées en vertu de ladite directive. Cette autorité, qui exerce ses tâches en ayant en vue la protection des droits fondamentaux en matière de traitement des données à caractère personnel (11), est notamment chargée, d'une part, de traiter les réclamations introduites par toute personne concernée, d'enquêter sur l'affaire et d'informer la personne concernée de l'état d'avancement du dossier et de l'issue de la réclamation dans un délai raisonnable, et, d'autre part, de vérifier la licéité du traitement des données, d'effectuer des enquêtes, des inspections et des audits conformément au droit national, de sa propre initiative ou en se fondant sur une réclamation (12).

4. ***Autres actes pertinents de droit de l'Union***

19. Le cadre juridique de la présente affaire est complété par la directive API et la directive police. Pour des raisons de lisibilité des présentes conclusions, le contenu des dispositions pertinentes de ces actes sera exposé dans la mesure où cela s'avère nécessaire pour le traitement des questions qui les concernent ou, plus généralement, pour les besoins de l'analyse juridique.

B. **Le droit belge**

20. Conformément à l'article 22 de la Constitution belge, « [c]hacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi ».

21. Aux termes de son article 2, la loi PNR transpose la directive API et la directive PNR, ainsi que, partiellement, la directive 2010/65/UE (13).

22. Conformément à son article 3, § 1, la loi PNR « détermine les obligations des transporteurs et des opérateurs de voyage relatives à la transmission des données des passagers à destination du, en provenance du et transitant par le territoire national ». Aux termes de l'article 4, points 1 et 2, de cette loi, l'on entend par « transporteur » « toute personne physique ou morale qui assure, à titre professionnel, le transport de personnes par voie aérienne, maritime, ferroviaire ou terrestre » et par « opérateur de voyage » « tout organisateur ou intermédiaire de voyage, au sens de la loi du 16 février 1994 régissant le contrat d'organisation de voyages et le contrat d'intermédiaire de voyages ».

23. L'article 8 de la loi PNR dispose :

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

1° de la recherche et la poursuite, en ce compris l'exécution des peines ou des mesures limitatives de liberté, relatives aux infractions visées à l'article 90 ter, § 2, [...] 7°, [...] 8°, [...] 11°, [...] 14°, [...] 17°, 18°, 19° et § 3, du Code d'instruction criminelle ;

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

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

4° du suivi des activités visées aux articles 7, 1° et 3°/1, et 11, § 1er, 1° à 3° et 5°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (14) ;

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

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

24. L'article 9 de la loi PNR contient la liste des données qui font l'objet de transfert. Ces données correspondent à celles énumérées à l'annexe I.

25. Conformément à l'article 18 de la loi PNR, « les données des passagers sont conservées dans la banque de données des passagers pour une durée maximale de cinq ans à compter de leur enregistrement. À l'issue de ce délai, elles sont détruites ».

26. L'article 19 de cette loi prévoit que, « [à] l'expiration d'une période de six mois, à compter de l'enregistrement des données des passagers dans la banque de données des passagers, toutes les données des passagers sont dépersonnalisées, par masquage des éléments d'information ».

27. L'article 24 de la loi PNR prévoit :

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

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

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

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

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

28. L'article 25 de la loi PNR reprend le contenu de l'article 6, paragraphe 4, de la directive PNR.

29. Le chapitre 11 de la loi PNR contient les dispositions régissant le traitement des données des passagers en vue de l'amélioration du contrôle aux frontières et de la lutte contre l'immigration illégale. Ces dispositions constituent la transposition en droit belge de la directive API.

30. L'article 44 de la loi PNR prévoit que l'UIP désigne un délégué à la protection des données au sein du service public fédéral intérieur. La surveillance sur l'application des dispositions de la loi PNR est exercée par la Commission de la protection de la vie privée.

31. L'article 51 de la loi PNR modifie la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, en insérant un article 16/3 rédigé comme suit :

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, décider de façon dûment motivée d'accéder aux données des passagers visés à l'article 7 de la loi [PNR].

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

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

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

C. **Le litige au principal, les questions préjudicielles et la procédure devant la Cour**

32. Par une requête adressée à la Cour constitutionnelle le 24 juillet 2017, la LDH a introduit un recours visant l'annulation totale ou partielle de la loi PNR. À l'appui de son recours, elle a invoqué deux moyens.

33. Par son premier moyen, avancé à titre principal et tiré de la violation de l'article 22 de la Constitution belge, lu en combinaison avec l'article 23 du RGPD, les articles 7, 8, et l'article 52, paragraphe 1, de la Charte ainsi que l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »), la LDH estime que la loi attaquée ne respecte pas le principe de proportionnalité quant à son champ d'application et aux catégories de données visées, aux traitements de données qu'elle instaure, à ses finalités et à la durée de conservation des données. En particulier, elle soutient que la définition des données PNR est trop large et susceptible d'aboutir à la révélation de données sensibles, et que la définition de la notion de « passager » contenue dans cette loi permet un traitement systématique non ciblé des données de tous les passagers concernés. En outre, la LDH considère que la loi PNR ne définit pas de manière suffisamment claire la nature et les modalités de la méthode de *pre-screening* des banques de données des passagers ainsi que les critères servant d'« indicateurs de menace ». Enfin, elle est d'avis que la loi PNR excède les limites du strict nécessaire, en ce sens qu'elle poursuit des finalités de traitement des données PNR plus larges que celles admises par la directive PNR et que le délai de cinq ans pour la conservation des données PNR est disproportionné. Par son second moyen, avancé à titre subsidiaire et tiré de la violation de l'article 22 de la Constitution belge, lu en combinaison avec l'article 3, paragraphe 2, TUE et avec l'article 45 de la Charte, la LDH s'attaque aux dispositions du chapitre 11 de la loi PNR qui transposent la directive API.

34. Le Conseil des ministres du Royaume de Belgique, en tant que partie intervenante devant la Cour constitutionnelle, s'oppose au recours de la LDH, en contestant tant la recevabilité que le bien-fondé des deux moyens soulevées à son appui.

35. La Cour constitutionnelle avance, pour sa part, les considérations suivantes.

36. S'agissant du premier moyen, elle s'interroge, tout d'abord, sur le point de savoir si la définition des données PNR, figurant à l'annexe I, est suffisamment claire et précise. La description de certaines de ces données revêtirait un caractère exemplatif et non exhaustif. Ensuite, ladite juridiction relève que la définition de la notion de « passager » figurant à l'article 3, point 4, de la directive PNR entraîne la collecte, le transfert, le traitement et la conservation des données PNR de toute personne transportée ou devant être transportée et inscrite sur la liste des passagers, indépendamment de l'existence de motifs sérieux de croire que la personne concernée ait commis une infraction ou est sur le point de commettre une infraction, ou ait été reconnue coupable d'une

infraction. S'agissant des traitements des données PNR, elle observe que ces dernières font systématiquement l'objet d'une évaluation préalable impliquant le croisement des données PNR de tous les passagers avec des banques de données ou des critères préétablis, en vue d'établir des correspondances. Néanmoins, la Cour constitutionnelle précise que, si les critères doivent être spécifiques, fiables et non discriminatoires, il lui apparaît techniquement impossible de définir davantage les critères préétablis qui serviront à la détermination de profils à risque. En ce qui concerne le délai de conservation des données PNR prévu à l'article 12, paragraphe 1, de la directive PNR en vertu duquel lesdites données peuvent être conservées pour une période de cinq ans, la juridiction de renvoi considère que les données PNR seraient conservées sans tenir compte de la question de savoir si les passagers concernés seraient, dans le cadre de l'évaluation préalable, susceptibles ou non de présenter un risque pour la sécurité publique. Dans ces conditions, la juridiction de renvoi s'interroge sur le point de savoir si, eu égard à la jurisprudence issue notamment de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (15) et de l'avis1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (16), le système de collecte, de transfert, de traitement et de conservation des données PNR établi par la directive PNR peut être considéré comme ne dépassant pas les limites du strict nécessaire. Dans ce contexte, cette juridiction s'interroge, également, sur le point de savoir si la directive PNR s'oppose à une réglementation nationale, telle que celle résultant de l'article 8, paragraphe 1, point 4), de la loi PNR, qui autorise le traitement des données PNR pour une finalité autre que celles prévues par cette directive. Enfin, elle se demande si l'UIP peut être considéré comme « autre autorité nationale » susceptible, en vertu de l'article 12, paragraphe 3, sous b), ii), de la directive PNR, d'autoriser la communication de l'intégralité des données PNR après un délai de six mois. Quant au second moyen, la juridiction de renvoi relève que celui-ci est dirigé contre l'article 3, paragraphe 1, l'article 8, paragraphe 2, ainsi que les articles 28 à 31 de la loi PNR régissant la collecte et le traitement des données des passagers aux fins de lutter contre l'immigration illégale et d'améliorer les contrôles aux frontières. Rappelant que, selon la première de ces dispositions, cette loi couvre les vols à destination du territoire national, en provenance de celui-ci et transitant par celui-ci, cette juridiction précise que le législateur national avait inclus les vols « intra-UE » dans le champ d'application de ladite loi afin d'obtenir « un tableau plus complet des passagers qui constituent une menace potentielle pour la sécurité [au sein de l'Union] et nationale », en se fondant sur la possibilité prévue à l'article 2 de la directive PNR, lu en combinaison avec le considérant 10 de celle-ci.

37. C'est dans ce contexte que la Cour constitutionnelle a décidé de surseoir à statuer et de poser à la Cour des questions préjudicielles suivantes :

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

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

3) Les points 12 et 18 de l'annexe I [...] sont-ils compatibles avec les articles 7, 8, et l'article 52, paragraphe 1, de la [Charte], en ce que, compte tenu des termes "notamment" et "y compris", les données qu'ils visent sont mentionnées à titre exemplatif et non exhaustif, de sorte que l'exigence de précision et de clarté des règles emportant une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel ne serait pas respectée ?

4) L'article 3, point 4), de la directive [PNR] et l'annexe I [...] sont-ils compatibles avec les articles 7, 8, et l'article 52, paragraphe 1, de la [Charte], en ce que le système de collecte, de transfert et de traitement généralisés des données des passagers que ces dispositions instaurent vise toute personne qui utilise le moyen de transport concerné, indépendamment de tout élément objectif permettant de considérer que cette personne est susceptible de présenter un risque pour la sécurité publique ?

5) L'article 6 de la directive [PNR], lu en combinaison avec les articles 7, 8, et l'article 52, paragraphe 1, de la [Charte], doit-il être interprété comme s'opposant à une législation nationale telle que la loi attaquée, qui admet, comme finalité du traitement des données PNR, le suivi des activités visées par les services de renseignement et de sécurité, intégrant ainsi cette finalité dans la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que dans les enquêtes et les poursuites en la matière ?

6) L'article 6 de la directive [PNR] est-il compatible avec les articles 7, 8, et l'article 52, paragraphe 1, de la Charte, en ce que l'évaluation préalable qu'il organise, par une corrélation avec des banques de données et des critères préétablis, s'applique de manière systématique et généralisée aux données des passagers, indépendamment de tout élément objectif permettant de considérer que ces passagers sont susceptibles de présenter un risque pour la sécurité publique ?

7) La notion d'"autre autorité nationale compétente" visée à l'article 12, paragraphe 3, de la directive [PNR] peut-elle être interprétée comme visant l'UIP créée par la loi [PNR], qui pourrait dès lors autoriser l'accès aux données PNR, après un délai de six mois, dans le cadre de recherches ponctuelles ?

8) L'article 12 de la directive [PNR], lu en combinaison avec les articles 7, 8, et l'article 52, paragraphe 1, de la [Charte] doit-il être interprété comme s'opposant à une législation nationale telle que la loi attaquée qui prévoit un délai général de conservation des données de cinq ans, sans distinguer si les passagers concernés se révèlent, dans le cadre de l'évaluation préalable, susceptibles ou non de présenter un risque pour la sécurité publique ?

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

b) La directive [API], lue en combinaison avec l'article 3, paragraphe 2, [TUE] et avec l'article 45 de la [Charte], doit-elle être interprétée comme s'opposant à une législation nationale telle que la loi attaquée qui, aux fins de lutter contre l'immigration illégale et d'améliorer les contrôles aux frontières, autorise un système de collecte et de traitement des données des passagers "à destination du, en provenance du et transitant par le territoire national", ce qui pourrait impliquer indirectement un rétablissement des contrôles aux frontières intérieures ?

10) Si, sur la base des réponses données aux questions préjudicielles qui précèdent, la Cour constitutionnelle devait arriver à la conclusion que la loi attaquée, qui transpose notamment la directive [PNR], méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi [PNR] afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées aux fins visées par [cette] loi ? »

38. Des observations écrites ont été déposées, en vertu de l'article 23 du statut de la Cour de justice de l'Union européenne, par la LDH, par les gouvernements belge, tchèque, danois, allemand,

estonien, irlandais, espagnol, français, chypriote, letton, néerlandais, autrichien, polonais, finlandais, ainsi que par le Parlement européen, le Conseil de l'Union européenne, et la Commission européenne. Conformément à l'article 24 du statut de la Cour de justice de l'Union européenne, la Commission, le Contrôleur européen de la protection des données (CEPD) et l'Agence des droits fondamentaux de l'Union européenne (FRA) ont été invités à répondre par écrit à des questions posées par la Cour. Une audience de plaidoiries s'est déroulée le 13 juillet 2021.

III. **Analyse**

A. **Sur la première question préjudicielle**

39. Par sa première question préjudicielle, la juridiction de renvoi demande en substance à la Cour si l'article 2, paragraphe 2, sous d), du RGPD doit être interprété en ce sens que ce règlement, et notamment son article 23, paragraphe 1, aux termes duquel le droit de l'Union ou les droits des États membres peuvent, par la voie de mesures législatives, limiter, pour des raisons exhaustivement énumérées, la portée des obligations et des droits prévus par ledit règlement, s'applique aux traitements de données effectués sur le fondement d'une législation nationale, telle que la loi PNR, transposant en droit interne la directive PNR ainsi que la directive API et la directive 2010/65.

40. L'article 2, paragraphe 2, du RGPD prévoit des exceptions au champ d'application de ce règlement, tel que défini, de manière très large (17), à son article 2, paragraphe 1 (18). En tant que dérogations à l'application d'une réglementation régissant le traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales, ces exceptions doivent recevoir une interprétation stricte (19).

41. L'article 2, paragraphe 2, sous d), du RGPD contient, notamment, une clause d'exclusion aux termes de laquelle ce règlement ne s'applique pas au traitement de données à caractère personnel effectué « par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces ». Cette clause d'exclusion se fonde sur un double critère subjectif et objectif. Sont ainsi exclus du champ d'application dudit règlement les traitements de données effectués, premièrement, par les « autorités compétentes » et, deuxièmement, aux fins énumérées à cette disposition. Il convient, dès lors, d'apprécier les différents types de traitement de données couverts par la loi PNR au regard de ce double critère.

42. S'agissant, en premier lieu, des traitements de données effectués par les transporteurs (aériens, ferroviaires, terrestres et maritimes) à l'UIP ou par les opérateurs de voyage *à des fins de prestation de service ou commerciales*, pour autant que visés par ladite loi, ils demeurent régis par le RGPD, étant donné que ni le volet subjectif ni le volet objectif du critère d'exclusion contenu à l'article 2, paragraphe 2, sous d), de ce règlement ne sont remplis.

43. En ce qui concerne, en deuxième lieu, le *transfert par les transporteurs ou les opérateurs de voyage des données PNR à l'UIP*, qui constitue, en soi, un « traitement » au sens de l'article 4, point 2, du RGPD (20), son inclusion dans le champ d'application de ce règlement est moins évidente.

44. En effet, d'une part, ce transfert n'est pas opéré par une « autorité compétente » au sens de l'article 3, point 7), de la directive police, auquel il convient de se référer par analogie, en l'absence de définition de cette notion par le RGPD (21). Un opérateur économique, tel qu'une compagnie de

transport ou une agence de voyage, auquel incombe uniquement une obligation légale de transfert de données à caractère personnel et auquel n'a été confiée aucune prérogative de puissance publique (22), ne saurait être considéré comme un organisme ou une entité au sens dudit article 3, point 7, sous b) (23).

45. D'autre part, le transfert des données PNR par les compagnies de transport et les opérateurs de voyage est effectué pour exécuter une obligation imposée par la loi dans le but de permettre la poursuite des fins énumérées à l'article 2, paragraphe 2, sous d), du RGPD.

46. Or, il ressort à mon sens clairement du libellé de cette disposition que seuls les traitements qui répondent à la fois au volet subjectif et au volet objectif du critère d'exclusion qu'elle énonce se situent en dehors du champ d'application du RGPD. Le transfert des données PNR à l'UIP imposé par la loi PNR aux compagnies de transport et aux opérateurs de voyage relève dès lors de ce règlement.

47. Pour ce qui est des dispositions de la loi PNR transposant la directive PNR, cette conclusion est corroborée par l'article 21, paragraphe 2, de cette directive, qui prévoit que celle-ci « s'applique sans préjudice de l'applicabilité de la directive 95/46/CE (24) au traitement des données à caractère personnel par les transporteurs aériens ». La lecture de cette disposition que suggère, notamment, le gouvernement français, selon laquelle celle-ci se borne à prévoir que les transporteurs restent soumis aux obligations fixées par le RGPD pour les traitements de données qui ne sont pas prévus par la directive PNR, doit à mon sens être écartée. En effet, au vu de son libellé, la portée de cette « clause de non-préjudice » est large et se définit uniquement par référence à l'auteur du traitement, aucune mention n'étant faite de la finalité du traitement ou du cadre dans lequel celui-ci intervient, s'il est effectué dans l'exercice de l'activité commerciale du transporteur aérien ou en exécution d'une obligation légale. J'observe, en outre, qu'une clause de la même teneur est contenue à l'article 13, paragraphe 3, de la directive PNR, qui se réfère tout particulièrement aux obligations incombant aux transporteurs aériens en vertu du RGPD « de prendre des mesures techniques et organisationnelles appropriées pour protéger la sécurité et la confidentialité des données à caractère personnel ». Or, cette disposition figure parmi celles qui organisent la protection des données personnelles traitées au titre de la directive PNR et suit l'article 13, paragraphe 1, de cette directive, qui, de manière générale, soumet tout traitement de données effectué en application de celle-ci aux dispositions de la décision-cadre 2008/977 qui y sont mentionnées. Contrairement à ce que soutient le gouvernement français, un tel agencement normatif permet, d'une part, de lire le paragraphe 3 dudit article 13 comme une clause ramenant sous l'empire du RGPD le seul traitement de données prévu par la directive PNR qui n'est pas effectué par des « autorités compétentes » au sens de la directive police et, d'autre part, de comprendre la référence au respect des obligations imposées par ledit règlement en matière de sécurité et de confidentialité des données comme un rappel des garanties qui doivent obligatoirement entourer le transfert des données PNR par les transporteurs aux UIP.

48. La conclusion énoncée au point 46 des présentes conclusions n'est pas remise en cause par le considérant 19 du RGPD et par le considérant 11 de la directive police, auxquels font, entre autres, référence les gouvernements allemand, irlandais et français pour soutenir la nature de lex specialis de la directive PNR. À cet égard, il est certes vrai que cette directive instaure, pour les traitements de données à caractère personnel qu'elle vise, un cadre de protection de ces données autonome par rapport au RGPD. Cependant, ce cadre spécifique ne s'applique qu'aux traitements des données PNR effectués par les « autorités compétentes », aux sens de l'article 3, point 7, de la directive police, au nombre desquelles figurent notamment les UIP, alors que le transfert des données PNR aux UIP reste soumis au cadre général établi par le RGPD en application, entre autres, de la « clause de non-préjudice » prévue à l'article 21, paragraphe 2, de la directive PNR.

49. À l'appui de leur thèse selon laquelle le RGPD ne s'applique pas au transfert des données PNR aux UIP par les transporteurs et les opérateurs de voyage, les gouvernements belge, irlandais, français et chypriote renvoient à l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (25), dans lequel la Cour a dit pour droit que le transfert des données PNR par des transporteurs aériens communautaires aux autorités des États-Unis d'Amérique, dans le cadre d'un accord négocié entre ces derniers et la Communauté européenne, constituait un traitement de données à caractère personnel au sens de l'article 3, paragraphe 2, premier tiret, de la directive 95/46 (26) et ne relevait dès lors pas du champ d'application de cette directive. Pour arriver à cette conclusion, la Cour a tenu compte de la *finalité du transfert* ainsi que du fait que celui-ci « s'insérait dans un cadre institué par les pouvoirs publics », bien que les données fussent collectées et transférés par des opérateurs privés (27).

50. À cet égard, il suffit de relever que, dans l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (28), la Cour a, en substance, considéré l'arrêt Parlement/Conseil comme étant non transposable dans le contexte du RGPD (29).

51. Par ailleurs, au point 102 de l'arrêt La Quadrature du Net (30), procédant à une application par analogie du raisonnement suivi dans les arrêts Tele2 Sverige et du 2 octobre 2018, Ministerio Fiscal (31), la Cour a affirmé que, « si le [RGPD] précise, à son article 2, paragraphe 2, sous d), qu'il ne s'applique pas aux traitements "effectués par les autorités compétentes" à des fins, notamment, de prévention et de détection des infractions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, il ressort de l'article 23, paragraphe 1, sous d) et h), du même règlement que les traitements de données à caractère personnel effectués à ces mêmes fins par des particuliers relèvent du champ d'application de celui-ci » (32).

52. Pour les raisons déjà exposées, je suis persuadé que la conclusion selon laquelle le transfert des données PNR par les compagnies de transport et les opérateurs de voyage aux UIP relève du RGPD ressort déjà clairement du libellé de l'article 2, paragraphe 2, sous d), du RGPD, qui ne se réfère qu'aux traitements effectués par des « autorités compétentes », sans qu'il soit nécessaire de se référer à la clause de limitation contenue à l'article 23, paragraphe 1, dudit règlement (33). Néanmoins, l'affirmation contenue au point 102 de l'arrêt La Quadrature du Net constitue une prise de position claire de la Cour en faveur d'une telle conclusion.

53. Puisque le transfert des données PNR par les compagnies de transport et les opérateurs de voyage tombent dans le champ d'application du RGPD, une législation nationale, telle la loi PNR, qui oblige ces compagnies et ces opérateurs à opérer un tel transfert, constitue une « mesure législative » au titre de l'article 23, point 1, sous d), du RGPD et doit, dès lors, répondre aux conditions prévues à cette disposition (34).

54. S'agissant, en troisième lieu, des traitements des données PNR effectués *par l'UIP et les autorités nationales compétentes*, l'applicabilité du RGPD dépend, ainsi que cela ressort des développements qui précèdent, des finalités que ces traitements poursuivent.

55. Ainsi, premièrement, les traitements de données PNR effectués par l'UIP et par les autorités nationales compétentes pour les finalités énumérées à l'article 8, § 1, points de 1 à 3 et 5, de la loi PNR (35), sont exclus du champ d'application du RGPD dans la mesure où, comme cela semble être le cas, lesdites finalités se rangent parmi celles couvertes par la clause d'exclusion inscrite à l'article 2, paragraphe 2, sous d), du RGPD. La protection des données des personnes concernées par ces traitements relève du droit national, sous réserve de l'application de la directive police (36) et, dans le cadre de son champ d'application, de la directive PNR.

56. Il en va de même, deuxièmement, des traitements des données PNR effectués par l'UIP et par les services de sécurité et de renseignement dans le cadre du suivi des activités visées aux dispositions de la loi organique des services de renseignement et de sécurité énumérées à l'article 8, § 1, point 4, de la loi PNR, dans la mesure où ils répondent aux finalités énoncées à l'article 2, paragraphe 2, sous d), du RGPD, ce qu'il incombe à la juridiction de renvoi d'apprécier.

57. Le gouvernement belge soutient que les traitements effectués au titre de l'article 8, § 1, point 4, de la loi PNR tombent en tous cas sous le coup de la clause d'exclusion prévues à l'article 2, paragraphe 2, sous a), du RGPD, ainsi que de celle prévue à l'article 2, paragraphe 3, sous a), de la directive police, étant donné que les activités des services de sécurité et de renseignement ne relèvent pas du champ d'application du droit de l'Union.

58. À cet égard, tout en soulignant que la Cour n'est pas saisie d'une question visant l'interprétation de ces dispositions, je relève, tout d'abord, que la Cour a déjà affirmé qu'une réglementation nationale imposant des obligations de traitement à des opérateurs privés relève des dispositions du droit de l'Union en matière de protection des données à caractère personnel, même lorsqu'elle vise la protection de la sécurité nationale (37). Il s'ensuit que le transfert des données PNR imposé par la loi PNR aux transporteurs et aux opérateurs de voyage relève en principe du RGDP même lorsqu'il est effectué aux fins de l'article 8, § 1, point 4, de cette loi.

59. Ensuite, je relève que, si le considérant 16 du RGPD énonce que celui-ci ne s'applique pas aux « activités relatives à la sécurité nationale » et le considérant 14 de la directive police précise qu'« il convient que les activités relatives à la sécurité nationale, les activités des agences ou des services responsables des questions de sécurité nationale [...] ne soient pas considérées comme des activités relevant du champ d'application de [cette] directive », les critères sur le fondement desquels un traitement de données personnelles effectué par une autorité, un service ou une agence publics d'un État membre tombe dans le champ d'application de l'un ou de l'autre acte de droit de l'Union organisant la protection des personnes concernées à l'égard de tels traitements ou se situe en dehors du champ d'application de ce droit répondent à une logique liée tant aux fonctions attribuées à cette autorité, à ce service ou à cette agence qu'aux finalités dudit traitement. Ainsi, la Cour a-t-elle jugé que l'article 2, paragraphe 2, sous a), du RGPD, lu à la lumière du considérant 16 de ce règlement, « doit être considéré comme ayant pour seul objet d'exclure du champ d'application dudit règlement les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité qui vise à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie, de telle sorte que le seul fait qu'une activité soit propre à l'État ou à une autorité publique ne suffit pas pour que cette exception soit automatiquement applicable à une telle activité » (38). La Cour a également précisé que « les activités qui ont pour but de préserver la sécurité nationale visées à l'article 2, paragraphe 2, sous a), du RGPD couvrent, en particulier [...] celles ayant pour objet de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société » (39). Il en résulte que, dans le cas où un État membre chargerait ses services de sécurité et de renseignement de missions dans les domaines énumérés à l'article 3, point 7, sous a), de la directive police, les traitements de données effectués par ces services pour l'accomplissement de ces missions tomberaient dans le champ d'application de cette directive ainsi que, le cas échéant, de la directive PNR. De manière plus générale, je relève que la Cour a itérativement jugé, dans le cadre de l'interprétation de l'article 4, paragraphe 2, TUE, sur lequel s'appuie entre autres le gouvernement belge, que le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit (40), se montrant ainsi réticente à une exclusion automatique et en bloc du champ d'application du droit de l'Union des activités des États membres liées à la protection de la sécurité nationale.

60. Troisièmement, conformément à l'avis de tous les intéressés ayant présenté des observations, à l'exception du gouvernement français, il y a lieu de considérer que les traitements des données PNR effectués par les autorités compétentes belges pour les finalités énoncées à l'article 8, § 2, de la loi PNR, à savoir « l'amélioration des contrôles de personnes aux frontières extérieures et [la lutte] contre l'immigration illégale » (41) ne relèvent pas de la clause d'exclusion contenue à l'article 2, paragraphe 2, sous d), du RGPD, ni d'une autre cause d'exclusion prévue à cet article et tombent, dès lors, dans le champ d'application de ce règlement. Contrairement à ce que soutient le gouvernement français, lesdits traitements ne sauraient être régis par la directive PNR, dont l'article 1er, paragraphe 2, établit que « [l]es 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 » ni, en principe, par la directive police, qui, conformément à son article 1, paragraphe 1, ne s'applique qu'aux traitements de 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 ». Ainsi qu'il ressort de la décision de renvoi, l'article 8, § 2, de la loi PNR et le chapitre 11 de cette loi, qui contient les dispositions régissant le traitement des données PNR en vue de l'amélioration du contrôle aux frontières et de la lutte contre l'immigration illégale, et qui prévoit à cette fin le transfert de ces données par l'UIP notamment aux services de police chargés du contrôle des frontières, visent à transposer en droit belge la directive API et la directive 2010/65. Or, ces deux directives imposent aux autorités compétentes, pour les traitements qu'elles prévoient, le respect des dispositions de la directive 95/46 (42). Contrairement à ce que soutient le gouvernement français, le renvoi aux règles protectrices de cette directive doit s'entendre comme couvrant tout traitement de données à caractère personnel effectués sur la base de la directive API et de la directive 2010/65. Le fait que la directive API soit antérieure à l'entrée en vigueur de la décision-cadre 2008/977 n'est pas pertinent à cet égard puisque cette décision-cadre, ainsi que la directive police qui l'a remplacée, ne concernent que les traitements de données à caractère personnel visées à l'article 3, paragraphe 1, de la directive API, effectués par les autorités compétentes à des fins répressives (43).

61. Sur la base de l'ensemble des considérations qui précèdent, je propose à la Cour de répondre à la première question préjudicielle que l'article 23 du RGPD, lu en combinaison avec l'article 2, paragraphe 2, sous d), de ce règlement, doit être interprété en ce sens :

– qu'il s'applique à une législation nationale transposant la directive PNR dans la mesure où cette législation régit les traitements des données PNR effectués par les transporteurs et par d'autres opérateurs économiques, y inclus le transfert de données PNR aux UIP, prévu à l'article 8 de ladite directive ;

– qu'il ne s'applique pas à une législation nationale transposant la directive PNR dans la mesure où celle-ci régit les traitements de données effectués pour les finalités prévues à l'article 1er, paragraphe 2, de cette directive par les autorités nationales compétentes, y incluses les UIP et, le cas échéant, les services de sécurité et de renseignement de l'État membre intéressé ;

– qu'il s'applique à une législation nationale transposant la directive API et la directive 2010/65 en vue de l'amélioration du contrôle de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale.

B. **Sur les deuxième, troisième, quatrième, sixième et huitième questions préjudicielles**

62. Par ses deuxième, troisième, quatrième et sixième questions préjudicielles, la Cour constitutionnelle interroge la Cour sur la validité de la directive PNR à l'égard des articles 7, 8, et de l'article 52, paragraphe 1, de la Charte. La huitième question préjudicielle, bien qu'étant libellée comme une question d'interprétation, vise, elle aussi, en substance, à obtenir de la Cour qu'elle se prononce sur la validité de cette directive.

63. Ces questions portent sur les différents éléments du système de traitement des données PNR établi par la directive PNR et sollicitent, par rapport à chacun de ces éléments, une évaluation du respect des conditions auxquelles est soumise la légalité des limitations apportées à l'exercice des droits fondamentaux énoncés aux articles 7 et 8 de la Charte. Ainsi, les deuxième et troisième questions préjudicielles visent le catalogue des données PNR figurant à l'annexe I, la quatrième concerne la définition de la notion de « passager » visée à l'article 3, point 4), de la directive PNR, la sixième porte sur l'utilisation des données PNR aux fins de l'évaluation préalable au titre de l'article 6 de cette directive et la huitième concerne le délai de conservation des données PNR prévu à l'article 12, paragraphe 1, de ladite directive.

1. ***Sur les droits fondamentaux énoncés aux articles 7 et 8 de la Charte***

64. L'article 7 de la Charte garantit à toute personne le droit au respect de sa vie privée et familiale, de son domicile et de ses communications. Quant à l'article 8, paragraphe 1, de la Charte, celui-ci reconnaît explicitement à toute personne le droit à la protection des données à caractère personnel la concernant. Selon une jurisprudence constante, ces droits, qui se rapportent à toute information concernant une personne physique identifiée ou identifiable, sont étroitement liés, l'accès à des données à caractère personnel d'une personne physique en vue de leur conservation ou de leur utilisation affectant le droit de cette personne au respect de la vie privée (44).

65. Les droits consacrés aux articles 7 et 8 de la Charte n'apparaissent cependant pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (45). L'article 8, paragraphe 2, de la Charte autorise ainsi le traitement des données à caractère personnel si certaines conditions sont réunies. Cette disposition prévoit que les données à caractère personnel 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 ».

66. Toute limitation apportée au droit à la protection des données personnelles, ainsi qu'au droit à la vie privée, doit en outre respecter les prescriptions de l'article 52, paragraphe 1, de la Charte. Ainsi, une telle limitation doit être prévue par la loi, respecter le contenu essentiel desdits droits et, dans le respect du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

67. L'appréciation d'une mesure limitant lesdits droits doit tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte, et de celle qui revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui (46). À cet égard, l'article 6 de la Charte consacre le droit de toute personne non seulement à la liberté mais également à la sûreté (47).

68. Par ailleurs, l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits énoncés dans celle-ci et les droits correspondants garantis par la CEDH, dont il convient de tenir compte en tant que seuil de protection minimale (48). Le droit au respect de la vie privée et familiale, consacré à l'article 7 de la Charte, correspond à celui garanti à l'article 8 de la

CEDH et doit, par conséquent, se voir reconnaître le même sens et la même portée (49). Il ressort de la jurisprudence de la Cour européenne des droits de l'homme (ci-après la « Cour EDH ») qu'une ingérence dans les droits garantis à cet article ne peut se justifier au regard du paragraphe 2 dudit article que si elle est prévue par la loi, vise un ou plusieurs des buts légitimes énumérés dans ce paragraphe et est nécessaire, dans une société démocratique, pour atteindre ce ou ces buts (50). La mesure doit aussi être compatible avec la prééminence du droit, expressément mentionnée dans le préambule de la CEDH et inhérente à l'objet et au but de l'article 8 de celle-ci (51).

69. C'est à la lumière de ces principes qu'il convient d'examiner les questions en appréciation de validité posées par la Cour constitutionnelle.

2. ***Sur l'ingérence dans les droits fondamentaux énoncés aux articles 7 et 8 de la Charte***

70. La Cour a déjà jugé que des dispositions imposant ou permettant la communication de données personnelles de personnes physiques à un tiers, telle une autorité publique, doivent être qualifiées, en l'absence de consentement de ces personnes physiques et quelle que soit l'utilisation ultérieure des données en cause, d'ingérences dans leur vie privée et, partant, de limitation apportée au droit fondamental garanti à l'article 7 de la Charte, sans préjudice de leur éventuelle justification (52). Il en est ainsi même en l'absence de circonstances permettant de qualifier une telle ingérence de « grave » et sans qu'il importe 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 ladite ingérence (53). L'accès des autorités publiques à de telles informations constitue pareillement une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel (54). De même, constitue en soi une ingérence dans les droits garantis aux articles 7 et 8 de la Charte la conservation, pendant une certaine durée, des données relative à la vie privée d'une personne (55).

71. La Cour a également déjà jugé que les données PNR, telles que celles énumérées à l'annexe I, comportent des informations sur des personnes physiques identifiées, à savoir les passagers aériens concernés, et que, dès lors, les différents traitements dont ces données peuvent faire l'objet affectent le droit fondamental au respect de la vie privée, garanti à l'article 7 de la Charte. Ces traitements relèvent également de l'article 8 de la Charte et doivent, par suite, nécessairement satisfaire aux exigences de protection des données prévues à cet article (56).

72. Ainsi, les traitements des données PNR que permet la directive PNR et, notamment, pour ce qui revêt un intérêt aux fins de la présente affaire, le transfert de ces données par les transporteurs aériens aux UIP, leur utilisation par ces unités, leur transfert ultérieur vers des autorités nationales compétentes au sens de l'article 7 de cette directive, ainsi que leur conservation constituent autant d'ingérences dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte.

73. Quant à la gravité de ces ingérences, il y a lieu de relever, premièrement, que la directive PNR prévoit le transfert *systématique* et *continu* aux UIP des données PNR de tout passager aérien, tel que cela est défini à l'article 3, point 4, de cette directive, empruntant un vol « extra-UE » au sens de l'article 3, point 2, de celle-ci. Un tel transfert implique un accès général de la part des UIP à toutes les données PNR communiquées (57). Cette constatation n'est pas remise en cause, contrairement à ce que font valoir certains États membres dans la présente procédure, par la circonstance que, puisque ces données sont soumises à un traitement automatisé, les UIP n'auront concrètement accès qu'aux données dont l'analyse a produit un résultat positif. En effet, d'une part, une telle circonstance n'a, à ce jour, pas empêché la Cour d'affirmer, dans le cadre de systèmes similaires de traitement automatisé de données personnelles collectées ou conservées « en vrac », le

caractère général de l'accès des autorités publiques concernées à de telles données. D'autre part, la simple mise à la disposition des autorités publiques de données à caractère personnel en vue de leur traitement et de leur conservation par ces autorités comporte un accès a priori général et complet de celles-ci à de telles données et une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel.

74. Deuxièmement, conformément à l'article 2, paragraphe 1, de la directive PNR, les États membres peuvent décider d'appliquer cette dernière aux vols « intra-UE » au sens de l'article 3, point 3, de celle-ci. À cet égard, je relève, d'une part, que la directive PNR ne se limite pas à prévoir la faculté pour les États membres d'étendre son application aux vols intra-UE, mais elle détermine également les conditions tant formelles que matérielles régissant l'exercice de cette faculté (58) et précise que, lorsque celle-ci n'est exercée que pour certains vols intra-UE, la sélection de ces vols doit être opérée en tenant compte des objectifs poursuivis par ladite directive (59). D'autre part, la directive PNR établit les conséquences de l'exercice d'une telle faculté, en prévoyant, à son article 2, paragraphe 2, que, lorsqu'un État membre décide d'appliquer cette directive aux vols intra-UE, toutes les dispositions de celle-ci « 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 ».

75. Dans ces circonstances, je suis d'avis, contrairement à ce qu'ont fait valoir un certain nombre de gouvernements ayant présenté des observations dans la présente procédure que, bien que l'application de la directive PNR aux vols intra-UE dépende du choix des États membres, la base légale des ingérences dans les droits au respect de la vie privée et à la protection des données à caractère personnel liées au transfert, au traitement et à la conservation des données PNR relatives à ces vols est constituée, lorsqu'un tel choix est effectué, par la directive PNR.

76. Or, mis à part le Royaume de Danemark, qui n'est pas soumis à cette directive (60), presque tous les États membres appliquent le régime établi par celle-ci aux vols « intra-UE » (61). Il s'ensuit que ce régime s'applique à tous les vols entrant et sortant de l'Union ainsi qu'à quasiment tous les vols opérés au sein de l'Union.

77. Troisièmement, s'agissant des données PNR à transférer, l'annexe I énumère 19 rubriques, visant des données biographiques (62), les détails du voyage aérien (63) et d'autres données recueillies dans le contexte du contrat de transport aérien, telles que le numéro de téléphone, l'adresse électronique, les modes de paiement, l'agence ou l'agent de voyage, les informations relatives aux bagages ainsi que des remarques générales (64). Or, ainsi que la Cour l'a indiqué au point 128 de l'avis 1/15, se prononçant sur les rubriques figurant à l'annexe du projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers (ci-après le « projet d'accord PNR Canada-UE »), formulées de manière largement analogues à celles de l'annexe I, « même si certaines des données PNR, prises isolément, ne paraissent pas pouvoir révéler des informations importantes sur la vie privée des personnes concernées, il n'en demeure pas moins que, prises ensemble, lesdites données peuvent, entre autres, révéler un itinéraire de voyage complet, des habitudes de voyage, des relations existant entre deux ou plusieurs personnes ainsi que des informations sur la situation financière des passagers aériens, leurs habitudes alimentaires ou leur état de santé, et pourraient même fournir des informations sensibles sur ces passagers ».

78. Quatrièmement, aux termes de l'article 6 de la directive PNR, les données transférées par les transporteurs aériens sont destinées à être analysées par les UIP par des moyens automatisés et cela *de manière systématique*, c'est-à-dire indépendamment du point de savoir s'il existe la moindre indication que les personnes concernées risquent d'être impliquées dans des infractions de

terrorisme ou des formes graves de criminalité. Plus particulièrement, dans le cadre de l'évaluation préalable des passagers prévue à l'article 6, paragraphe 2, sous a), de cette directive et conformément au paragraphe 3, de cet article, lesdites données peuvent être vérifiées par recoupement avec des bases de données « utiles » [article 6, paragraphe 3, sous a)] et traitées au regard de critères préétablis [article 6, paragraphe 3, sous b)]. Or, le premier type de traitement est susceptibles de fournir des informations supplémentaires sur la vie privée des personnes concernées (65) et, en fonction des bases de données utilisées pour le recoupement, peut même permettre de tracer un *profil précis* de ces personnes. Dans ces circonstances, l'objection soulevée par plusieurs gouvernements, selon laquelle la directive PNR ne permet l'accès qu'à un ensemble de données personnelles relativement limité ne reflète pas de manière adéquate l'étendue potentielle des ingérences que cette directive comporte dans les droits fondamentaux protégés par les articles 7 et 8 de la Charte, sous l'angle de l'étendue des données auxquelles elle est susceptible de permettre l'accès. S'agissant du second type de traitement de données, prévu à l'article 6, paragraphe 3, sous b), de la directive PNR, je rappelle que, aux points 169 et 172 de l'avis 1/15, la Cour a souligné qu'il est inhérent à tout type d'analyse fondée sur des critères préétablis de présenter un certain taux d'erreur, et notamment un certain nombre de résultats « faux positifs ». Selon les données chiffrées contenues dans le document de travail des services de la Commission (66) (ci-après le « document de travail de 2020 ») annexé au rapport de la Commission de 2020, le nombre de cas de concordances positives s'étant, à la suite du réexamen individuel prévu à l'article 6, paragraphe 5, de la directive PNR, révélées erronées est assez conséquent et s'élevait, au cours des années 2018 et 2019, à au moins cinq sur six personnes identifiées (67).

79. Cinquièmement, conformément à l'article 12, paragraphe 1, de la directive PNR, les données PNR sont conservées dans une base de données pendant une période de cinq ans suivant leur transfert à l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol. La directive PNR permet, dès lors, de disposer d'informations sur la vie privée des passagers aériens sur une durée particulièrement longue (68). Par ailleurs, puisque le transfert des données PNR concerne la presque totalité des vols opérés au départ et à l'entrée de l'Union ainsi qu'au sein de celle-ci et que l'avion est devenu un moyen de transport plutôt habituel, une partie significative de passagers aériens pourraient voir leurs données personnelles conservées de manière pratiquement permanente, du seul fait qu'ils se déplacent en avion au moins deux fois tous les cinq ans.

80. Enfin, sur un plan plus général, la directive PNR prévoit des mesures qui, considérées globalement, visent à mettre en place au niveau de l'Union un système de surveillance « non ciblée », à savoir non déclenchée en fonction d'un soupçon pesant sur une ou plusieurs personnes spécifiques, « massive », en ce qu'elle s'exerce sur les données à caractère personnel d'un grand nombre d'individus (69), couvrant une même catégorie de personnes dans son entièreté (70) et « proactive », dans la mesure où elle vise non seulement à enquêter sur des menaces connues, mais également à trouver ou à identifier des dangers jusque-là inconnu (71). De telles mesures donnent lieu, par leur nature même, à des ingérences graves dans les droits fondamentaux protégés par les articles 7 et 8 de la Charte (72), liées notamment à leur finalité préventive et prédictive, qui nécessite l'évaluation de données à caractère personnel relatives à de larges segments de la population, le but étant d'« identifier » les personnes qui devraient, en fonction des résultat de cette évaluation, être soumises à un examen plus approfondi par les autorités compétentes (73). Par ailleurs, le recours de plus en plus généralisé, à des fins de prévention de certaines formes graves de criminalité, au traitement de grandes quantités de données à caractère personnel de nature diverse collectées « en vrac », ainsi que leur mise en relation et leur traitement combiné entraînent un « effet cumulatif » qui amplifie la gravité des restrictions aux droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, et risque de favoriser un processus de glissement graduel vers une « société de surveillance » (74).

81. Sur la base de l'ensemble des considérations qui précèdent, j'estime que l'ingérence que comporte la directive PNR dans les droits fondamentaux protégés par les articles 7 et 8 de la Charte doit à tout le moins être qualifiée de « grave ».

82. Il est vrai, ainsi que le soutient, en particulier, la Commission, que l'ensemble des garanties et des garde-fous que la directive PNR prévoit, notamment pour éviter une utilisation abusive des données PNR, est susceptible de réduire l'intensité ou la gravité de ces ingérences. Il n'en demeure pas moins que tout régime prévoyant l'accès et le traitement de données à caractère personnel de la part d'autorités publiques présente un niveau de gravité, sous l'angle de la protection des droits fondamentaux impactés, qui est inhérent à ses caractéristiques objectives. Ce niveau de gravité doit, à mon sens, être déterminé avant de procéder, dans le cadre de l'appréciation de la proportionnalité desdites ingérences, à l'évaluation du caractère suffisant et adéquat des garanties que ce régime prévoit. C'est ainsi que la Cour a, me semble-t-il, procédé jusqu'à présent.

83. Pour être compatibles avec la Charte, les ingérences que la directive PNR comporte dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel doivent satisfaire aux conditions énoncées aux points 65 et 66 des présentes conclusions, ce qui sera examiné ci-après dans les limites des aspects qui ont été soumis à l'attention de la Cour par la juridiction de renvoi.

3. *Sur la justification de l'ingérence résultant de la directive PNR*

84. Alors que la troisième question préjudicielle porte sur le respect de la condition visée à l'article 52, paragraphe 1, première phrase, de la Charte, selon laquelle toute ingérence dans un droit fondamental doit être « prévue par la loi », les deuxième, quatrième, sixième et huitième questions préjudicielles interrogent la Cour notamment sur le respect du principe de proportionnalité, visé à la seconde phrase de cette disposition.

a) *Sur le respect de l'exigence selon laquelle toute limitation à l'exercice d'un droit fondamental prévu par la Charte doit être prévue par la loi*

85. Selon une jurisprudence bien établie de la Cour (75), s'inspirant de la jurisprudence de la Cour EDH (76), l'exigence selon laquelle toute limitation à l'exercice d'un droit fondamental doit être « prévue par la loi » ne vise pas uniquement l'origine « légale » de l'ingérence – qui n'est pas en cause dans la présente affaire –, mais implique aussi que la base légale qui permet cette ingérence doit définir elle-même, de manière *claire* et *précise*, la portée de celle-ci. Ayant trait à la « qualité de la loi » et, donc, à l'accessibilité et à la prévisibilité de la mesure en cause (77), ce second volet que recouvre l'expression « prévue par la loi » au sens tant de l'article 52, paragraphe 1, de la Charte que de l'article 8, paragraphe 2, de celle-ci et de l'article 8 de la CEDH vise non seulement à assurer le respect du principe de légalité et une protection adéquate contre l'arbitraire (78), mais répond également à un impératif de sécurité juridique. Cette exigence est aussi affirmée dans l'avis du 19 août 2016 du comité consultatif de la convention 108 (79) sur les implications en matière de protection de données du traitement des données passagers (ci-après « l'avis du 19 août 2016 ») (80).

86. En adoptant la directive PNR, le législateur de l'Union a procédé lui-même à la limitation des droits consacrés aux articles 7 et 8 de la Charte. Les ingérences que cette directive permet dans lesdits droits ne sauraient donc être considérées comme la conséquence du choix des États membres (81), malgré la marge d'appréciation dont ces derniers ont pu bénéficier au moment de sa transposition dans le droit national, mais trouvent leurs base légale dans la directive PNR elle-même. Dans ces conditions, il incombait au législateur de l'Union, afin de se conformer à la

jurisprudence rappelée au point 80 des présentes conclusions, ainsi qu'aux « normes élevées » de protection des droits fondamentaux contenues notamment dans la Charte et dans la CEDH auxquelles se réfère le considérant 15 de la directive PNR, d'édicter des règles claires et précises définissant tant la portée que l'application des mesures comportant lesdites ingérences.

87. Si, par sa troisième question préjudicielle, la juridiction de renvoi s'interroge spécifiquement sur le respect de cette obligation à l'égard des points 12 et 18 de l'annexe I, l'examen des deuxième, quatrième et sixième questions préjudicielles, par lesquelles cette juridiction soulève des doutes quant au caractère nécessaire des ingérences que comporte la directive PNR dans les droits fondamentaux énoncés aux article 7 et 8 de la Charte, requerra également de prendre position sur le caractère suffisamment clair et précis des dispositions de la directive PNR mises en cause.

88. Bien que cette analyse ait trait, ainsi que je l'ai exposé au point 85 des présentes conclusions, à la légalité de l'ingérence, au sens de l'article 52, paragraphe 1, première phrase, de la Charte, j'y procéderai dans le cadre de l'examen de sa proportionnalité, visé à la seconde phrase de ce paragraphe, conformément à l'approche suivi tant par la Cour que par la Cour EDH dans les affaires où sont en cause des mesures ayant pour objet le traitement des données personnelles (82).

b) ***Sur le respect du contenu essentiel des droits énoncés aux articles 7 et 8 de la Charte***

89. Conformément à l'article 52, paragraphe 1, première phrase, de la Charte, toute restriction apportée à l'exercice des droits fondamentaux doit non seulement reposer sur une base légale suffisamment précise, mais également respecter le *contenu essentiel* de ces droits.

90. Ainsi que je l'ai exposé au point 66 des présentes conclusions, cette exigence – que l'on retrouve incorporée dans les constitutions de différents États membres (83), et qui, tout en n'étant pas expressément reconnue par la CEDH, est néanmoins bien ancrée dans la jurisprudence de la Cour EDH (84) – se trouve inscrite à l'article 52, paragraphe 1, de la Charte (85). Reconnue par la Cour bien avant sa codification (86), une telle exigence a été constamment réaffirmée dans la jurisprudence des juridictions de l'Union, même après l'entrée en vigueur du traité de Lisbonne.

91. Il ressort notamment de l'arrêt du 6 octobre 2015, Schrems (87), que le non-respect du contenu essentiel d'un droit fondamental par un acte de l'Union entraîne *de manière automatique* la nullité ou l'invalidité de celui-ci, sans qu'il soit nécessaire de procéder à un balancement des intérêts en jeu. La Cour reconnaît ainsi que tout droit fondamental présente un « noyau dur », garantissant à tout un chacun une sphère de liberté à l'abri de toute ingérence par les pouvoirs publics et qui ne peut subir de limitations (88), sauf à remettre en question les principes démocratique, de l'État de droit et du respect de la dignité humaine qui sous-tendent la protection des droits fondamentaux. Il ressort, par ailleurs, tant du libellé de l'article 52, paragraphe 1, de la Charte que de la jurisprudence de la Cour, et, notamment, de l'arrêt Schrems I, que l'appréciation portant sur l'existence d'une ingérence dans le contenu essentiel du droit fondamental en cause doit être menée préalablement à et indépendamment de l'évaluation de la proportionnalité de la mesure incriminée. Il s'agit, en d'autres termes, d'un test doté de sa propre autonomie.

92. Cela étant, déterminer ce que constitue le « contenu essentiel », et, dès lors, intouchable, d'un droit fondamental susceptible d'être limité dans son exercice est une opération extrêmement complexe. Si, pour remplir sa fonction, cette notion devrait pouvoir être définie en des termes absolus, eu égard aux caractéristiques essentielles du droit fondamental en cause, aux intérêts subjectifs et objectifs qu'il vise à protéger, et, plus en général, à sa fonction dans une société démocratique fondée sur le respect de la dignité humaine (89), en pratique une telle opération s'avère presque impossible, à tout le moins sans tenir compte de critères qui sont habituellement

employés dans l'examen de la proportionnalité de l'ingérence dans le droit en cause, tels la gravité de cette ingérence, son étendue ou sa dimension temporelle et, dès lors, sans tenir compte des spécificités de chaque cas d'espèce.

93. S'agissant notamment du droit fondamental au respect de la vie privée, il convient de tenir compte non seulement de l'importance que revêt, pour la santé mentale et physique de tout individu, son bien-être, son autonomie, son épanouissement personnel, sa capacité de construire et de cultiver des relations sociales, le fait de disposer d'une sphère privée dans laquelle développer son intériorité personnelle, mais également du rôle que joue ce droit afin de préserver d'autres droits et libertés, tels que, notamment les libertés de pensée, de conscience, de religion, d'expression, d'information, dont la pleine jouissance suppose la reconnaissance d'une sphère d'intimité. Plus généralement, il convient de tenir compte de la fonction que remplit dans une société démocratique le respect du droit à la vie privée (90). La Cour semble apprécier l'existence d'une atteinte au contenu essentiel de ce droit en considérant tant l'*intensité* que l'*étendue* de l'ingérence, ce qui conduit à considérer qu'une telle atteinte est définie plutôt quantitativement que qualitativement. Ainsi, d'une part, dans l'arrêt Digital Rights, la Cour a en substance considéré que l'obligation de conservation des données imposée par la directive 2006/24/CE (91) n'atteignait pas un niveau de gravité telle qu'elle impacterait le contenu essentiel du droit au respect de la vie privé, puisqu'elle ne permettait pas de « prendre connaissance du contenu des communications électroniques en tant que tel » (92). D'autre part, dans l'avis 1/15, la Cour a en substance considéré qu'une limitation cantonnée à seulement certains aspects de la vie privée des personnes concernées ne pouvait pas donner lieu à une ingérence dans le contenu essentiel de ce droit fondamental (93).

94. Quant au droit fondamental à la protection des données à caractère personnel, la Cour semble considérer que le contenu essentiel de ce droit est préservé lorsque la mesure qui établit l'ingérence circonscrit les finalités du traitement et prévoit des règles assurant la sécurité des données visées, notamment contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle (94).

95. Dans la présente affaire, si la juridiction de renvoi n'a pas évoqué de manière explicite l'exigence de respect du contenu essentiel des droits énoncés aux articles 7 et 8 de la Charte, la question du respect de cette exigence est, à mon sens, sous-jacente à la quatrième et à la sixième question préjudicielle. C'est la raison pour laquelle je suggère à la Cour de l'aborder.

96. À cet égard, je rappelle que, au point 150 de l'avis 1/15, tout en reconnaissant que les données PNR « peuvent, le cas échéant, révéler des informations très précises sur la vie privée d'une personne » (95) et que ces informations peuvent dévoiler, directement ou indirectement, des données sensibles de la personne concernée (96), la Cour a néanmoins conclu, s'agissant du projet d'accord PNR Canada-UE, que, puisque la « nature de ces informations [était] limitée à certains aspects de cette vie privée, relatifs en particulier aux voyages aériens entre le Canada et l'Union », l'atteinte au droit fondamental au respect de la vie privée n'était pas de nature à affecter le contenu essentiel dudit droit.

97. Or, mise à part la circonstance que les données PNR visées par le projet d'accord PNR Canada-UE devaient être transférées vers un État tiers et que leur traitement ultérieur devait être effectué par les autorités de cet État tiers sur son territoire, les ingérences dans le droit fondamental au respect de la vie privée résultant dudit projet d'accord et celles prévues par la directive PNR sont, quant à leur nature, largement coïncidentes. Il en est ainsi, notamment, des données PNR visées, du caractère systématique et généralisé du transfert et du traitement de ces données, de la nature automatisée de celui-ci ainsi que de la conservation desdites données. En revanche, ce qui différencie les deux affaires est, pour ainsi dire, la « couverture géographique » de ces ingérences. En effet, ainsi que je l'ai indiqué au point 77 des présentes conclusions, les traitements des données

en cause dans la présente affaire ne sont pas limités aux liaisons aériennes avec un seul pays tiers, comme c'était le cas dans l'avis 1/15, mais portent sur quasiment tous les vols entrant et sortant de l'Union, et opérés au sein de celle-ci. Il s'ensuit que, par rapport au projet d'accord PNR Canada-UE, la directive PNR impose le traitement systématique d'un nombre sensiblement plus important de passagers aériens, se déplaçant par avion à l'intérieur et à l'extérieur de l'Union. En outre, étant donné l'augmentation du volume des données traitées ainsi que de la fréquence avec laquelle elles sont collectées, leur traitement est vraisemblablement susceptible de fournir des informations à la fois plus précises et plus amples sur la vie privée des personnes concernées (habitudes de voyage, relations personnelles, situations financières, etc.).

98. Il n'en reste pas moins que, comme c'était le cas dans l'avis 1/15, ces informations, considérées de manière isolée, ne portent que sur certains aspects de la vie privée, liés aux voyages aériens. Or, compte tenu de la nécessité de définir la notion de « contenu essentiel » des droits fondamentaux de manière restrictive, afin que celle-ci garde sa fonction de bastion contre les attaques à la substance même de ces droits, je suis de l'avis que la conclusion à laquelle la Cour est arrivée au point 150 de l'avis 1/15 peut être transposée à la présente affaire.

99. Dans l'avis 1/15, la Cour a aussi exclu une atteinte au contenu essentiel du droit à la protection des données à caractère personnel (97). Cette conclusion est, à mes yeux, également transposable aux circonstances de la présente affaire. En effet, tout comme c'était le cas du projet d'accord PNR Canada-UE, la directive PNR circonscrit, à son article 1, paragraphe 2, les finalités du traitement des données PNR. Par ailleurs, cette directive ainsi que les autres actes de l'Union auxquelles celle-ci renvoie, notamment le RGPD et la directive police, contiennent des dispositions spécifiques destinées à assurer, en particulier, la sécurité, la confidentialité et l'intégrité de ces données, ainsi qu'à les protéger contre les accès et les traitements illégaux. S'il ne saurait être considéré qu'une réglementation telle que celle prévue par la directive PNR touche au contenu essentiel des droits fondamentaux protégés par les articles 7 et 8 de la Charte, il n'en reste pas moins qu'elle doit être soumise à un contrôle strict et rigoureux de sa proportionnalité.

c) ***Sur le respect de l'exigence selon laquelle l'ingérence doit répondre à un objectif d'intérêt général***

100. La directive PNR vise, notamment, à assurer la sécurité intérieure de l'Union et à protéger la vie et la sécurité des personnes au moyen d'un transfert des données PNR aux autorités compétentes des États membres en vue de leur utilisation dans le cadre de la lutte contre le terrorisme et la criminalité grave (98).

101. Plus particulièrement, il ressort de l'article 1, paragraphe 2, de la directive PNR, lu en combinaison avec ses considérants 6 et 7, ainsi que de la proposition de la Commission ayant mené à l'adoption de cette directive (ci-après la « proposition de directive PNR ») (99), que, dans le cadre d'un tel objectif, les données PNR sont utilisées par les autorités répressives (100) de différentes manières. Premièrement, ces données sont utilisées afin d'identifier des personnes impliquées ou suspectées d'être impliquées dans des infractions terroristes et des formes graves de criminalité qui ont déjà été commises, de rassembler des preuves ainsi que, le cas échéant, de trouver les complices de criminels et de démanteler des réseaux criminels (utilisation en « mode réactif »). Deuxièmement, les données PNR peuvent être évaluées avant l'arrivée ou le départ des passagers afin de prévenir la commission d'un crime et d'identifier des personnes qui n'étaient pas auparavant soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité et qui, sur la base du résultat de cette évaluation, devraient être soumises à un examen plus approfondi par les autorités répressives (utilisation en «mode réel »). Enfin, les données PNR sont utilisées aux fins de définir des critères d'évaluation pouvant par la suite être appliqués dans l'appréciation du

risque que représentent les passagers avant leur arrivée et avant leur départ (utilisation en « mode proactif »). Une telle utilisation proactive des données PNR devrait permettre aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent de ce que permet le traitement d'autres catégories de données à caractère personnel (101).

102. Il ressort de la jurisprudence de la Cour que l'objectif de protection de la sécurité publique, couvrant notamment la prévention, la recherche, la détection et la poursuite tant d'infractions terroristes que d'infractions pénales relevant de la criminalité grave, constitue un objectif d'intérêt général de l'Union, au sens de l'article 52, paragraphe 1, de la Charte, susceptible de justifier des ingérences, même graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte (102).

103. La Cour a également reconnu que les objectifs de sauvegarde de la sécurité publique et de lutte contre la criminalité grave contribuent à la protection des droits et des libertés d'autrui (103). Ainsi, s'agissant de la pondération équilibrée entre ces objectifs et les droits fondamentaux consacrés aux articles 7 et 8 de la Charte (104), il convient de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte. À cet égard, si, dans l'arrêt La Quadrature du Net, la Cour a considéré que l'article 6 de la Charte « ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer certaines infractions pénales » (105), en revanche, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, elle a souligné que des obligations positives à la charge des pouvoirs publics peuvent résulter tant de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale, que des articles 3 et 4 de celle-ci, s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants (106).

104. Enfin, la Cour a considéré que l'importance de l'objectif de sauvegarde de la *sécurité nationale* dépasse celle des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique et qu'il est, dès lors, susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs (107). Les activités de terrorisme étant susceptibles de constituer des menaces à la sécurité nationale des États membres, le système mis en œuvre par la directive PNR, dans la mesure où il sert d'instrument de lutte contre de telles activités, participe à l'objectif de sauvegarde de la sécurité nationale des États membres.

d) ***Sur le respect du principe de proportionnalité***

105. Conformément à l'article 52, paragraphe 1, seconde phrase, de la Charte, dans le respect du principe de proportionnalité, des limitations à l'exercice d'un droit fondamental reconnu par celle-ci 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 des libertés d'autrui.

106. À cet égard, il convient de rappeler que 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 (108).

107. Conformément à la jurisprudence constante de la Cour, la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du *strict nécessaire*. En

outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, cela en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause (109). Plus particulièrement, la proportionnalité d'une limitation aux droits consacrés aux articles 7 et 8 de la Charte doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (110).

108. Il ressort de la jurisprudence de la Cour que, pour satisfaire à l'exigence de proportionnalité, la directive PNR, en tant que base légale comportant les ingérences dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte décrites aux points 70 à 83 des présentes conclusions, doit prévoir des règles claires et précises régissant la portée et l'application des mesures comportant de telles ingérences, et imposer des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données (111). La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme en l'espèce, les données à caractère personnel sont soumises à un traitement automatisé et lorsque est en jeu la protection de cette catégorie particulière des données à caractère personnel que sont les données sensibles (112).

109. S'agissant de l'étendue du contrôle juridictionnel du respect des exigences découlant du principe de proportionnalité, compte tenu du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et de l'ingérence dans ces droits que comporte la directive PNR, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte que ce contrôle doit être strict (113).

1) *Sur l'aptitude des traitements des données PNR visés par la directive PNR au regard de l'objectif poursuivi*

110. Au point 153 de l'avis 1/15, la Cour a affirmé, s'agissant du projet d'accord PNR Canada-UE, que le transfert des données PNR vers le Canada et les traitements ultérieurs de celles-ci peuvent être considérés comme étant aptes à garantir la réalisation de l'objectif tenant à la protection de la sécurité et de la sûreté publiques. Cette aptitude, reconnue depuis longtemps tant aux niveaux de l'Union que mondial (114) ne me semble pouvoir être remise en cause s'agissant de la collecte et du traitement ultérieure des données PNR pour ce qui concerne tant les vols extra-UE que les vols intra-UE (115).

111. Cela étant, l'efficacité du système de traitement des données PNR établi par la directive ne peut qu'être évalué en concret, en appréciant les résultats de son application (116). Dans cette optique, il est essentiel qu'une telle efficacité fasse l'objet d'une évaluation continue sur la base de données statistiques le plus précises et fiables possible (117). À cet égard, la Commission devrait, à des échéances régulières, procéder à un réexamen analogue à celui déjà prévu à l'article 19 de la directive PNR.

2) *Sur le caractère strictement nécessaire de l'ingérence*

112. Bien que la Cour constitutionnelle n'ait pas soulevé de manière explicite des doutes quant au fait que la directive PNR contient des règles claires, précises et limitées au strict nécessaire en ce qui concerne la délimitation des finalités du traitement des données PNR (118), l'analyse de la proportionnalité du système prévu par cette directive, sollicitée par la juridiction de renvoi, ne peut pas, à mon sens, omettre d'aborder cette question (119).

i) *Sur la délimitation des finalités du traitement des données PNR*

113. Une claire délimitation des finalités pour lesquelles l'accès à des données à caractère personnel par les autorités compétentes ainsi que leur utilisation ultérieure par celles-ci sont permis constitue une exigence essentielle de tout système de traitement de données notamment à des fins répressives. La satisfaction de cette exigence est, par ailleurs, nécessaire afin de permettre à la Cour d'apprécier la proportionnalité des mesures en cause, en appliquant le test de gravité de l'ingérence par rapport à l'importance de l'objectif poursuivi établi dans sa jurisprudence (120).

114. La Cour a souligné l'importance d'une claire délimitation des finalités des mesures comportant des limitations aux droits fondamentaux au respect de la vie privée et à la protection des données personnelles, notamment dans l'arrêt Digital Rights, dans lequel elle a déclaré comme étant invalide la directive 2006/24. Au point 60 de cet arrêt, la Cour a observé que cette directive ne prévoyait « aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence » et qu'elle se bornait, au contraire, « à renvoyer, à son article 1er, paragraphe 1, de manière générale aux infractions graves telles qu[e] définies par chaque État membre dans son droit interne ».

115. L'article 1, paragraphe 2, de la directive PNR énonce un critère général de limitation des finalités selon lequel « [l]es 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 ». Toutefois, contrairement à la directive 2006/24, la directive PNR ne se limite pas à une telle énonciation, mais définit elle-même, à son article 3, points 8 et 9, tant la notion d'« infractions terroristes » que celle de « formes graves de criminalité », la première par renvoi aux articles 1er à 4 de la décision-cadre 2002/475/JAI du Conseil, du 13 juin 2002, relative à la lutte contre le terrorisme (JO 2002, L 164, p. 3) (remplacée par la directive (UE) 2017/541) (121), et la seconde, d'une part, en énumérant, à l'annexe II, les catégories d'infractions pénales correspondant à cette notion et, d'autre part, en établissant un seuil de gravité en termes de durée maximale de la peine de détention ou de la mesure de sûreté dont ces infractions sont passibles.

116. Si le renvoi aux dispositions pertinentes de la directive 2017/541 permet de caractériser de manière suffisamment claire et précise les actes susceptibles d'être qualifiés d'infractions terroristes au titre de l'article 3, point 8, de la directive PNR et d'en apprécier la gravité aux fins de la mise en balance de l'importance de l'objectif de protection de la sécurité publique poursuivi par cette directive et de la gravité de l'ingérence que celle-ci comporte dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, la même conclusion ne s'impose pas avec une pareille évidence s'agissant de toutes les infractions énumérées à l'annexe II.

117. Au point 177 de l'avis 1/15, la Cour a considéré que le projet d'accord PNR Canada-UE définissait avec clarté et précision le degré de gravité des infractions visées par la notion de « criminalité transnationale grave », en imposant que ces infractions soient « punissables d'une peine privative de liberté d'au moins quatre ans ou d'une peine plus lourde », en renvoyant « aux infractions définies par le droit canadien » et en énonçant « les différentes hypothèses dans lesquelles un crime est considéré comme étant de nature transnationale ».

118. Par rapport à la réglementation examinée par la Cour dans cet avis, la directive PNR, premièrement, ne tient pas compte, dans la définition des infractions visées, de leur caractère

transnational, deuxièmement, prévoit un catalogue exhaustif d'infractions qui, par leur nature, sont considérées comme relevant de la criminalité grave, à condition d'atteindre le minimum de peine maximale prévu à l'article 3, point 9, de cette directive, troisièmement, baisse, en principe, le seuil de gravité, en adoptant un critère fondé sur le niveau de la peine maximale et en fixant ce seuil à trois ans.

119. En ce qui concerne, premièrement, l'absence de critère de limitation fondé sur le caractère transnational, il est certes vrai que circonscrire le champ d'application matériel de la directive PNR à la seule criminalité « transfrontalière » grave aurait permis de cibler des infractions susceptibles, par leur nature, d'entretenir, à tout le moins potentiellement, un lien objectif avec les voyages aériens et, par conséquent, avec les catégories de données collectées et traitées en application de la directive PNR (122). Cependant, je partage, sur le principe, le point de vue exprimé par la Commission, selon lequel, diversement que dans le contexte d'un accord international, la pertinence et la nécessité d'un tel critère est moins évident s'agissant d'un dispositif de lutte contre la criminalité dont l'objectif est celui de protéger la sécurité intérieure de l'Union. Par ailleurs, comme l'affirme toujours la Commission, l'absence d'éléments transfrontaliers n'est pas en soi un indice permettant d'exclure la gravité d'une infraction.

120. S'agissant, deuxièmement, du critère fixant le seuil de gravité des infractions visées – qui, afin de permettre une appréciation ex ante de cette gravité, doit être interprété en ce sens qu'il se réfère à la durée maximale de la peine de détention ou de la mesure de sûreté prévue par la loi et non pas à celle susceptible d'être concrètement encourue dans un cas particulier – ce critère, bien que se fondant sur le minimum de peine maximale et non pas sur le minimum de peine minimale n'est pas en soi inapte à identifier un niveau suffisant de gravité susceptible de justifier l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comportent les traitements de données prévus par la directive PNR. Il convient cependant, à mes yeux, de l'interpréter comme un critère identifiant un niveau de gravité « minimal ». Ainsi, un tel critère, s'il interdit aux États membres de considérer comme « formes graves de criminalité » des infractions visées à l'annexe II pour lesquelles leur droit pénal national prévoit une peine de détention ou de mesure de sûreté d'une durée maximale inférieure à trois ans, il ne les oblige en revanche pas à reconnaître automatiquement une telle qualification à toutes les infractions susceptibles d'être incluses dans ladite annexe II qui sont passibles d'une peine atteignant le seuil prévu à l'article 3, point 9, de la directive PNR, lorsque, compte tenu des spécificités de leur système pénal, une telle reconnaissance aboutirait à une utilisation du régime prévu par la directive PNR à des fins de prévention, de détection, d'enquête et de poursuite de formes de criminalité commune, contraire aux finalités poursuivies par cette directive.

121. En ce qui concerne, troisièmement, le catalogue de l'annexe II, il convient, tout d'abord, de relever que la circonstance que la directive PNR énumère limitativement les infractions relevant de la définition des « formes graves de criminalité » constitue une garantie formelle et substantielle fondamentale afin d'assurer la légalité du système établi par la directive PNR et la sécurité juridique des passagers. Force est, cependant, de constater que ledit catalogue inclut tant des infractions qui, par leur nature, revêtent un niveau de gravité incontestablement élevé – telles que, par exemple, la traite des êtres humains, l'exploitation sexuelle des enfants et la pédopornographie, le trafic d'armes, ou de matières nucléaires ou radioactive, le détournement d'avion/de navire, les infractions graves relevant de la Cour pénale internationale, le meurtre, le viol, l'enlèvement, la séquestration et la prise d'otage (123) – que des infractions pour lesquelles un tel niveau de gravité s'avère moins évident, comme la fraude, la contrefaçon et le piratage des produits, la falsification de documents administratifs et le trafic de faux, ainsi que le trafic de véhicules volés (124). Par ailleurs, parmi les infractions incluses à l'annexe II, certaines sont plus susceptibles que d'autres de revêtir, par leur nature même, un caractère transnational, comme la traite des êtres humains, le trafic

de stupéfiants ou d'armes, l'exploitation sexuelle des enfants, l'aide à l'entrée et au séjour irréguliers, le détournement d'avion, et d'avoir aussi un lien avec le transport aérien de passagers.

122. Quant au caractère suffisamment clair et précis des rubriques figurant à l'annexe II, là aussi, le niveau est très variable. Ainsi, bien que la liste contenue à cette annexe doive être considérée comme étant exhaustive, plusieurs de ses rubriques ont un caractère « ouvert » (125) et d'autres renvoient à des notions génériques, susceptibles d'inclure un nombre très large d'infractions de gravité variable, bien que toujours dans la limite du seuil maximal prévu à l'article 3, point 9, de la directive PNR (126).

123. À cet égard, je relève, d'une part, que les directives d'harmonisation adoptées dans les domaines visés à l'article 83, paragraphe 1, TFUE, mentionnées à la note en bas de page 123 des présentes conclusions, fournissent des éléments pertinents permettant d'identifier à tout le moins certaines des infractions pénales graves susceptibles d'entrer dans les rubriques correspondantes de l'annexe II. Ainsi, notamment, la directive 2013/40 définit, à ses articles 3 à 8, différentes infractions pénales relevant de la notion de « cybercriminalité » visée au point 9 de cette annexe II, prenant soin, dans chaque cas, d'exclure les actes constituant des « cas mineurs » (127). De même, la directive 2019/713 définit certaines typologies d'infractions frauduleuses, et la directive 2017/1371 définit les éléments constitutifs d'une « fraude contre les intérêts financiers de l'Union ». Dans ce contexte, il convient également de mentionner la directive 2008/99/CE, adoptée sur la base de l'article 175, paragraphe 1, CE, relative à la protection de l'environnement par le droit pénal (128), qui définit, à son article 3, une série d'infractions environnementales graves, susceptibles d'être incluses à la rubrique 10 de l'annexe II, y compris les actes qualifiables de « trafic d'espèces animales menacées et [de] trafic d'espèces et d'essences végétales menacées », en excluant tous agissements ayant un impact négligeable sur le bien protégé. Je rappellerai, enfin, la directive 2002/90/CE (129), qui définit l'aide à l'entrée, au transit et au séjour irréguliers ainsi que la décision-cadre 2002/946/JAI (130), visant à renforcer le cadre pénal pour la répression de ces infractions, la décision-cadre 2003/568/JAI (131), qui définit les infraction pénales qualifiées de « corruption active et passive dans le secteur privé », et la décision-cadre 2008/841/JAI (132), qui définit les infractions relatives à la participation à une organisation criminelle.

124. D'autre part, je relève, comme l'a, à juste titre, fait observer la Commission, que, en l'absence d'une harmonisation complète du droit pénal matériel, il ne saurait être reproché au législateur de l'Union de ne pas avoir précisé davantage les infractions visées à l'annexe II. Ainsi, à la différence de ce qui sera observé plus loin dans les présentes conclusions s'agissant de la liste des données PNR contenue à l'annexe I, la transposition en droit interne du catalogue d'infractions de l'annexe II requiert nécessairement des États membres qu'ils définissent, en fonction des spécificités de leurs systèmes pénaux nationaux, les infractions susceptibles d'être visées. Cette opération doit cependant être effectuée dans le plein respect du critère selon lequel toute ingérence dans les droits fondamentaux énoncés aux articles 7 et 8 de la Charte doit être limitée au strict nécessaire. Ainsi, par exemple, il n'est, à mon sens, pas exclu pour les États membres de prévoir que l'utilisation des données PNR soit limitée, pour certaines infractions, telles que, par exemple, celles visées aux points 7, 16, 17, 18, 25 de l'annexe II aux cas où ces infractions revêtent un caractère transfrontalier, ou sont commises dans le cadre d'une organisation criminelle, ou comportent certaines circonstances aggravantes. Il incombera aux juridictions des États membres, sous le contrôle de la Cour, d'interpréter les dispositions nationales transposant ledit catalogue en droit interne de manière conforme tant à la directive PNR qu'à la Charte, de sorte que le traitement des données PNR reste, pour chaque rubrique, limité aux infractions qui atteignent le niveau de gravité élevé requis par cette directive ainsi qu'aux infractions pour lesquelles un tel traitement s'avère pertinent (133).

125. Sous réserve des précisions apportées aux points 120 et 124 des présentes conclusions, j'estime que l'article 3, point 9, de la directive PNR ainsi que le catalogue d'infractions contenu à son annexe II répondent aux exigences de clarté et de précision, et ne dépassent pas les limites du strict nécessaire.

126. Force est cependant de reconnaître que la solution illustrée au point 124 des présentes conclusions n'est pas complètement satisfaisante. En effet, d'une part, elle laisse une marge importante de discrétion aux États membres, de sorte que le champ d'application matérielle du traitement des données PNR est susceptible de varier sensiblement d'un État membre à l'autre, compromettant ainsi l'objectif d'harmonisation poursuivi par le législateur de l'Union (134). D'autre part, elle implique que le contrôle de proportionnalité sur un élément essentiel du système, tel que la limitation des finalités de ce traitement, soit exercé ex post sur les mesures nationales de transposition, plutôt qu'ex ante sur la directive PNR elle-même. Il serait dès lors souhaitable que, dans l'hypothèse où la Cour déciderait, comme je lui suggère de le faire, de considérer l'article 3, point 9, de la directive PNR ainsi que le catalogue d'infractions contenu à son annexe II comme étant conforme aux articles 7, 8, et à l'article 51, paragraphe 2, de la Charte, elle attire l'attention du législateur de l'Union sur le fait qu'une telle appréciation n'est que provisoire et qu'elle implique de la part de ce législateur qu'il vérifie, à la lumière de la transposition qui a été faite par les États membres de cette disposition et de ce catalogue ainsi que sur la base des données statistiques visées à l'article 20 de la directive PNR, la nécessité: i) de préciser davantage, en en restreignant la portée, les catégories d'infractions visées par ledit catalogue, ii) d'éliminer de celui-ci les infractions pour lesquelles le traitement des données PNR s'avère soit disproportionné, soit non pertinent ou inefficace, et iii) de relever le seuil de gravité des infractions visées à l'article 3, point 9, de la directive PNR (135). À cet égard, je relève que, si l'article 19, paragraphe 2, sous b), de la directive PNR impose à la Commission de procéder au réexamen de tous les éléments de cette directive, en accordant une attention particulière « à la nécessité et à la proportionnalité de la collecte et du traitement des données PNR au regard de chacune des finalités énoncées » dans celle-ci, ni le rapport de la Commission de 2020 ni le document de travail de 2020 l'accompagnant ne contiennent, à mon sens, un examen satisfaisant sur ce point.

ii) *Sur les catégories de données PNR visées par la directive PNR (deuxième et troisième questions préjudicielles)*

127. La directive PNR prévoit le transfert aux UIP de 19 catégories de données PNR collectées par les transporteurs aériens aux fins de la réservation de vols. Ces catégories, énumérées à l'annexe I, correspondent à celles qui apparaissent dans les systèmes de réservations des compagnies aériennes et à celles énumérées à l'annexe I des lignes directrices sur les données des dossiers passagers adoptées par l'Organisation de l'aviation civile internationale (OACI) en 2010 (136) (ci-après les « lignes directrices de l'OACI).

128. Par sa deuxième question préjudicielle, la juridiction de renvoi s'interroge sur la validité de l'annexe I au regard des articles 7, 8, et de l'article 52, paragraphe 1, de la Charte, compte tenu, d'une part, de l'ampleur des données à caractère personnel énumérés à cette annexe – et notamment des données API visées au point 18 de celle-ci, en ce qu'elles dépassent les données énumérées à l'article 3, paragraphe 2, de la directive API – et, d'autre part, de la possibilité que ces données, prises ensemble, révèlent des données sensibles et violent ainsi les limites du « strict nécessaire ». Par sa troisième question préjudicielle – qui porte, ainsi que j'ai déjà eu l'occasion de le souligner, sur le respect de la première des trois conditions visées à l'article 52, paragraphe 1, de la Charte, selon laquelle toute ingérence dans un droit fondamental doit être « prévue par la loi » – la Cour constitutionnelle interroge en revanche la Cour au sujet de la validité des points 12 et 18 de l'annexe I, compte tenu notamment de leur caractère « ouvert ».

129. Puisque l'examen à conduire dans le cadre de la deuxième question préjudicielle présuppose celui sur le caractère suffisamment clair et précis des catégories de données à caractère personnel visées à l'annexe I, j'aborderai en premier la troisième question préjudicielle.

– *Sur le caractère suffisamment clair et précis des points 12 et 18 de l'annexe I (troisième question préjudicielle)*

130. Il convient de relever, à titre liminaire, que l'ampleur et la gravité de l'ingérence dans les droits fondamentaux énoncés aux articles 7 et 8 de la Charte qui comporte une mesure introduisant des limitations à l'exercice de ces droits dépend, avant tout, de l'étendue et de la nature des données à caractère personnel qui constituent l'objet du traitement. L'identification de ces données constitue donc une opération essentielle, à laquelle toute base légale introduisant une telle mesure doit obligatoirement procéder de la manière la plus claire et précise possible.

131. Cette exigence a été reconnue, en ce qui concerne le traitement des données PNR, par l'avis 1/15. Se prononçant à l'égard des rubriques figurant à l'annexe du projet d'accord PNR Canada-UE contenant l'énumération des données PNR visées par l'accord envisagé, la Cour a notamment considéré, dans cet avis, que le recours à des catégories générales d'informations qui ne déterminent pas suffisamment l'étendue des données à transférer, ainsi que le recours à des listes exemplatives de données qui ne fixent aucune limitation quant à la nature et à l'ampleur des informations susceptibles de figurer dans la rubrique concernée ne satisfaisaient pas aux conditions de clarté et de précision.

132. C'est à la lumière de ces principes qu'il convient d'examiner la troisième question préjudicielle.

133. Concernant le point 12 de l'annexe I, celui-ci est rédigé comme suit :

« 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). »

134. En ce qu'il vise les « remarques générales », ce point constitue, à l'instar de la rubrique 17 de l'annexe du projet d'accord PNR Canada-UE, une rubrique dite « texte libre », ayant vocation à inclure toute information collectée par les transporteurs aériens dans le cadre de leur activité de prestation de service, en plus de celles expressément énumérées aux autres points de l'annexe I. Or, force est de constater, ainsi que l'a fait la Cour au point 160 de l'avis 1/15, qu'une rubrique de ce type « ne fournit aucune indication sur la nature et l'étendue des renseignements qui doivent être transmis et paraît même susceptible d'englober des informations dépourvues de tout rapport avec la finalité du transfert des données PNR ». En outre, dès lors que la précision entre parenthèses qui figure dans le libellé du point 12 de l'annexe 1, visant les informations sur les mineurs non accompagnés, n'est fournie qu'à titre d'exemple, comme en témoigne l'usage du terme « notamment », ce point ne fixe aucune limitation quant à la nature et à l'étendue des informations susceptibles d'y figurer (137).

135. Dans ces conditions, le point 12 de l'annexe I ne saurait être considéré comme étant délimité avec suffisamment de clarté et de précision.

136. Si la Commission et le Parlement semblent partager cette conclusion, les États membres ayant présenté des observations sur la troisième question préjudicielle ainsi que le Conseil s'y opposent et cela sur la base d'argumentations qui se recoupent largement.

137. En premier lieu, une première série d'arguments vise, de manière générale, à mettre en cause la possibilité de transposer à la présente affaire les conclusions auxquelles la Cour est arrivée dans l'avis 1/15.

138. À cet égard, tout en étant conscient de la différence de contexte qui caractérise les deux affaires, je me bornerai ici à observer que la conclusion à laquelle la Cour est arrivée au point 160 de l'avis 1/15 s'agissant de la rubrique 17 de l'annexe au projet d'accord PNR Canada-UE était fondée sur une interprétation exclusivement sémantique et structurelle de cette rubrique. Or, une telle interprétation est parfaitement transposable au point 12 de l'annexe I, dont le libellé est, pour la partie non exemplative, identique à celui de ladite rubrique et présente une structure analogue. Par ailleurs, ainsi qu'on le verra plus en détail ci-après, les deux règles en cause s'insèrent dans le même contexte réglementaire multilatéral, constitué notamment des lignes directrices de l'OACI, auxquelles la Cour s'est d'ailleurs référée expressément au point 156 de l'avis 1/15. Dans ces conditions, non seulement rien ne s'oppose à ce que l'on suive, pour le point 12 de l'annexe I, la même interprétation que celle retenue par la Cour au point 160 de l'avis 1/15 pour la rubrique 17 de l'annexe au projet d'accord PNR Canada-UE, mais surtout rien ne justifie que l'on se départe de celle-ci.

139. En deuxième lieu, bon nombre d'États membres soulignent que les différents points de l'annexe I, y inclus le point 12, correspondent aux rubriques de l'annexe I des lignes directrices de l'OACI, que les transporteurs aériens connaissent bien et auxquelles ils sont parfaitement capables d'attribuer un contenu précis. Ce point 12 correspondrait notamment aux deux dernières rubriques de ladite annexe, intitulées respectivement « remarques générales » et « Texte libre/champs de code dans OSI [Other Supplementary Information], SSR [Special Service Request], SSI [Special Service Information], Remarques/historiques » et visant des « renseignements supplémentaires » ou « relatifs à des services demandés » (138).

140. À cet égard, j'observe tout d'abord que la correspondance entre les rubriques de l'annexe I du projet d'accord PNR Canada-UE, d'une part, et les rubriques de l'annexe I des lignes directrices de l'OACI, d'autre part, n'a pas empêché la Cour de déclarer, dans l'avis 1/15, que certaines des rubriques figurant à l'annexe I audit projet d'accord ne satisfaisaient pas aux exigences de clarté et de précision auxquelles doit répondre une mesure limitant l'exercice de droits fondamentaux. Ensuite, je relève qu'un renvoi, par ailleurs non explicite (139), aux lignes directrices de l'OACI, ne permet pas, contrairement à ce que certains États membres semblent considérer, de préciser davantage la nature et l'étendue des informations susceptibles d'être visées au point 12 de l'annexe I. Au contraire, la lecture de ces lignes directrices renforce la conclusion selon laquelle une rubrique « texte libre », telle que ledit point 12, inclut un nombre indéfini d'informations de nature diverse en plus de celles qui figurent d'office dans les PNR (140).

141. En troisième lieu, certains gouvernements soutiennent qu'il incombe aux États membres, au moyen de mesures législatives internes et dans le respect des limites imposées par les articles 7, 8, et l'article 52, paragraphe 1, de la Charte, de préciser les informations susceptibles de figurer au point 12 de l'annexe I. En effet, il serait dans la nature même d'une directive de laisser aux États membres une marge discrétionnaire quant aux moyens nécessaires pour mettre en œuvre les dispositions que celle-ci édicte.

142. À cet égard, ainsi que je l'ai déjà exposé au point 86 des présentes conclusions, je suis de l'avis que, lorsque des mesures comportant des ingérences dans les droits fondamentaux établis par la Charte trouvent leur source dans un acte législatif de l'Union, il incombe au législateur de l'Union de fixer, dans le respect des critères de clarté et de précision susmentionnés, ainsi que du principe de proportionnalité, la portée exacte de ces ingérences. Il s'ensuit que, lorsque l'instrument choisi par ce législateur est une directive, il ne saurait, à mon sens, être délégué aux États membres, lors de la transposition de celle-ci dans leurs droits nationaux, la détermination d'éléments essentiels définissant la portée de l'ingérence, tels que, s'agissant de limitations aux droits fondamentaux énoncés aux articles 7 et 8 de la Charte, la nature et l'étendue des données à caractère personnel soumis à traitement.

143. En quatrième lieu, certains États membres font observer que le point 12 de l'annexe I doit s'entendre comme visant uniquement des informations ayant un rapport avec la prestation de transport. Ainsi interprété, ce point serait compatible avec les articles 7, 8, et l'article 52, paragraphe 1, de la Charte.

144. Cet argument ne me convainc pas non plus. Tout d'abord, en effet, les informations pouvant figurer dans une rubrique « remarques générales » et sous les codes OSI, SSI et SSR sont de nature très hétérogène (soins médicaux, repas spéciaux ou préférences alimentaires, toute demande d'assistance, informations portant sur les mineurs voyageant seuls, etc.) (141) et toutes ont un lien avec la prestation de transport en ce qu'elles visent, notamment, à permettre au transporteur aérien d'adapter cette prestation aux exigences de chaque passager. Un critère interprétatif fondé sur la pertinence de l'information par rapport à la prestation de transport ne permettrait donc pas de préciser davantage la portée de ce point 12. Ensuite, je relève que, tout en ayant eu recours, au point 159 de l'avis 1/15, à ce critère afin d'interpréter de manière conforme aux exigences de clarté et de précision une rubrique différente de l'annexe au projet d'accord PNR Canada-UE, la Cour a néanmoins exclu de pouvoir procéder de la sorte s'agissant de la rubrique 17 de cette annexe, correspondant au point 12 de l'annexe I.

145. En cinquième lieu, quelques États membres ont mis l'accent sur le fait que les renseignements ayant vocation à être visés au point 12 de l'annexe I sont volontairement fournis aux transporteurs aériens par les passagers eux-mêmes, qui sont dûment informés du transfert ultérieur de ces données aux autorités publiques. L'idée sous-tendant un tel argument est, me semble-t-il, qu'il y ait une sorte de consentement implicite de la part du passager concerné à ce que les données qu'il fournit aux compagnies aériennes soient par la suite transférées aux autorités publiques.

146. À cet égard, la Cour a déjà eu l'occasion de préciser qu'il ne saurait être question de « consentement » lorsque la personne concernée ne peut pas s'opposer librement au traitement de ses données personnelles (142). Or, pour une grande partie des renseignements susceptibles de figurer au point 12 de l'annexe I, le passager concerné ne dispose pas d'un véritable choix, mais il est tenu de les fournir pour pouvoir profiter de la prestation de transport. Il en est ainsi, notamment, des personnes handicapées ou à mobilité réduite, ou des personnes nécessitant des soins médicaux ou encore des mineurs non accompagnés. Je rappelle par ailleurs que, aux points 142 et 143 de l'avis 1/15, la Cour a clairement affirmé que les traitements des données PNR par des autorités publiques, poursuivant une finalité différente de celle pour laquelle ces données sont collectées par les transporteurs aériens, ne peuvent être considérés comme étant fondés sur une quelconque forme de consentement donné par les passagers en vue de cette collecte.

147. Enfin, la plupart des États membres font valoir que les traitements de données prévus par la directive PNR sont entourés de nombreuses garanties, parmi lesquelles, s'agissant du transfert de données aux UIP, l'obligation qui incombe à celles-ci d'effacer les données ne figurant pas à

l'annexe I ainsi que les données susceptibles de révéler 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.

148. À cet égard, je dirai d'emblée que, à mes yeux, l'appréciation du caractère suffisamment clair et précis des règles définissant l'étendue et la nature des données qui peuvent faire l'objet d'un transfert aux autorités publiques, en ce qu'elle vise à s'assurer qu'une mesure comportant des ingérences dans les droits fondamentaux énoncés aux articles 7 et 8 de la Charte respecte les principes de légalité et de sécurité juridique, doit être conduite sans tenir compte des garanties qui entourent les traitements auxquels ces données seront soumises par lesdites autorités, ces garanties n'entrant en ligne de compte que lors de l'examen de la proportionnalité de la mesure en cause. C'est d'ailleurs de cette manière que la Cour a procédé, aux points 155 à 163 de l'avis 1/15, à son appréciation des rubriques du projet d'accord PNR Canada-UE. J'ajoute, de manière plus générale, qu'une attention particulière devrait être prêtée à la nécessité de garder une nette distinction entre les différentes phases que comporte l'examen d'une mesure comportant des ingérences dans les droits fondamentaux, un amalgame entre ces différentes phases allant, à mon sens, toujours au détriment d'une protection effective de ceux-ci.

149. Cela étant dit, je me borne ici à relever, d'une part, que l'obligation qui incombe aux UIP, conformément à l'article 6, paragraphe 1, de la directive PNR, d'effacer les données autres que celles énumérées à l'annexe I n'a d'utilité que si cette annexe contient un catalogue clair et fermé de données à transférer. Il en va de même pour ce qui est de l'obligation qu'ont les UIP, conformément à l'article 13, paragraphe 4, de la directive PNR, d'effacer les données dites « sensibles » (143). En effet, une définition trop vague, imprécise ou ouverte des informations qui doivent être transmises accroît tant la probabilité que de telles données fassent indirectement l'objet de transfert que le risque qu'elles ne soient pas immédiatement identifiées et effacés. En d'autres termes, les garanties susmentionnées ne sauraient remplir utilement leur fonction que si les règles qui définissent la nature et l'étendue des données PNR que les transporteurs aériens sont appelés à transférer aux UIP sont suffisamment claires et précises et si la liste de ces données présente un caractère fermé et exhaustif.

150. Sur la base de l'ensemble des considérations qui précèdent, et ainsi que je l'ai anticipé au point 135 des présentes conclusions, je suis de l'avis que le point 12 de l'annexe I, dans la partie où il inclut « les remarques générales » parmi les données que les transporteurs aériens sont tenus de transférer aux UIP conformément à la directive PNR ne répond pas aux exigences de clarté et de précision requises à l'article 52, paragraphe 1, de la Charte ainsi qu'interprété par la Cour (144) et qu'il devrait, dès lors, être, dans cette mesure, déclaré comme étant invalide.

151. Dans leurs observations écrites, la Commission et le Parlement ont suggéré à la Cour d'avoir plutôt recours à une « interprétation conforme » du point 12 de l'annexe I, en le lisant en ce sens qu'il ne vise que les renseignements sur les mineurs qui y sont explicitement mentionnés entre parenthèses. J'avoue que j'éprouve quelques difficultés à considérer qu'une telle lecture respecte les limites d'une simple interprétation conforme. Il est, certes, vrai que, selon un principe général d'interprétation, un acte de l'Union doit être interprété, dans la mesure du possible, d'une manière qui ne remet pas en cause sa validité et en conformité avec l'ensemble du droit primaire et, notamment, avec les dispositions de la Charte (145). Il est tout aussi vrai que, s'agissant de la directive PNR, la possibilité d'une telle interprétation apparaît favorisée par l'accent que mettent, notamment, bon nombre de considérants de cette directive sur le plein respect des droits fondamentaux, du droit au respect de la vie privée ainsi que du principe de proportionnalité (146). Cependant, il est également de jurisprudence constante qu'une interprétation conforme n'est admise que lorsque le texte de droit dérivé de l'Union est susceptible de plus d'une interprétation et qu'il

est dès lors possible de donner la préférence à celle qui rend la disposition conforme au droit primaire plutôt qu'à celle conduisant à constater son incompatibilité avec celui-ci (147).

152. Or, le point 12 de l'annexe I n'est à mon sens, pas susceptible d'être interprété tel que le suggèrent la Commission et le Parlement, sauf à en donner une lecture « contra legem ». En effet, ce point vise, ainsi que je l'ai exposé ci-dessus, une catégorie large de données de natures diverses, non identifiables a priori, par rapport à laquelle les données sur les mineurs ne constituent qu'une sous-catégorie. Lire ce point comme ne visant que cette seule sous-catégorie reviendrait non seulement à ignorer une partie de son libellé, mais aussi subvertirait l'ordre logique de l'énoncé que ce point contient. Une telle opération, qui consiste en substance à éliminer la partie du libellé du point 12 de l'annexe I qui serait considérée comme étant non conforme aux exigences de clarté et de précision, ne peut, à mon sens, s'effectuer qu'en prononçant une annulation partielle.

153. S'agissant de la partie restante du point 12 de l'annexe I, qui énumère une série de données concernant les mineurs non accompagnés, je suis de l'avis qu'elle répond aux exigences de clarté et de précision à condition qu'elle soit interprétée en ce sens qu'elle ne couvre que les renseignements concernant les mineurs non accompagnés qui ont un rapport direct avec le vol et qui sont expressément visées par ce point.

154. Concernant le point 18 de l'annexe I, celui-ci est rédigé comme suit :

« 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). »

155. Ce point présente une structure analogue à celle du point 12 de l'annexe I. Il mentionne aussi une catégorie générale de données, à savoir les informations préalables sur les passagers (Advance Passenger Information – API), suivie, entre parenthèses, d'une liste de données considérées comme étant incluses dans cette catégorie générale, laquelle est fournie à titre purement exemplatif, ainsi que l'atteste l'emploi de l'expression « y compris ».

156. Toutefois, contrairement au point 12 de l'annexe I, le point 18 de cette annexe renvoie à une catégorie de données mieux identifiables pour ce qui est tant de leur nature que de leur étendue. En effet, il ressort du considérant 4 de la directive PNR que, lorsque celle-ci se réfère à cette catégorie de données, elle vise les informations qui, conformément à la directive API, à laquelle ce considérant renvoie expressément, font l'objet de transmission par les transporteurs aériens aux autorités nationales compétentes, en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration illégale. Ces données sont énumérées à l'article 3, paragraphe 2, de cette dernière directive.

157. En outre, il ressort du considérant 9 (148) de la directive PNR ainsi que de l'article 3, paragraphe 2, de la directive API et de la liste exemplative contenue au point 18 de l'annexe I que les données API visées par ledit point sont, d'une part, des données biographiques permettant de vérifier l'identité du passager aérien et, d'autre part, des données concernant le vol réservé. S'agissant, plus précisément, de la première catégorie, celle des données biographiques, les informations énumérées à l'article 3, paragraphe 2, de la directive API et au point 18 de l'annexe I recouvrent des données, générées à l'enregistrement, susceptibles d'être extraites de la partie d'un passeport (ou autre document de voyage) lisible à la machine (149).

158. Ainsi, le point 18 de l'annexe I, interprété à la lumière des considérants 4 et 9 de la directive PNR, identifie en principe avec suffisamment de clarté et de précision à tout le moins la nature des données qu'il vise.

159. Quant à leur étendue, force est de constater, d'une part, que l'article 3, paragraphe 2, de la directive API est lui aussi rédigé de manière « ouverte », la liste de données qu'il énumère étant précédée de l'expression « parmi ces données figurent » (150), et, d'autre part, que, dans la catégorie des données API, telle qu'elle est définie dans les instruments multilatéraux d'harmonisation en la matière, figurent également des données autres que celles visées tant par la directive API que par le point 18 de l'annexe I (151).

160. Dans ces circonstances, pour que le point 18 de l'annexe I réponde aux exigences de clarté et précision requises aux bases légales comportant des ingérences aux articles 7 et 8 de la Charte, il convient de l'interpréter en ce sens qu'il ne couvre que les données API qui sont expressément énumérées à ce point ainsi qu'à l'article 3, paragraphe 2, de la directive API et qui ont été recueillies par les transporteurs aériens dans le cours normal de leurs activités (152).

161. Il convient à ce stade de passer brièvement en revue les autres points de l'annexe I qui, compte tenu de leur libellé, présentent également un caractère « ouvert » ou qui ne sont pas suffisamment précis, et cela bien que la juridiction de renvoi n'ait pas interrogé expressément la Cour à leur égard (153).

162. S'agissant, tout d'abord, du point 5 de l'annexe I, mentionnant « adresse et coordonnées (numéro de téléphone, adresse électronique) », s'il doit être considéré comme ne visant que les coordonnées expressément mentionnées entre parenthèses et présente donc un caractère exhaustif, il ne précise cependant pas, comme c'était le cas de la rubrique correspondante du projet d'accord PNR Canada-UE (154), si ces coordonnées se réfèrent au seul voyageur ou aux tiers ayant effectué la réservation du vol pour le passager aérien, aux tiers par l'intermédiaire desquels un passager aérien peut être joint, ou encore aux tiers devant être informés en cas d'urgence (155). Compte tenu du fait qu'interpréter le point 5 de l'annexe I comme visant également les catégories de tiers susmentionnés étendrait l'ingérence que comporte la directive PNR à d'autres sujets que les passagers aériens au sens de l'article 3, point 4, de la directive PNR, je suggère à la Cour, en l'absence de données précises permettant de considérer que l'acquisition systématique et généralisée des coordonnées de ces tiers constitue un élément strictement nécessaire à l'efficacité du système de traitement des données PNR institué par cette directive, d'interpréter ledit point comme ne visant que les coordonnées qui y sont expressément mentionnées et qui concernent le passager aérien au nom duquel la réservation est faite. Certes, la directive PNR n'exclut pas que puissent faire l'objet de transfert aux UIP également des données à caractère personnel d'autres sujets que le passagers ariens (156). Cependant, il est essentiel que les hypothèses où cela est possible soient indiquées de manière claire et explicite, comme c'est le cas pour les agents de voyage, mentionnés à l'annexe I, point 9, ou les tuteurs des mineurs voyageant seuls, visés au point 12 de cette annexe. C'est en effet seulement si cette condition est remplie qu'il peut être considéré que la décision d'inclure ces données dans celles devant être transférées aux UIP a fait l'objet d'une pondération entre les différents intérêts en jeu, au sens du considérant 15 de la directive PNR, et que les tiers concernés peuvent être adéquatement informés du traitement de leurs données à caractère personnel.

163. En ce qui concerne, ensuite, le point 6 de l'annexe I, visant « [t]outes les informations relatives aux modes de paiement, y compris l'adresse de facturation », à l'instar de ce que la Cour a jugé au point 159 de l'avis 1/15, s'agissant de la rubrique correspondante de l'annexe au projet d'accord PNR Canada-UE, pour répondre aux exigences de clarté et de précision, ce point doit être interprété

comme « ne visant que les informations relatives aux modalités de paiement et à la facturation du billet d'avion, à l'exclusion de toute autre information sans rapport direct avec le vol ». Ces informations ne sauraient, dès lors, inclure, par exemple, celles relatives aux modalités de paiement d'autres services non directement liés au vol, comme la location d'un véhicule à l'arrivée (157).

164. Quant au point 8, visant les « [i]nformations "grands voyageurs" », il est défini par les normes de l'OACI comme portant sur le numéro de compte et le statut du grand voyageur (158). Interprété en ce sens, ce point satisfait aux exigences de clarté et de précision.

165. S'agissant du point 10 de l'annexe I, visant le « [s]tatut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation » et du point 13 de cette annexe, concernant les « [i]nformations 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 », malgré leur libellé ouvert, ces points ne visent que des informations très précises et clairement identifiables, en rapport direct avec le vol. Cela vaut également pour ce qui est du point 14 de l'annexe I, visant le « numéro du siège et autres informations concernant le siège » et du point 16 de cette annexe, visant « toutes les informations relatives aux bagages ».

– *Sur l'étendue des données énumérées à l'annexe I (deuxième question préjudicielle)*

166. Parmi les éléments dont la Cour tient compte pour apprécier le caractère proportionné d'une mesure comportant des ingérences dans les droits consacrés aux articles 7 et 8 de la Charte figure le caractère adéquat, pertinent et non excessif des données à caractère personnel traitées (principe de la « minimisation des données ») (159). Le même test est prévu par la jurisprudence de la Cour EDH (160) et préconisé par la convention 108 (161).

167. Il résulte du considérant 15 de la directive PNR que la liste des données PNR à transmettre aux UIP a été établie dans le but, à la fois, de refléter les exigences légitimes des pouvoirs publics en matière de lutte contre le terrorisme et les formes graves de criminalité et de protéger les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel par l'application de « normes élevées », conformément à la Charte, à la convention 108 et à la CEDH. Le même considérant précise que les données PNR ne devraient, notamment, comporter que des informations relatives aux réservations et aux itinéraires de voyage des passagers qui permettent aux autorités compétentes d'identifier les passagers aériens représentant une menace pour la sécurité intérieure.

168. S'agissant, en premier lieu, du caractère adéquat et pertinent des données PNR figurant à l'annexe I, les différents points de cette annexe, y inclus les points 5, 6, 8 et 18, tels que je propose de les interpréter (162), et le point 12, à l'exception de la partie que je propose de déclarer invalide (163), ne visent que des données fournissant des informations directement liées aux voyages aériens entrant dans le champ d'application de la directive PNR. Ces données entretiennent, en outre, un lien objectif avec les finalités poursuivies par cette directive. Plus particulièrement, les données API sont susceptibles d'être utilisées notamment en « mode réactif », afin d'identifier une personne déjà connue par les services répressifs, par exemple parce qu'elle est suspectée d'être impliquée dans des infractions terroristes ou des formes graves de criminalité qui ont déjà été commises, ou d'être sur le point de commettre une telle infraction, alors que les données PNR sont susceptibles d'être utilisées plutôt en « mode réel ou proactif », afin d'identifier des menaces provenant de personne non encore connues par les services répressif.

169. En ce qui concerne, en second lieu, l'étendue des données PNR énumérées à l'annexe I, ces données, y inclus celles figurant sous les points 5, 6, 8 12 et 18 de cette annexe, tels que je propose de les interpréter aux points 134 à 164 des présentes conclusions, n'apparaissent pas excessives, compte tenu, d'une part, de l'importance de l'objectif de sécurité publique poursuivi par la directive PNR et, d'autre part, de l'aptitude du régime institué par cette directive à poursuivre un tel objectif.

170. S'agissant, notamment, des données API, sur lesquelles s'interroge en particulier la juridiction de renvoi, je relève que ces données, d'ordre biographique et concernant le trajet emprunté, ne permettent, en règle générale, de tirer que des informations limitées sur la vie privée des passagers concernés. Par ailleurs, s'il est vrai que le point 18 de l'annexe I vise des informations qui ne figurent pas parmi celles expressément mentionnées à l'article 3, paragraphe 2, de la directive API, ces informations, relatives à l'identité du passager aérien (le sexe), au document de voyage utilisé (pays de délivrance, date d'expiration de tout document d'identité), ou encore au vol emprunté (compagnie aérienne, numéro de vol, date et aéroport de départ et d'arrivée), se recoupent en partie ou peuvent être extraites des données PNR figurant à d'autres points de l'annexe I, par exemple les points 3, 7 et 13. En outre, dans la mesure où elles portent sur des données biographiques ou sur les documents de voyage utilisés, lesdites informations sont susceptibles d'aider les services répressifs à vérifier l'identité d'une personne et réduisent ainsi, comme le relève le considérant 9 de la directive PNR, le risque de soumettre des personnes innocentes à des vérifications et à des enquêtes injustifiées. Enfin, il convient de souligner que le seul fait que le point 18 de l'annexe I inclut des données supplémentaires par rapport à celles qui figurent à l'article 3, paragraphe 2, de la directive API ne saurait conduire automatiquement à affirmer le caractère excessif de ces données, dans la mesure où cette directive et la directive PNR poursuivent des objectifs différents.

171. Quant aux données concernant les mineurs non accompagnés, énumérées au point 12 de l'annexe I, elles visent une catégorie vulnérable de personnes bénéficiant d'une protection particulière, y inclus en ce qui concerne le respect de leur vie privée et la protection de leurs données personnelles (164). Il n'en demeure pas moins qu'une limitation de ces droits peut s'avérer nécessaire, notamment pour protéger les enfants de formes graves de criminalité dont ils peuvent être victimes, telles que la traite et l'exploitation sexuelle des enfants ou l'enlèvement d'enfants. Il ne saurait donc a priori être considéré que le point 12 de l'annexe I, en ce qu'il exige le transfert d'un nombre de données personnelles plus important pour ce qui concerne les mineurs non accompagnés excède ce qui est strictement nécessaire.

172. Si les données à caractère personnel que les transporteurs aériens sont tenus de transmettre aux UIP conformément à la directive PNR répondent, à mon sens, aux exigences d'adéquation et de pertinence et si leur étendue n'excède pas ce qui est strictement nécessaire au fonctionnement du régime institué par cette directive, il n'en demeure pas moins qu'une telle transmission concerne un nombre significatif de données à caractère personnel de natures variées pour chaque passager concerné ainsi qu'un nombre extrêmement élevé de telles données en termes absolus. Dans ces circonstances, il est primordial qu'un tel transfert soit entouré de garanties suffisantes visant, d'une part, à veiller à ce que ne soient transférées que les données expressément visées et, d'autre part, à assurer la sécurité et la confidentialité des données transférées.

173. À cet égard, il convient de relever, d'une part, que le législateur de l'Union a, tout d'abord, prévu une série de garanties permettant de limiter les catégories de données PNR rendues accessibles par les services répressifs et d'assurer que cet accès reste circonscrit aux seules données dont le traitement est considéré comme étant nécessaire aux fins des objectifs poursuivis par la directive PNR. Ainsi, premièrement, cette directive énumère, sous réserve des considérations développées dans le cadre de la réponse à la troisième question préjudicielle, de manière exhaustive et précise les données qui peuvent être transférées aux UIP. Deuxièmement, la directive PNR

indique explicitement que seules les données contenues dans cette liste, qui résulte d'une pondération entre les différents intérêts et exigences mentionnés au considérant 15 de cette directive, peuvent faire l'objet d'un transfert aux UIP (article 6, paragraphe 1, de la directive PNR). Troisièmement, cette directive précise que, lorsque les données PNR transférées comportent des données autres que celles énumérées à l'annexe I, l'UIP les efface « immédiatement et de façon définitive dès leur réception » (article 6, paragraphe 1, de la directive PNR). Quatrièmement, ladite directive prévoit que les données PNR visées à l'annexe I peuvent faire l'objet de transfert seulement pour autant qu'elles aient déjà été recueillies par les transporteurs aériens dans le cours normal de leurs activités (article 8, paragraphe 1, et considérant8, de la directive PNR), ce qui implique que toutes les données figurant dans l'annexe I ne sont pas systématiquement accessibles aux UIP, mais que seules celles qui figurent dans le système de réservation de l'opérateur concerné le sont. Cinquièmement, l'article 8, paragraphe 1, de la directive PNR impose aux transporteurs aériens d'utiliser la méthode « push » pour transmettre les données PNR aux UIP. Cette méthode, recommandée par les lignes directrices de l'OACI (165), implique que lesdits transporteurs transfèrent eux-mêmes les données PNR dans les bases de données des UIP. Par rapport à la méthode « pull », qui permet aux autorités compétentes d'accéder aux systèmes des exploitants et extraire de leurs bases de données une copie des données requises, la méthode « push », présente plus de garanties puisqu'elle confère au transporteur aérien concerné le rôle de gardien et de contrôleur des données PNR. Enfin, se conformant aux lignes directrices de l'OACI et au principe du « guichet unique » (166), la directive PNR prévoit que le transfert des données PNR intervienne par l'intermédiaire d'un seul organisme, l'UIP, qui agit sous la supervision du délégué visé à l'article 5 de cette directive et, surtout, sous celle de l'autorité de contrôle nationale visée à l'article 15 de ladite directive.

174. D'autre part, la directive PNR prévoit un certain nombre de garanties visant à préserver la *sécurité* des données PNR. Je renvoie à cet égard à l'article 13, paragraphe 2, de cette directive, qui rend applicable à tous les traitements de données à caractère personnel effectués en vertu de celle-ci les articles 28 et 29 de la directive police, concernant la confidentialité du traitement et la sécurité des données, ainsi qu'au paragraphe 3 de ce même article qui, s'agissant du traitement des données PNR par les transporteurs aériens, rappelle les obligations qui incombent à ces derniers en vertu du RGPD, notamment en ce qui concerne les mesures techniques et organisationnelles appropriées à prendre pour protéger la sécurité et la confidentialité de ces données (167).

175. Enfin, il y a lieu de souligner que la directive PNR reconnaît, à ses considérants 29 et 37, le droit des passagers à recevoir des « informations précises, aisément accessibles et facilement compréhensibles », entre autres, sur la collecte des données PNR, en sollicitant les États membres à veiller à ce que ce droit soit respecté. Si cette reconnaissance ne se traduit pas, dans le texte de la directive PNR, en une disposition ayant une valeur contraignante, je rappelle que, ainsi que je l'ai indiqué lors de l'examen de la première question préjudicielle, les dispositions du RGPD s'appliquent au transfert des données PNR aux UIP. Les transporteurs aériens sont, dès lors, tenus, dans le cadre de ce transfert, de se conformer, entre autres, aux articles 13 et 14 du RGPD, prévoyant le droit à l'information des personnes concernées par un traitement de données à caractère personnel. S'il conviendrait que, dans le cadre de la transposition de la directive PNR, les États membres prévoient expressément le droit à l'information des passagers aériens, tel qu'il est reconnu par les considérants 29 et 37 de cette directive, il leur est en tout cas exclu, en ce qu'il serait contraire à l'esprit de celle-ci, de limiter la portée des articles 13 et 14 du RGPD en application de l'article 23, paragraphe 1, de ce règlement. Or, pour être effectif, un tel droit doit porter également sur les catégories de données PNR faisant l'objet de transfert.

176. Compte tenu de l'ensemble des considérations qui précèdent, je suis de l'avis que les données PNR dont le traitement est prévu par la directive PNR, sous réserve des limitations suggérées et des

précisions apportées dans le cadre de la troisième question préjudicielle, sont pertinentes, adéquates et non excessives eu égard aux finalités poursuivies par cette directive et que leur étendue ne dépasse pas ce qui est strictement nécessaire à la réalisation de ces finalités.

– *Sur les données sensibles*

177. La directive PNR interdit de manière générale tout traitement des « données sensibles » (168).

178. Si cette directive ne contient pas de définition de la notion de « données sensibles », il ressort de son article 13, paragraphe 4, que celle-ci inclut, à tout le moins, les « 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 » (169). Au point 165 de l'avis 1/15, la Cour a précisé que toute mesure fondée sur le postulat selon lequel une ou plusieurs de ces caractéristiques « pourraient, par elles-mêmes et indépendamment du comportement individuel du voyageur concerné, être pertinentes au regard de la finalité des traitements des données PNR [...] méconnaîtrait les droits garantis aux articles 7 et 8 de la Charte, lus en combinaison avec l'article 21 de celle-ci ». En interdisant tout traitement des données visées à son article 13, paragraphe 4, la directive PNR respecte donc les limites imposées par la Cour à l'utilisation de ces catégories de données dans le cadre d'un système de traitement des données PNR, qu'il relève du droit national, du droit de l'Union ou d'un accord international conclu par l'Union.

179. L'interdiction générale de traitement des données sensibles édictée par la directive PNR inclut également leur *collecte*. Ainsi, comme l'indique expressément le considérant 15 de cette directive, les 19 rubriques figurant à l'annexe I ne sont pas fondées sur les données PNR visées à l'article 13, paragraphe 4, de celle-ci.

180. Si aucune de ces rubriques ne vise explicitement de telles données, ces dernières pourraient néanmoins relever notamment de la rubrique « Remarques générales », visée au point 12 de l'annexe I, qui constitue un « champ ouvert », pouvant couvrir, ainsi que j'ai déjà eu l'occasion de l'observer dans le cadre de l'examen de la troisième question préjudicielle, un nombre indéfini d'informations de natures diverses. Il existe en effet un risque concret, comme l'a d'ailleurs relevé la Cour au point 164 de l'avis 1/15, que des informations relevant de ladite rubrique, portant par exemple sur des préférences diététiques, des demandes d'assistance, des forfaits de prix en faveur de certaines catégories de personnes ou d'associations, révèlent, de manière directe, des données sensibles au sens de l'article 13, paragraphe 4, de la directive PNR, relatives notamment aux convictions religieuses des passagers concernés, à leur état de santé ou à leur appartenance à un syndicat ou à un parti politique.

181. Or, puisque le traitement de ces données est de toute manière exclu par la directive PNR, leur transfert par les transporteurs aériens non seulement excède manifestement ce qui est strictement nécessaire, mais s'avère également dépourvu de toute utilité. À cet égard, il importe de souligner que le fait que les UIP sont en tout cas tenues, conformément à l'article 13, paragraphe 4, seconde phrase, de la directive PNR, d'effacer immédiatement les données PNR révélant l'une des informations énumérées à la première phrase de ce paragraphe ne permet pas d'autoriser ou de justifier un transfert de ces données (170), l'interdiction de traitement de celles-ci édictée par ladite directive devant opérer à partir de la première étape de traitement des données PNR. L'obligation d'effacement des données sensibles ne constitue donc qu'une garantie supplémentaire que cette directive prévoit dans l'hypothèse où, exceptionnellement, de telles données seraient transférées aux UIP par erreur.

182. Je relève, par ailleurs, ainsi que l'a remarqué M. l'avocat général Mengozzi au point 222 de ses conclusions dans l'avis 1/15 (171), que, puisque les informations relevant des rubriques « texte libre » telle que la rubrique « Remarques générales », visée au point 12 de l'annexe I susceptibles de contenir des données sensibles au titre de l'article 13, paragraphe 4, de la directive PNR ne sont communiquées par les passagers que de manière facultative, il est peu probable que des personnes impliquées dans des infractions de terrorisme ou relevant de la criminalité grave procèdent à une telle communication spontanée, de sorte que le transfert systématique de ces données n'est vraisemblablement susceptible de concerner, pour la plupart, que des personnes ayant demandé à bénéficier d'un service supplémentaire qui ne présentent en réalité aucun intérêt pour les services répressifs (172).

183. Dans le cadre de l'examen de la troisième question préjudicielle, je suis arrivé à la conclusion que le point 12 de l'annexe I, en ce qu'il vise la rubrique « Remarques générales », ne satisfait pas aux exigences de clarté et de précision requises à l'article 52, paragraphe 1, première phrase, de la Charte. Pour les raisons que je viens d'exposer, j'estime que l'inclusion de cette rubrique dans les catégories de données faisant l'objet d'un transfert systématique aux UIP, sans qu'aucune précision ne soit apportée quant aux informations qu'elle est susceptible de viser, ne satisfait pas non plus au critère de nécessité prévu à l'article 52, paragraphe 1, seconde phrase, de la Charte, tel qu'interprété par la Cour (173).

184. Cela étant, exclure les rubriques dites « texte libre » de la liste des données PNR à transférer aux autorités étatiques dans le cadre d'un système de traitement des données PNR ne suffit pas à éliminer le risque que des données sensibles soient néanmoins mises à la disposition de ces autorités. De telles données peuvent en effet non seulement être directement inférées d'informations relevant de telles rubriques, mais également être indirectement révélées ou présumées par des informations contenues dans des rubriques « codées ». Ainsi, pour donner un exemple, le nom du passager aérien peut fournir des indications ou, à tout le moins, permettre d'avancer des hypothèses, sur l'origine ethnique ou sur l'appartenance religieuse du passager concerné. Il en va de même de la nationalité. Ces données ne se prêtent, en principe, pas à être exclues de la liste des données PNR à transférer, ni à être effacées par les autorités habilitées à les réceptionner. Dès lors, afin d'éviter le risque de stigmatisation, sur la base de caractéristiques protégées, d'un grand nombre d'individus qui ne sont pourtant soupçonnés d'aucune infraction, il importe qu'un système de traitement des données PNR prévoie des garanties suffisantes permettant d'exclure, à chaque étape du traitement des données collectées, que ce traitement puisse directement ou indirectement prendre en compte de telles caractéristiques, par exemple en appliquant, lors de l'analyse automatisée, des sélecteurs fondés sur ces caractéristiques. Je reviendrai sur ce point dans la suite de mon examen.

185. Sur la base de l'ensemble des considérations qui précèdent, j'estime, sous réserve de la conclusion à laquelle je suis arrivé au point 183 ci-dessus, que la directive PNR prévoit, au stade du transfert des données PNR aux UIP, des garanties suffisantes visant à protéger les données sensibles.

iii) *Sur la notion de « passager » (quatrième question préjudicielle)*

186. Par sa quatrième question préjudicielle, la juridiction de renvoi demande en substance à la Cour si le système établi par la directive PNR, en ce qu'il permet le transfert et le traitement généralisés des données PNR de toute personne répondant à la notion de « passager » au sens de l'article 3, point 4, de cette directive, indépendamment de tout élément objectif permettant de considérer que la personne concernée est susceptible de présenter un risque pour la sécurité publique, est compatible avec les articles 7, 8, et l'article 52, paragraphe 1, de la Charte. Elle s'interroge notamment sur la possibilité de transposer au système de traitement de données à

caractère personnel instauré par la directive PNR la jurisprudence de la Cour en matière de conservation et d'accès aux données dans le secteur des communications électroniques.

187. Dans cette jurisprudence, pour ce qui revêt un intérêt dans la présente procédure, la Cour a conclu qu'une réglementation qui, en vue de lutter contre la criminalité grave, prévoit la *conservation* préventive généralisée et indifférenciée des données relatives au trafic afférentes aux communications électroniques et des données de localisation (174), en vue de l'accès de la part des autorités répressives, sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi, ne saurait, en principe, être considérée comme étant justifiée dans une société démocratique (175). La Cour en a jugé de même s'agissant d'une réglementation nationale qui, en vue de la lutte contre le terrorisme, prévoyait l'*analyse automatisé de la totalité desdites* données au moyen d'un filtrage effectué par les fournisseurs de services de communications électroniques à la demande des autorités nationales compétentes et en application de paramètres déterminés par celles-ci (176). Selon la Cour, de telles mesures ne sauraient être justifiées que dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, et lorsque la décision prévoyant leur mise en œuvre fait l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante (177). Le recours à ces mesures dans de telles situations doit, en outre, selon la Cour, être temporellement limité au strict nécessaire et ne saurait en tout cas avoir un caractère systématique (178).

188. Je relève, par ailleurs, que si, dans cette jurisprudence, la Cour n'est pas allée jusqu'à affirmer expressément, comme dans l'arrêt Schrems I, l'existence d'une atteinte au contenu essentiel du droit au respect de la vie privée, elle a néanmoins considéré que les mesures en cause atteignaient un niveau de gravité de l'ingérence tel que, sauf dans le cas limité de menaces spécifiques à la sécurité nationale d'un État membre, elles ne pouvaient tout simplement pas être considérées comme étant limitées au strict nécessaire et donc être conformes à la Charte (179), indépendamment des éventuelles garanties prévues contre les risques d'abus et d'accès illicite aux données concernées (180).

189. J'ai déjà eu l'occasion de souligner qu'une réglementation comme celle prévue par la directive PNR partage, avec des mesures du type de celles examinées par la Cour dans la jurisprudence rappelée aux points précédents des présentes conclusions, un certain nombre d'éléments communs, qui lui confèrent un caractère particulièrement intrusif. Ainsi, cette directive institue un système généralisé et indifférencié de collecte et d'analyse automatisée des données personnelles d'une portion significative de la population, s'appliquant de manière globale à l'ensemble des personnes répondant à la notion de « passagers » figurant à l'article 3, point 4, de ladite directive et, par suite, également à celles pour lesquelles il n'existe aucun indice de nature à laisser croire que les comportements de ces personnes pourraient avoir un lien, même indirect ou lointain, avec des activités de terrorisme ou relevant de la criminalité grave. C'est dans ces circonstances que la juridiction de renvoi se pose la question de savoir si cette jurisprudence est transposable à un système de traitement des données PNR tel que celui institué par la directive PNR.

190. À cet égard, je relève que, dans l'avis 1/15, lorsqu'elle a examiné, aux points 186 à 189 de celui-ci, le champ d'application ratione personae du projet d'accord PNR Canada-UE, la Cour a évité toute mise en parallèle entre, d'une part, les mesures visant la conservation et l'accès généralisé et indifférencié au contenu des communications électroniques, aux données relatives au trafic et aux données de localisation et, d'autre part, le transfert des données PNR et leur traitement automatisé dans le cadre de l'évaluation préalable des passagers visé par ledit accord. Il existait pourtant déjà, à l'époque où cet avis avait été prononcé, une jurisprudence bien établie – confirmée, quelques mois seulement avant ce prononcé, par l'arrêt Tele2 Sverige, auquel renvoie la juridiction

de renvoi –, dans laquelle lesdites mesures étaient, sauf situations spécifiques et ponctuelles (181), jugées incompatibles avec la Charte (182). Les arrêts les plus récents de la Cour dans ce domaine, et notamment l'arrêt La Quadrature du Net, se situent dans le sillage de cette jurisprudence, en la précisant et, sous certains aspects, en la nuançant.

191. Dans lesdits points de l'avis 1/15, la Cour a explicitement considéré qu'il n'apparaissait pas que l'accord PNR Canada-UE dépassait les limites du strict nécessaire en ce qu'il permettait le *transfert* et le *traitement automatisé*, aux fins de leur évaluation préalable, des données PNR de l'ensemble des passagers aériens vers le Canada, et cela bien qu'un tel transfert et un tel traitement fussent censés intervenir « indépendamment de tout élément objectif permettant de considérer que les passagers sont susceptibles de présenter un risque pour la sécurité publique au Canada » (183). Au point 187 de cet avis, la Cour est allée jusqu'à affirmer que « l'exclusion de certaines catégories de personnes, ou de certaines zones d'origine, serait de nature à faire obstacle à la réalisation de l'objectif du traitement automatisé des données PNR, à savoir l'identification, au moyen d'une vérification de ces données, des personnes susceptibles de présenter un risque pour la sécurité publique parmi l'ensemble des passagers aériens, et à permettre que cette vérification puisse être contournée » (184).

192. Ainsi, à tout le moins pour ce qui est du transfert généralisé et indifférencié des données PNR, la Cour s'est démarquée de l'approche, plus rigoureuse, adoptée en matière de conservation et d'accès aux métadonnées.

193. S'il est indéniable que, dans son raisonnement, elle a tenu compte, ainsi que cela ressort notamment des points 152 et 188 de l'avis 1/15, d'une part, de la constatation selon laquelle le traitement automatisé des données PNR facilite les contrôles de sécurité, notamment aux frontières, et, d'autre part, du fait que, conformément à la convention de Chicago, les passagers aériens désireux d'entrer sur le territoire d'un État partie à cette convention sont tenus de se soumettre aux contrôles et de respecter les conditions d'entrée et de sortie prescrites par cet État, y inclus la vérification de leurs données PNR, j'estime que d'autres raisons militent en faveur d'une telle diversité d'approche et, parmi celles-ci, en premier lieu, la nature des données traitées.

194. La Cour a maintes fois souligné que non seulement le contenu des communications électroniques, mais également les métadonnées sont susceptibles de révéler des informations sur « un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé », que ces données, prises dans leur ensemble, « peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci » et que lesdites données fournissent, en particulier, les moyens d'établir « le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications des données » (185). Je rappelle, par ailleurs, que les réglementations examinées jusqu'ici par la Cour, y inclus celle contenue dans la directive 2006/24, ne prévoyaient aucune exception et s'appliquaient également aux communications vers ou à partir de services à caractère social ou religieux ou de professionnels soumis à des obligations de secret professionnel. Ainsi, tout en n'établissant pas une violation du contenu essentiel du droit au respect de la vie privée, la Cour a néanmoins affirmé que, « compte tenu du caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée » (186).

195. En revanche, s'il est vrai que, comme je l'ai rappelé aux points 77 et 98 des présentes conclusions, la Cour a reconnu, dans l'avis 1/15, que les données PNR peuvent, le cas échéant, révéler des informations très précises sur la vie privée d'une personne (187), elle a néanmoins affirmé que la nature de ces informations est limitée à certains aspects de cette vie privée (188), ce qui rend l'accès à de telles données moins intrusif que l'accès au contenu des communications électroniques ainsi qu'aux données relatives au trafic et aux données de localisation.

196. En deuxième lieu, non seulement la nature des données PNR diffère de celle des données relatives au trafic et des données de localisation, mais également diffèrent le nombre et la variété des informations susceptibles d'être révélées par ces diverses catégories de données, celles contenues dans les données PNR étant tant quantitativement que qualitativement plus limitées. Cela dépend non seulement du fait que les systèmes de traitement généralisé et indifférencié des données relatives aux communications électroniques sont susceptibles de concerner la presque totalité de la population visée, alors que les systèmes de traitement des données PNR s'appliquent à un cercle plus restreint, bien que numériquement significatif, d'individus, mais également de la fréquence d'utilisation des moyens de communications électroniques et de la multiplicité de ceux-ci. Par ailleurs, la directive PNR prévoit la collecte et le traitement d'un nombre limité et exhaustivement déterminé de données PNR, à l'exclusion de données relevant des catégories énumérées à l'article 13, paragraphe 4, de cette directive, de sorte que, sinon la quantité à tout le moins la sensibilité des informations sur la vie privée des personnes concernées qui peuvent en découler sont susceptibles d'être, en partie, appréciées à l'avance (189). Or, une telle limitation de la typologie de données visées, permettant d'exclure une grande partie de celles pouvant receler des informations sensibles, n'est que partiellement possible s'agissant des données relatives au trafic et des données de localisation, compte tenu du nombre d'utilisateurs et de moyens de communication concernés (190).

197. En troisième lieu, tout traitement des métadonnées des communications électroniques non seulement est susceptible de toucher à la sphère intime de la vie de presque la totalité de la population, mais aussi empiète sur l'exercice d'autres libertés au travers desquelles s'exerce la participation de chaque individu à la vie sociale et démocratique d'un pays (191), et risque, notamment, d'entraîner un effet dissuasif sur la liberté d'expression des utilisateurs des moyens de communications électroniques (192), qui constitue « l'un des fondements essentiels d'une société démocratique et pluraliste » faisant partie des valeurs sur lesquelles est fondée l'Union (193). Cet aspect est inhérent aux mesures portant sur ces catégories de données à caractère personnel et ne concerne en principe pas les systèmes de traitement des données PNR.

198. En quatrième lieu, en raison principalement du nombre et de la variété des informations à caractère sensible pouvant être extraites du contenu des communications électroniques ainsi que des données relatives au trafic et des données de localisation, il existe un risque d'arbitraire lié au traitement de ces données significativement plus élevé qu'en ce qui concerne les systèmes de traitement des données PNR.

199. Pour l'ensemble des raisons que je viens d'exposer, je suis de l'avis que l'approche plus stricte adoptée par la Cour dans le domaine des communications électroniques n'est pas transposable en tant que telle aux systèmes de traitement des données PNR. La Cour s'est déjà exprimée, à tout le moins implicitement, en ce sens dans l'avis 1/15, dans le contexte d'un accord international instituant un tel système aux fins de la protection de la sécurité d'un pays tiers. La même position se justifie, à mon sens, à plus forte raison, s'agissant de la directive PNR, dont l'objectif est la protection de la sécurité interne de l'Union.

200. Cela étant dit, il y a lieu de relever, comme l'a fait l'avocat général Mengozzi au point 216 de ses conclusions dans l'avis 1/15 (194), que l'intérêt même des systèmes de traitement des données PNR, qu'ils soient adoptés de manière unilatérale ou qu'ils fassent l'objet d'un accord international, est précisément de garantir la transmission massive de données permettant aux autorités compétentes d'identifier, à l'aide d'outils de traitement automatisé et de scénarios ou de critères d'évaluation préétablis, des individus, inconnus des services répressifs, mais qui paraissent présenter un « intérêt » ou un risque pour la sécurité publique et qui sont, dès lors, susceptibles d'être soumis ultérieurement à des contrôles individuels plus poussés. L'exigence d'un « soupçon raisonnable » que l'on trouve affirmée dans la jurisprudence de la Cour EDH relative aux interceptions ciblées pratiquées dans le cadre d'une enquête pénale (195) et dans celle de la Cour sur la conservation des métadonnées (196) est, dès lors, moins pertinente dans le contexte d'une telle transmission et d'un tel traitement (197). L'objectif, notamment, de prévention poursuivi par de tels régimes ne saurait non plus être réalisé en circonscrivant leur application à une catégorie déterminée d'individus, comme la Cour l'a d'ailleurs affirmé dans les points de l'avis 1/15 rappelés au point 191 des présentes conclusions, de sorte que la portée de la directive PNR apparaît assurer la réalisation efficace de cet objectif (198).

201. Il convient également de souligner que l'importance stratégique du traitement des données PNR en tant qu'instrument essentiel de la réponse commune de l'Union au terrorisme et aux formes graves de criminalité et en tant que composante majeure de l'Union de la sécurité a été mise en exergue à plusieurs reprises par la Commission (199). Dans le cadre d'une « démarche globale » pour la lutte contre le terrorisme, le rôle joué par les systèmes de traitement des données PNR a également été reconnu par le Conseil de sécurité des Nations unies qui, dans la résolution 2396 (2017) (200), a imposé aux États membres des Nations unies de « renfor[cer] leur capacité de collecter, de traiter et d'analyser, dans le cadre des normes et pratiques recommandées de l'OACI, les données des [PNR] et de veiller à ce que ces données soient communiquées à toutes les autorités nationales compétentes et utilisées par celles-ci, dans le plein respect des droits de l'homme et des libertés fondamentales aux fins de prévenir, de détecter et d'instruire les infractions terroristes et les voyages de terroristes » (201). Cette obligation est réaffirmée dans la résolution 2482/2019 en matière de terrorisme et de criminalité transnationale grave (202).

202. Dans ce contexte, l'adoption d'un système de traitement des données PNR harmonisé au niveau de l'Union, pour ce qui concerne tant les vols extra-UE que, pour les États qui ont fait usage de l'article 2 de la directive PNR, les vols intra-UE, permet d'assurer que le traitement de ces données intervient dans le respect du niveau élevé de protection des droits consacrés aux articles 7 et 8 de la Charte fixé par cette directive et fournit un système juridique de référence pour la négociation d'accords internationaux sur le traitement et le transfert des données PNR (203).

203. Par ailleurs, s'il est vrai que le système mis en place par la directive PNR vise de manière indifférenciée tous les passagers aériens, comme l'a à juste titre souligné notamment le Parlement dans ses observations écrites et comme l'a également mis en exergue le Conseil de sécurité des Nations unies dans la résolution 2396 (2017), qui évoque le risque concret d'utilisation de l'aviation civile à des fins terroristes à la fois comme moyen de transport et comme cible (204), il existe un lien objectif entre le transport aérien et les menaces pour la sécurité publique se ralliant, notamment, au terrorisme et, à tout le moins, à certaines formes de criminalité grave, telles que, en particulier, le trafic de drogue ou le trafic d'êtres humains, qui ont, au demeurant, une forte composante transfrontalière.

204. Il importe, enfin, de souligner, ainsi que l'ont fait valoir le Parlement, le Conseil et plusieurs États membres ayant déposé des observations écrites, que les passagers aériens à l'entrée ou à la sortie de l'Union, sont tenus de se soumettre à des contrôles de sécurité (205). Le transfert et le

traitement des données PNR avant leur arrivée ou avant leur départ facilite et accélère ces contrôles, ainsi que la Cour l'a également relevé dans l'avis 1/15, en permettant aux services répressifs de se concentrer sur les passagers pour lesquels ils disposent d'éléments factuels indiquant un risque réel pour la sécurité (206).

205. Enfin, s'agissant, notamment, de l'extension du système de la directive PNR aux vols intra-UE, si tout impact sur la liberté de circulation des citoyens de l'Union, consacrée notamment à l'article 45 de la Charte, ne peut pas être a priori exclu, l'ingérence dans la vie privée que comporte la directive PNR, bien que grave, n'est, à mon sens, pas telle qu'elle entraînerait, en elle-même, un effet dissuasif sur l'exercice de cette liberté, le traitement de données PNR pouvant même être perçu par le public comme une mesure nécessaire à assurer la sûreté des voyages par voie aérienne (207). Il reste que l'éventualité d'un tel effet dissuasif doit faire l'objet d'une évaluation et d'un monitorage continus.

206. Cependant, afin de respecter la jurisprudence rappelée aux points 107 et 108 des présentes conclusions, la directive PNR ne saurait se limiter à exiger que l'accès et le traitement automatisé des données PNR de l'ensemble des passagers aériens réponde à la finalité poursuivie, mais elle doit également prévoir, et cela de manière claire et précise, les conditions matérielles et procédurales régissant cet accès et ce traitement ainsi que l'utilisation ultérieure de ces données (208), et prévoir des garanties adéquates à chaque étape de ce processus. J'ai déjà évoqué, lors de l'examen de la deuxième question préjudicielle, les garanties qui entourent le transfert des données PNR aux UIP. Je passerai en revue, lors de l'examen de la sixième question préjudicielle, celles qui accompagnent plus spécifiquement le traitement automatisé de ces données, ainsi que, dans le cadre de l'examen de la huitième question préjudicielle, celles liées à la conservation de celles-ci.

207. Avant de poursuivre cet examen, je souhaite souligner, l'importance fondamentale que revêt, dans le cadre du système de garanties mis en place par la directive PNR, le contrôle exercé par l'autorité indépendante visée à l'article 15 de cette directive. Conformément à cet article, tout traitement de données prévu par ladite directive est soumis à la surveillance d'une autorité de contrôle indépendante, qui a le pouvoir de vérifier la licéité de ce traitement, d'effectuer des enquêtes, des inspections et des audits, et de traiter les réclamations introduites par toute personne concernée. Un tel contrôle, exercé par un sujet externe, chargé de la défense d'intérêts potentiellement en conflit avec ceux poursuivis par les auteurs des traitements des données PNR, et investi du rôle de veiller au respect de l'ensemble des limitations et des garde-fous qui entourent lesdits traitements, constitue une garantie essentielle, explicitement énoncée à l'article 8, paragraphe 3, de la Charte, dont l'efficacité, en termes de protection des droits fondamentaux concernés, est même supérieure au système des voies de recours mises à la disposition des particuliers. Il est dès lors fondamental, à mon sens, que la Cour interprète extensivement la portée des pouvoirs de surveillance prévus à l'article 15 de la directive PNR et que les États membres, lors de la transposition de cette directive en droit interne, reconnaissent à leur autorité nationale de contrôle toute l'étendue de ces pouvoirs en la dotant des moyens matériels et personnels nécessaires à l'accomplissement de sa tâche.

208. Sur la base de l'ensemble des considérations qui précèdent, j'estime que la directive PNR ne dépasse pas les limites du strict nécessaire en ce qu'elle permet le transfert et le traitement automatisé des données de toute personne répondant à la notion de « passager » au sens de l'article 3, point 4, de cette directive.

iv) *Sur le caractère suffisamment clair précis et limité au strict nécessaire de l'évaluation préalable des passagers (sixième question préjudicielle)*

209. Par sa sixième question préjudicielle, la juridiction de renvoi demande en substance à la Cour si l'évaluation préalable visée par l'article 6 de la directive PNR est compatible avec les articles 7, 8, et l'article 52, paragraphe 1, de la Charte. Bien que le libellé de cette question se focalise sur le caractère systématique et généralisé du traitement automatisé des données PNR de tous les passagers aériens que comporte cette évaluation préalable, il ressort des motifs de la décision de renvoi que la Cour constitutionnelle sollicite de la Cour une appréciation plus globale du respect des exigences de légalité et de proportionnalité dans le contexte d'un tel traitement. Je procéderai ci-après à cette appréciation, tout en renvoyant à l'analyse effectuée lors de l'examen de la quatrième question préjudicielle pour ce qui est du caractère non ciblé dudit traitement automatisé.

210. L'article 6, paragraphe 2, sous a), de la directive PNR prévoit que les UIP procèdent à une évaluation préalable des passagers aériens avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci. Cette évaluation vise à identifier les personnes pour lesquelles est requis un examen plus approfondi de la part des autorités compétentes, « compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité ». Conformément à l'article 6, paragraphe 6, de la directive PNR, l'UIP d'un État membre transmet les données PNR des personnes identifiées dans le cadre de cette évaluation ou le résultat du traitement de ces données aux autorités compétentes, visées à l'article 7 de cette directive, de ce même État membre, en vue d'un « examen plus approfondi ».

211. Aux termes de l'article 6, paragraphe 3, de la directive PNR, l'évaluation préalable réalisée au titre du paragraphe 2, sous a), de cet article est conduite en confrontant les données PNR avec des bases de données « utiles » [article 6, paragraphe 3, sous a)] ou en les traitant au regard de critères établis [article 6, paragraphe 3, sous b)].

212. Avant d'aborder l'examen de chacun de ces deux types de traitements de données, je relève que ne ressort pas clairement du libellé de l'article 6, paragraphe 3, susmentionné le point de savoir si les États membres sont tenus de prévoir que l'évaluation préalable des passagers se fasse en procédant systématiquement et dans tous les cas tant à l'une qu'à l'autre analyse automatisée ou si, comme semblerait le corroborer l'emploi du verbe « pouvoir » et de la préposition disjonctive « ou », ils sont habilités à aménager leurs systèmes de sorte à réserver, par exemple, l'examen prévu au paragraphe 3, sous b, de cet article 6, à des cas précis. À cet égard, je précise que la proposition de directive PNR prévoyait que cet examen était conduit uniquement dans le cadre de la lutte contre les infractions transfrontalières graves (209).

213. À l'instar de la Commission, j'estime qu'il ressort notamment de l'économie de la directive PNR que les États membres sont tenus de prévoir les deux types de traitements automatisés, pour des raisons tenant également à l'exigence d'assurer une application la plus uniforme possible du système de traitement des données PNR de l'Union. Cela n'implique cependant pas que les États membres ne soient pas autorisés – et même tenus, afin de garantir que le traitement de données que comporte l'évaluation préalable effectuée conformément à l'article 6, paragraphe 2, sous a), de la directive PNR soit limité à ce qui est strictement nécessaire – à circonscrire l'analyse, au titre de l'article 6, paragraphe 3, sous b), de la directive PNR, en fonction de ses résultats en termes d'efficacité pour chacune des infractions visées par cette directive et, le cas échéant, à la réserver seulement à certaines de ces infractions. Dans un tel sens milite le considérant 7 de la directive PNR, selon lequel « pour veiller à ce que le traitement de données PNR reste limité à ce qui est nécessaire, la création et l'application de critères d'évaluation devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente ».

– *Sur la confrontation avec des bases des données au sens de l'article 6, paragraphe 3, sous a), de la directive PNR*

214. Le premier volet de l'évaluation préalable à laquelle procèdent les UIP, au titre de l'article 6, paragraphe 2, sous a), de la directive PNR, implique, conformément au paragraphe 3, sous a), de cet article, de confronter les données PNR (« data matching ») avec des bases de données, afin de rechercher d'éventuelles correspondances positives (« hits »). Ces hits sont destinés à être vérifiés par les UIP, conformément à l'article 6, paragraphe 5, de la directive PNR et, le cas échéant, à être traduites en « match » avant d'être communiqués aux autorités compétentes.

215. Ainsi que la Cour l'a reconnu au point 172 de l'avis 1/15, l'étendue de l'ingérence que comportent ces types d'analyses automatisées dans les droits consacrés aux articles 7 et 8 de la Charte dépend essentiellement des bases de données sur lesquelles se fondent celles-ci. Il est par conséquent essentiel que les dispositions qui prévoient de tels traitements de données identifient de manière suffisamment claire et précise les bases de données avec lesquelles le recoupement des données à traiter est autorisé.

216. Aux termes de l'article 6, paragraphe 3, sous a), de la directive PNR, les UIP procèdent à une confrontation des données PNR aux « bases de données utiles » (210) au regard des objectifs poursuivis par cette directive. Cette disposition mentionne également une catégorie spécifique de bases de données, à savoir celles concernant « les personnes ou les objets recherchés ou faisant l'objet d'un signalement », auxquelles le législateur de l'Union a donc entendu conférer explicitement la qualification d'« utiles » au sens de cette disposition.

217. Hormis cette précision, la notion de « bases de données utiles » n'est pas davantage explicitée. Il n'est notamment pas indiqué si, pour être considérées comme « utiles », les bases de données utilisées aux fins du recoupement des données PNR doivent être gérées par des autorités répressives ou, plus généralement, par toute autorité publique, ou simplement leur être directement ou indirectement accessibles. La nature des données que de telles bases sont susceptibles de contenir et leur rapport avec les objectifs poursuivis par la directive PNR ne sont pas non plus précisés (211). Il ressort par ailleurs du libellé de l'article 6, paragraphe 3, sous a), de la directive PNR que sont susceptibles d'être qualifiées de « bases de données utiles » des bases de données tant nationales et de l'Union qu'internationales, ce qui élargit davantage la liste des bases de données potentiellement visées et augmente le caractère ouvert de cette notion (212).

218. Dans ces conditions, en application du principe général d'interprétation rappelé au point 151 des présentes conclusions, il revient à la Cour d'interpréter, dans la mesure du possible, l'article 6, paragraphe 3, sous a), de la directive PNR et, notamment, la notion de « bases de données utiles » en conformité avec les exigences de clarté et de précision requises par la Charte. En outre, puisque cette disposition prévoit une ingérence dans les droits fondamentaux énoncés aux articles 7 et 8 de la Charte, elle doit être interprétée de manière restrictive et en tenant compte de l'exigence d'assurer un niveau élevé de protection de ces droits fondamentaux, telle qu'elle est affirmée notamment au considérant 15 de la directive PNR. Elle doit, en outre, être interprétée à la lumière du principe de la limitation des finalités pour lesquelles les données PNR peuvent être traitées, énoncé à l'article 1, paragraphe 2, de la directive PNR.

219. Compte tenu de ces critères, il y a lieu, à mon avis, d'interpréter la notion de « bases de données utiles » en ce sens qu'elle ne vise que les base de données nationales gérées par les autorités compétentes au titre de l'article 7, paragraphe 1, de la directive PNR, ainsi que les bases de données de l'Union et internationales directement exploitées par ces autorités dans le cadre de leur mission. Lesdites bases de données doivent en outre être en rapport direct et étroit avec les finalités

de lutte contre le terrorisme et la criminalité grave poursuivies par la directive PNR, ce qui implique qu'elles aient été développées pour ces finalités. Ainsi interprétée, cette notion vise essentiellement sinon exclusivement les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, explicitement mentionnées à l'article 6, paragraphe 3, sous a), de la directive PNR.

220. Sont de manière générale exclues de la notion de « bases de données utiles » les bases de données gérées ou exploitées par les services de renseignement des États membres, à moins qu'elles ne répondent strictement à la condition d'être en rapport étroit avec les objectifs poursuivis par la directive PNR, et que l'État membre en question reconnaisse à ses services de renseignement des compétences spécifiques dans le domaine répressif (213).

221. L'interprétation proposée ci-dessus est en conformité avec les recommandations formulées par la Cour au point 172 de l'avis 1/15.

222. Toutefois, même ainsi interprété, l'article 6, paragraphe 3, sous a), de la directive PNR ne permet pas une identification suffisamment précise des bases de données qui seront utilisées par les États membres dans le cadre du recoupement avec les données PNR et ne saurait être considérée comme répondant aux exigences découlant de l'article 52, paragraphe 1, de la Charte, tel qu'interprété par la Cour. Cette disposition doit dès lors être lue en ce sens qu'elle oblige les États membres, dans le cadre de la transposition en droit national de la directive PNR, à publier une liste desdites bases de données et à tenir celle-ci à jour. Il serait par ailleurs souhaitable qu'une liste des bases de données « utiles », au sens de l'article 6, paragraphe 3, sous a), de la directive PNR, gérées par l'Union en collaboration avec les États membres et des bases de données internationales soit rédigée au niveau de l'Union, afin de rendre uniforme à cet égard la pratique des États membres.

– *Sur le traitement des données PNR à l'égard de critères préétablis*

223. Le second volet de l'évaluation préalable au titre de l'article 6, paragraphe 2, sous a), de la directive PNR consiste en une analyse automatisée au regard de critères préétablis. Dans le cadre de cette analyse, les données PNR sont traitées, essentiellement à des fins prédictives, par l'application d'algorithmes censés permettre d'« identifier » les passagers qui pourrait être impliqués dans des infractions terroristes ou des formes de criminalité grave. Dans ce contexte, l'UIP procède en substance à une activité de profilage (214). Étant susceptible d'avoir des conséquences importantes pour les individus identifiés par l'algorithme (215), un tel traitement requiert un encadrement précis en ce qui concerne tant les modalités de sa réalisation que les garanties qui doivent l'entourer. En effet, ainsi que la Cour l'a relevé au point 172 de l'avis 1/15, l'étendue de l'ingérence que comportent ces types d'analyses dans les droits consacrés aux articles 7 et 8 de la Charte dépend essentiellement des modèles et des critères préétablis appliqués.

224. À cet égard, je relève, en premier lieu, que l'article 6, paragraphe 4, deuxième phrase, de la directive PNR précise que les critères préétablis au regard desquels est réalisée l'évaluation préalable prévue à l'article 6, paragraphe 3, sous b), de cette directive doivent être « ciblés, proportionnés et spécifiques ». La première de ces exigences se rapporte à l'objectif visé par l'évaluation préalable prévue au paragraphe 2, sous a), de cet article, à savoir l'identification des personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes, et répond ainsi à la nécessité, mise en exergue par la Cour dans l'avis 1/15, que les critères utilisés parviennent à « cibler » les individus à l'égard desquels pourrait peser un « soupçon raisonnable » de participation à des infractions terroristes ou de criminalité grave (216). Un tel « ciblage » implique l'application de critères d'évaluation abstraits ou, pour utiliser une expression qui figure dans la recommandation de 2021 sur le profilage, de « profils » (217) au moyen desquels « filtrer »

les données PNR afin de repérer les passagers qui y répondent et qui pourraient, dès lors, devoir être soumis à un contrôle plus approfondi. En revanche, la directive PNR n'autorise pas un profilage individuel de tous les passagers aériens dont les données sont analysées, par exemple en associant à chacun d'eux une catégorie de risque sur une échelle prédéfinie, sous peine de méconnaître tant l'article 6, paragraphe 4, de cette directive que les limites imposées par la Cour au traitement automatisé des données PNR dans l'avis 1/15.

225. Conformément à l'article 6, paragraphe 4, deuxième phrase, les critères préétablis visés à l'article 6, paragraphe 3, sous b), de la directive PNR doivent, en outre, être « spécifiques » (218), à savoir adaptés à la finalité poursuivie et pertinents par rapport à celle-ci, ainsi que « proportionnés » (219), c'est-à-dire n'excédant pas les limites de cette finalité. Pour satisfaire à ces exigences, et notamment « pour veiller à ce que le traitement de données PNR reste limité à ce qui est nécessaire », le considérant 7 de la directive PNR, ainsi que je l'ai déjà souligné, énonce que « la création et l'application de critères d'évaluation devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente ».

226. Il ressort, enfin, tant du préambule et des dispositions de la directive PNR que des exigences énoncées par la Cour dans l'avis 1/15, que les critères préétablis visés à l'article 6, paragraphe 3, sous b), de la directive PNR doivent également être « fiables » (220), ce qui signifie, d'une part, qu'ils doivent être conçus pour minimiser le risque d'erreurs (221) et, d'autre part, qu'ils doivent être « actuels » (222). À cet égard, l'article 6, paragraphe 4, troisième phrase, de la directive PNR impose aux États membres de veiller 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 » (223). Pour assurer la fiabilité de ces critères et limiter autant que possible des résultats faux positifs, il est encore nécessaire, ainsi que l'a reconnu la Commission en répondant à une question écrite posée par la Cour, que ceux-ci soient conçus de manière à tenir compte tant des éléments à charge que des éléments à décharge.

227. En deuxième lieu, la directive PNR interdit expressément le profilage discriminatoire. Ainsi, l'article 6, paragraphe 4, première phrase, de cette directive prévoit que l'évaluation préalable au regard de critères préétablis au titre du paragraphe 3, point b), de cet article « est réalisée de façon non discriminatoire ». À cet égard, il convient de préciser que, si la troisième phrase de cet article 6, paragraphe 4, énonce que 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 », l'interdiction générale de profilage discriminatoire doit s'entendre comme recouvrant tous les motifs de discrimination mentionnés à l'article 21 de la Charte, même ceux qui ne sont pas expressément mentionnés (224).

228. En troisième lieu, il ressort tant du libellé de l'article 6, paragraphe 3, sous b), de la directive PNR que du système de garanties qui entoure le traitement automatisé des données PNR prévu par la directive PNR que le fonctionnement des algorithmes utilisés dans le cadre de l'analyse prévue à cette disposition doit être transparent et le résultat de leur application traçable. Cette exigence de transparence n'implique évidemment pas que les « profils » utilisés doivent être rendus publics. En revanche, elle requiert que soit assuré le caractère identifiable de la prise de décision algorithmique. En effet, d'une part, l'exigence selon laquelle les critères à l'égard desquels doit être effectuée cette analyse doivent être « préétablis » exclut que ceux-ci puissent être modifiés sans intervention humaine et s'oppose, dès lors, à l'utilisation de technologies d'intelligence artificielle dites de « machine learning » (225), qui, tout en pouvant présenter un plus haut degré de précision, sont difficiles à interpréter, même pour les opérateurs ayant procédé au traitement automatisé (226). D'autre part, la garantie énoncée à l'article 6, paragraphes 5 et 6, de la directive PNR, selon laquelle

toute concordance positive obtenue à la suite du traitement automatisé des données PNR effectué au titre du paragraphe 2, point a), de cet article est réexaminée individuellement par des moyens non automatisés, pour être effective, requiert – s'agissant de l'analyse visée à l'article 6, paragraphe 3, sous b), de la directive PNR – qu'il soit possible de comprendre la raison pour laquelle le programme est arrivé à une telle concordance, ce qui ne peut être assuré notamment lorsque sont utilisés des systèmes d'autoapprentissage. Il en va de même du contrôle de la licéité de cette analyse, y inclus ce qui concerne le caractère non discriminatoire des résultats obtenus, dont sont investis le délégué à la protection des données et l'autorité nationale de contrôle, au titre, respectivement, de l'article 6, paragraphe 7, de la directive PNR, et de l'article 15, paragraphe 3, sous b), de cette directive. La transparence du fonctionnement des algorithmes utilisés est également une condition nécessaire afin de permettre aux intéressés d'exercer leurs droits de réclamation ainsi que leur droit à un recours juridictionnel effectif.

– *Sur les garanties entourant le traitement automatisé des données PNR*

229. J'ai déjà eu l'occasion de mentionner certaines des garanties qui accompagnent le traitement automatisé des données PNR dans le cadre de l'évaluation préalable au titre de l'article 6, paragraphe 2, sous a), de la directive PNR, et qui répondent aux exigences énoncées par la Cour dans l'avis 1/15, à savoir, l'interdiction de traitement sur la base de critères préétablis discriminatoires (article 6, paragraphe 4, première et quatrième phrase, de la directive PNR ; avis 1/15, point 172), l'actualisation à intervalles réguliers des critères préétablis au regard desquels doit être effectuée l'évaluation préalable visée à l'article 6, paragraphe 3, sous b), de cette directive (article 6, paragraphe 4, troisième phrase, de la directive PNR ; avis 1/15, point 174), le réexamen par des moyens non automatisés de toute concordance positive obtenue à la suite du traitement automatisé des données PNR (article 6, paragraphes 5 et 6, de la directive PNR ; avis 1/15, point 173) et le contrôle de la licéité de ce traitement par le délégué à la protection des données et par l'autorité nationale de contrôle (article 6, paragraphe 7, et article 15, paragraphe 3, sous b), de la directive PNR). Dans ce contexte, il est primordial que le contrôle effectué par une autorité indépendante, telle que l'autorité visée à l'article 15 de directive PNR, d'une part, puisse porter sur tout aspect inhérent au traitement automatisé des données PNR, y inclus l'identification des bases de données utilisées aux fins de la confrontation au sens de l'article 6, paragraphe 3, sous a), de cette directive et l'élaboration des critères préétablis appliqués aux fins de l'analyse au titre de l'article 6, paragraphe 3, sous b), de ladite directive et, d'autre part, puisse être exercé tant ex ante que ex post.

230. Il importe de souligner que les garanties susvisées doivent se considérer comme étant applicables de manière transversale aux deux types d'analyses visées à l'article 6, paragraphe 3, de la directive PNR, et cela malgré les termes dans lesquels elles sont formulées. Ainsi, si l'article 6, paragraphe 4, première phrase, de cette directive rappelle l'exigence du respect du principe de non-discrimination seulement par rapport à l'évaluation préalable réalisée au regard de critères préétablies, cette exigence s'impose dans toute étape du processus de traitement des données PNR et donc également lorsque ceux-ci sont confrontés aux bases de données pertinentes dans le cadre de l'évaluation préalable au sens de l'article 6, paragraphe 3, sous a), de cette directive. Il en va de même de l'exigence selon laquelle les critères préétablis utilisés dans le cadre de l'analyse visée à l'article 6, paragraphe 3, sous b), de la directive PNR doivent être fiables et actualisés, qui doit s'entendre comme visant également les données contenues dans les bases de données utilisées aux fins de la confrontation prévue à l'article 6, paragraphe 3, sous a), de cette directive. À cet égard, je relève, plus généralement, que toutes les garanties applicables aux traitements automatisés de données à caractère personnel prévus par la directive police sont également applicables dans le cadre de la directive PNR, les analyses automatisées réalisées dans le cadre de cette directive devant être considérées comme entrant dans le champ d'application de la directive police.

231. Aux garanties énumérées au point 229 ci-dessus s'ajoute celle prévue à l'article 7, paragraphe 6, de la directive PNR qui vient compléter, d'une part, l'interdiction de fonder tout processus décisionnel exclusivement sur les résultats du traitement automatisé des données PNR et, d'autre part, l'interdiction de discrimination dans le traitement et l'utilisation de ces données. Ainsi, cette disposition prévoit que « les autorités compétentes ne peuvent prendre aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR » et que ces décisions « ne peuvent pas être fondées sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle ». À l'instar de ce que j'ai indiqué au point 227 des présentes conclusions s'agissant de l'article 6, paragraphe 4, quatrième phrase, de la directive PNR, il convient de compléter ce catalogue de motifs de discrimination en y ajoutant ceux qui figurent à l'article 21 de la Charte et qui ne sont pas expressément mentionnés.

232. S'agissant de la sécurité des données PNR, l'article 6, paragraphe 8, de la directive PNR prévoit que le stockage, le traitement et l'analyse de ces données par les UIP sont effectués exclusivement dans un ou des endroits sécurisés situés sur le territoire des États membres.

– *Conclusion sur la sixième question préjudicielle*

233. Compte tenu de l'ensemble des considérations qui précèdent et sous réserve des interprétations proposées notamment aux points 213, 219, 220, 222, 227, 228, 230 et 231 des présentes conclusions, je suis de l'avis que le traitement automatisé des données PNR dans le cadre de l'évaluation préalable visée à l'article 6, paragraphe 2, sous a), de la directive PNR respecte les exigences de clarté et de précision, et est limité au strict nécessaire.

v) *Sur la conservation des données PNR (huitième question préjudicielle)*

234. Par sa huitième question préjudicielle, la juridiction de renvoi demande à la Cour si l'article 12 de la directive PNR, lu en combinaison avec les articles 7, 8, et l'article 52, paragraphe 1, de la Charte doit être interprété en ce sens qu'il s'oppose à une législation nationale qui prévoit un délai général de conservation des données PNR de cinq ans, sans distinguer si les passagers concernés se révèlent, dans le cadre de l'évaluation préalable, susceptibles ou non de présenter un risque pour la sécurité publique.

235. L'article 12, paragraphe 1, de la directive PNR prévoit que les données PNR sont conservées dans une base de données « pendant une période de cinq ans suivant leur transfert à l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol ». Conformément au paragraphe 2 de cet article, à l'expiration d'un « délai initial de conservation » (227) d'une durée de six mois, les données PNR sont dépersonnalisées par le masquage de certaines données qui pourraient servir à identifier directement la personne concernée. Aux termes du paragraphe 3 dudit article, à l'expiration de cette période de six mois, la communication de l'intégralité des données PNR, incluant les éléments masqués, n'est autorisée que lorsqu'il existe des « motifs raisonnables » de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b), de la directive PNR et lorsqu'elle a été approuvée par une autorité judiciaire ou autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies. Enfin, le paragraphe 4, du même article prévoit que, à l'issu de la période de cinq ans visée au paragraphe 1, les données PNR sont effacés de manière définitive.

236. Il ressort de ce qui précède que la directive PNR établit elle-même le régime de conservation des données PNR, y inclus la durée de cette conservation, en la fixant à cinq ans (228), de sorte que

les États membres n'ont en principe aucune marge discrétionnaire à cet égard, ce qui a par ailleurs été confirmé par la Commission. Dans ces circonstances, ainsi que j'ai déjà eu l'occasion de l'observer, la huitième question préjudicielle, bien que formulée comme une question d'interprétation, invite en réalité la Cour à se prononcer sur la compatibilité dudit régime avec la Charte.

237. Il est un principe général en matière de protection des données à caractère personnel que ces données ne doivent être conservées, sous une forme permettant l'identification, directe ou indirecte, des personnes concernées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées (229). Par ailleurs, il est de jurisprudence constante qu'une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi (230).

238. Dans l'avis 1/15, la Cour a considéré, s'agissant des données collectées à l'entrée du Canada, que le rapport nécessaire entre les données PNR et l'objectif poursuivi par le projet d'accord PNR Canada-UE était établi pour tous les passagers aériens aussi longtemps qu'ils se trouvaient sur le territoire de ce pays tiers (231). S'agissant, en revanche, des passagers aériens ayant quitté le Canada et pour lesquels un risque en matière de terrorisme ou de criminalité transnationale grave n'avait pas été identifié à leur arrivée dans ce pays tiers et jusqu'à leur départ de celui-ci, la Cour a considéré qu'un tel rapport, ne serait-ce qu'indirect, justifiant la conservation de leurs données PNR, n'apparaissait pas exister (232). Elle a néanmoins retenu qu'une telle conservation pouvait être admissible « [d]ans la mesure où, toutefois, sont identifiés, dans des cas particuliers, des éléments objectifs permettant de considérer que certains passagers aériens pourraient, même après leur départ du Canada, présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave » (233).

239. Transposés dans le contexte de la directive PNR, les principes établis par la Cour dans l'avis 1/15 impliqueraient que les données PNR des vols extra-UE recueillis à l'entrée de l'Union ainsi que les données PNR des vols intra-UE recueillies à l'entrée de l'État membre concerné ne peuvent être conservées, après leur analyse préalable au sens de l'article 6, paragraphe 2, sous a), de la directive PNR, qu'aussi longtemps que les passagers concernés demeurent sur le territoire de l'Union ou de celui de cet État membre. S'agissant des données PNR des vols extra-UE recueillies à la sortie de l'Union et des données PNR des vols intra-UE recueillies à la sortie de l'État membre concerné, celles-ci ne pourraient, en principe, être conservées, après ladite évaluation préalable, que dans le cas des passagers pour lesquels des éléments objectifs permettraient de révéler l'existence d'un risque en termes de lutte contre le terrorisme et la criminalité grave (234).

240. Les gouvernements et les institutions ayant présenté des observations devant la Cour s'opposent de manière générale à une transposition dans le cadre de la présente affaire des principes établis dans l'avis 1/15 en matière de conservation des données PNR. À cet égard, il n'est, certes, pas exclu que le recours par la Cour à un critère lié au séjour de la personne concernée sur le territoire du Canada ait pu être influencé par la circonstance qu'elle était confrontée à une conservation de données personnelles sur le territoire d'un pays tiers. Il est tout aussi possible que l'application d'un tel critère dans le contexte de la directive PNR puisse concrètement se traduire par une ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel potentiellement plus importante pour certaines catégories de personnes, notamment celles ayant leur résidence permanente dans l'Union et qui se déplacent à l'intérieur de celle-ci ou qui rentrent après un séjour à l'étranger. Il est enfin vrai que ledit critère pourrait s'avérer difficile à mettre en œuvre dans la pratique, à tout le moins pour les vols intra-EU, ainsi que certains États membres et le Conseil l'ont souligné.

241. Il n'en demeure pas moins que, même à vouloir écarter le critère auquel a eu recours la Cour dans l'avis 1/15, une conservation de l'ensemble des données PNR de tous les passagers aériens, indépendamment du résultat de l'évaluation préalable visée à l'article 6, paragraphe 2, sous a), de la directive PNR et sans qu'aucune distinction soit faite en fonction du risque en matière de terrorisme ou de criminalité grave sur la base de critères objectifs et vérifiables, va à l'encontre de la jurisprudence constante de la Cour rappelée au point 237 des présentes conclusions, à laquelle la Cour a entendu donner application dans ledit avis. Or, les considérations exposées aux points 201 à 203 des présentes conclusions dans le cadre de l'examen de la quatrième question préjudicielle, si elles permettent, à mes yeux, de justifier le transfert généralisé et indifférencié des données PNR, ainsi que leur traitement automatique dans le cadre de l'évaluation préalable prévue à l'article 6, paragraphe 2, sous a), de la directive PNR, elles ne permettent pas, à mon sens, à elle seules de justifier une rétention généralisée et indifférenciée de ces données, même après une telle évaluation.

242. Je relève, par ailleurs, que le même délai de conservation de cinq ans est appliqué que ce soit pour la lutte contre le terrorisme ou pour la lutte contre la criminalité grave et, dans le cadre de cette dernière finalité, pour toutes les infractions visées à l'annexe II sans exception. Or, ainsi que cela ressort des considérations développées au point 121 des présentes conclusions, cette liste est particulièrement étendue et couvre des infractions de typologie et gravité différentes. À cet égard, il importe de relever que la justification avancée par pratiquement tous les États membres et les institutions ayant présenté des observations dans la présente procédure, tenant à la durée et à la complexité des enquêtes, n'est concrètement évoquée que pour les infractions terroristes et pour certaines infractions ayant un caractère éminemment transnational, comme le trafic d'êtres humains ou le trafic de stupéfiants, ainsi que, plus généralement, pour certaines formes de criminalité organisée. Je rappelle, par ailleurs, que, dans l'avis 1/15, une justification similaire n'a été acceptée par la Cour qu'en ce qui concerne la conservation des données PNR des passagers aériens pour lesquels il existe un risque objectif en termes de lutte contre le terrorisme ou la criminalité transnationale grave, pour lesquels une rétention des données de cinq ans a été considérée comme n'excédant pas les limites de ce qui est strictement nécessaire (235). En revanche, cette justification a été considérée comme ne pouvant pas autoriser « un stockage continu des données PNR de l'ensemble des passagers aériens [...] aux fins d'un accès éventuel auxdites données, indépendamment d'un lien quelconque avec la lutte contre le terrorisme et la criminalité transnationale grave » (236).

243. Il est, certes, vrai, comme le soulignent le Conseil, le Parlement et la Commission, ainsi que tous gouvernements ayant présenté des observations sur la huitième question préjudicielle, que la directive PNR prévoit des garanties spécifiques tant en ce qui concerne la conservation des données PNR, qui sont pour partie masquées après un délai initial de six mois, qu'en ce qui concerne leur utilisation pendant la période de rétention, laquelle est soumise à des conditions strictes. Cependant, premièrement, je relève, d'une part, que le projet d'accord PNR Canada-UE prévoyait aussi un système de dépersonnalisation des données PNR par masquage (237) et, d'autre part, que, si une telle dépersonnalisation, ainsi que le souligne notamment le comité consultatif de la convention 108 (238), peut atténuer les risques induits par une période de conservation prolongée des données, comme un accès abusif, les données masquées permettent néanmoins encore d'identifier les personnes et restent à ce titre des données à caractère personnel, dont la conservation doit aussi être limitée dans le temps pour prévenir une surveillance permanente généralisée. À cet égard, je relève qu'un délai de conservation de cinq ans a pour conséquence qu'un nombre important de passagers, notamment ceux qui se déplacent à l'intérieur de l'Union, pourront se retrouver fichés de manière quasi permanente. Deuxièmement, s'agissant des restrictions à l'utilisation des données, j'observe que la conservation de données à caractère personnel et l'accès à de telles données sont des ingérences distinctes dans les droits fondamentaux au respect de la vie privée et à la protection des données personnelles, qui nécessitent d'être justifiées de manière autonome. Si l'existence de

garanties strictes en matière d'accès aux données conservées permet d'apprécier globalement l'impact d'une mesure de surveillance sur lesdits droits fondamentaux, il n'en demeure pas moins qu'elles ne permettent pas d'éliminer les ingérences liées à une conservation généralisée prolongée.

244. Quant à l'argument de la Commission, selon lequel il est nécessaire de conserver les données PNR de tous les passagers aériens pour permettre aux UIP d'accomplir la tâche, visée à l'article 6, paragraphe 2, sous c), de la directive PNR, de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées au titre du paragraphe 3,sous b), de cet article, je relève que, tout en admettant que la précision de ces critères dépende en partie de leur confrontation à des comportements « normaux », ainsi que l'affirme la Commission, il n'en reste pas moins que leur élaboration doit être faite sur la base des comportements « criminels ». Un tel argument qui, au demeurant, n'est avancé que par un nombre limité d'États membres ne saurait, à mon sens, revêtir l'importance décisive que semble lui prêter la Commission et justifier, à lui seul, une conservation généralisée des données PNR de tous les passagers aériens, sous une forme non anonyme.

245. Compte tenu des considérations qui précèdent, afin d'assurer une interprétation de l'article 12, paragraphe 1, de la directive PNR qui soit conforme aux articles 7, 8, et l'article 52, paragraphe 1, de la Charte, il convient, à mon sens, d'interpréter cette disposition en ce sens que la conservation des données PNR fournies par les transporteurs aériens à l'UIP 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 n'est permise, après que l'évaluation préalable au titre de l'article 6, paragraphe 2, sous a), de cette directive a été effectuée, que dans la mesure où il est établi, sur la base de critères objectifs, un rapport entre ces données et la lutte contre le terrorisme ou la criminalité grave. Une conservation généralisée et indifférenciée des données PNR sous une forme non anonymisée ne saurait se justifier, par analogie à ce que la Cour a affirmé dans cette même jurisprudence, que face à une menace grave pour la sécurité des États membres qui s'avère réelle et actuelle ou prévisible, liée, par exemple, à des activités de terrorisme, et à la condition que la durée de cette conservation soit limitée au strict nécessaire.

246. La délimitation de la mesure de conservation prévue à l'article 12, paragraphe 1, de la directive PNR peut, par exemple, se fonder sur une évaluation des risques ou sur l'expérience acquise par les autorités nationales compétentes, permettant de viser certaines liaisons aériennes, des schémas de voyage définis, des agences par l'intermédiaire desquelles les réservations sont faites, ou, encore, des catégories de personnes ou des zones géographiques données, identifiées sur la base d'éléments objectifs et non discriminatoires, à l'instar de ce qui a été jugé par la Cour dans sa jurisprudence en matière de conservation des métadonnées des communications électroniques (239). Par ailleurs, par analogie avec l'avis 1/15, le rapport nécessaire entre les données PNR et l'objectif poursuivi par la directive PNR doit se considérer comme étant établi aussi longtemps que les passagers aériens se trouvent dans l'Union (ou dans l'État membre concerné) ou en partance de celle-ci. Il en va de même pour les données des passagers ayant donné lieu à une concordance positive vérifiée.

247. Pour conclure sur la huitième question préjudicielle, je souhaite consacrer quelques réflexions sur les règles régissant l'accès aux données PNR et leur utilisation après que l'évaluation préalable visée à l'article 6, paragraphe 2, sous a), de la directive PNR a été réalisée et avant leur dépersonnalisation à l'expiration de la période initiale de conservation de six mois prévue à l'article 12, paragraphe 2, de la directive PNR.

248. Il ressort d'une lecture combiné de l'article 6, paragraphe 2, sous b), et de l'article 12, paragraphe 3, de la directive PNR que, pendant cette période initiale, des données PNR non dépersonnalisées ou le résultat de leur traitement peuvent être communiqués aux autorités compétentes conformément à la première de ces dispositions, sans que soient respectées les

conditions fixées aux points a) et b) de la seconde desdites dispositions (240). L'article 6, paragraphe 2, sous b), de la directive PNR se borne en effet à prévoir que les demandes des autorités compétentes en vue d'un tel traitement et d'une telle communication doivent être « dûment motivées » et « fondées sur des motifs suffisants ».

249. Selon une jurisprudence constante, rappelée par la Cour dans l'avis 1/15, une réglementation de l'Union ne saurait se limiter à exiger que l'accès par une autorité à des données à caractère personnel légitimement conservées réponde à l'une des finalités de cette réglementation, mais doit également prévoir les conditions matérielles et procédurales régissant cette utilisation (241), afin, notamment, de protéger lesdites données contre les risques d'abus (242). Dans cet avis, la Cour a jugé que l'utilisation des données PNR après leur vérification à l'arrivée des passagers aériens au Canada et pendant leur séjour dans ce pays devait se fonder sur des circonstances nouvelles justifiant cette utilisation (243), en précisant que « lorsqu'il existe des éléments objectifs permettant de considérer que les données PNR d'un ou de plusieurs passagers aériens pourraient apporter une contribution effective à l'objectif de lutte contre les infractions terroristes et la criminalité transnationale grave, l'utilisation de ces données n'apparaît pas dépasser les limites du strict nécessaire » (244). Renvoyant par analogie au point 120 de l'arrêt Tele2 Sverige, la Cour a jugé que, afin de garantir, en pratique, le plein respect de ces conditions, « il est essentiel que l'utilisation pendant le séjour des passagers aériens au Canada des données PNR conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonnée à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée des autorités compétentes, présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales » (245). La Cour a, dès lors, soumis la possibilité d'une utilisation des données PNR conservées après leur vérification à l'occasion du voyage aérien à une double condition, à la fois matérielle – à savoir l'existence de motifs objectifs justifiant une telle utilisation – et procédurale – à savoir le contrôle de la part d'une juridiction ou d'une autorité administrative indépendante. L'interprétation retenue par la Cour, loin d'être « contextuelle », constitue l'application en matière de données PNR de la jurisprudence issue notamment des arrêts Digital Rights et Tele2 Sverige.

250. Or, le régime instauré par la directive PNR au cours des six premiers mois de conservation des données PNR, qui autorise, après l'évaluation préalable visée à l'article 6, paragraphe 2, sous a), de cette directive, la communication et le traitement, potentiellement répétés, des données PNR en l'absence de garanties procédurales adéquates et de règles matérielles suffisamment claires et précises définissant l'objet et les modalités de ces différentes ingérences ne respecte pas les exigences énoncées par la Cour dans l'avis 1/15. Il n'apparaît pas répondre non plus à l'exigence d'une utilisation des données PNR qui soit limitée au strict nécessaire.

251. Je propose dès lors à la Cour d'interpréter l'article 6, paragraphe 2, sous b), de la directive PNR de manière à ce que les traitements de données au titre de cette disposition qui interviennent au cours de la période initiale de six mois prévue à l'article 12, paragraphe 2, de cette directive respectent les exigences fixées par la Cour dans l'avis 1/15.

252. S'agissant de la première condition, d'ordre matériel, à laquelle la Cour a subordonné l'utilisation ultérieure des données PNR, je suis de l'avis que les notions de « motifs raisonnables » au sens de l'article 12, paragraphe 3, sous a), de la directive PNR et de « motifs suffisants » aux termes de l'article 6, paragraphe 2, sous b), de cette directive peuvent sans difficulté être interprétées en ce sens que les demandes de la part des autorités compétentes, visées à ces dispositions, doivent faire état d'« éléments objectifs permettant de considérer que les données PNR d'un ou de plusieurs passagers aériens pourraient apporter une contribution effective à l'objectif de lutte contre les infractions terroristes et la criminalité [...] grave » (246).

253. S'agissant de la seconde condition, d'ordre procédurale, il y a, à mon sens, lieu d'interpréter l'article 6, paragraphe 2, sous b), de la directive PNR, lu en combinaison avec l'article 12, paragraphe 3, de celle-ci et à la lumière des articles 7, 8, et l'article 52, paragraphe 1, de la Charte, en ce sens que l'exigence d'approbation préalable de la part d'une autorité judiciaire ou d'une autorité administrative indépendante prévue à l'article 12, paragraphe 3, sous b), de cette directive s'applique à tout traitement des données PNR effectué en application dudit article 6, paragraphe 2, sous b).

4. *Conclusions sur les deuxième, troisième, quatrième, sixième et huitième questions préjudicielles*

254. Sur la base de l'ensemble des considérations qui précèdent, je suggère à la Cour d'invalider le point 12 de l'annexe I dans la mesure où il inclut les « remarques générales » parmi les catégories de données PNR que les transporteurs aériens sont tenus de transmettre, conformément à l'article 8 de la directive PNR, aux UIP et de déclarer que l'examen des deuxième, troisième, quatrième, sixième et huitième questions préjudicielles n'a pas révélé d'autres éléments de nature à affecter la validité de cette directive, sous réserve des interprétations des dispositions de celle-ci proposées aux points 153, 160, 161 à 164, 219, 228, 239 et 251 des présentes conclusions.

255. À la lumière de la réponse que je suggère de donner aux questions préjudicielles portant sur la validité de la directive PNR, la demande avancée notamment par le Conseil, visant au maintien des effets de la directive PNR dans le cas où la Cour déciderait d'invalider totalement ou partiellement la directive PNR dans son ensemble, ne saurait, abstraction faite de toute autre considération, être accueillie.

C. **Sur la cinquième question préjudicielle**

256. Par sa cinquième question préjudicielle, la juridiction de renvoi demande en substance à la Cour si l'article 6 de la directive PNR, lu en combinaison avec les articles 7, 8, et l'article 52, paragraphe 1, de la Charte doit être interprété en ce sens qu'il s'oppose à une législation nationale qui admet comme finalité du traitement des données PNR « le suivi de certaines activités des services de renseignement et de sécurité ». Il ressort de la décision de renvoi que ces activités sont celles menées par la sûreté de l'État et le service général du renseignement et de la sécurité dans le cadre de leur mission relative à la protection de la sécurité nationale.

257. Ainsi que je l'ai indiqué aux points 113 et 114 des présentes conclusions, la limitation des finalités du traitement de données à caractère personnel est une garantie essentielle à respecter afin que les ingérences dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte n'aillent pas au-delà de ce qui est nécessaire au sens de la jurisprudence de la Cour. J'ai également déjà précisé que, s'agissant des ingérences dans ces droits fondamentaux prévues par la directive PNR, il incombait au législateur de l'Union, afin de respecter les principes de légalité et de proportionnalité inscrits notamment à l'article 52, paragraphe 1, de la Charte, de prévoir des règles claires et précises régissant la portée et l'application des mesures comportant de telles ingérences.

258. Or, l'article 1, paragraphe 2, de la directive PNR précise que les données PNR recueillies conformément à celle-ci « ne peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière, comme prévu à l'article 6, paragraphe 2, sous a), b) et c) de cette directive ». Conformément à cette disposition, les UIP ne traitent les données PNR que dans le but de réaliser une évaluation préalable des passagers aériens [article 6, paragraphe 2, sous a)], de répondre aux demandes ponctuelles des autorités compétentes [article 6, paragraphe 2, sous b)] et de mettre à jour

ou définir de nouveaux critères à utiliser pour les évaluations effectuées au titre du paragraphe 3, sous b), dudit article 6 [article 6, paragraphe 2, sous a)]. Dans les trois cas, sont expressément rappelés les objectifs indiqués à l'article 1, paragraphe 2, de la directive PNR en matière de lutte contre le terrorisme et la criminalité grave.

259. Par ailleurs, l'article 7, paragraphe 4, de cette directive précise que non seulement le traitement des données PNR prévu à l'article 6 de celle-ci, mais également le traitement ultérieur de ces données et du résultat de ce traitement par les autorités compétentes des États membres doivent être limités « aux seules fins spécifiques de la prévention ou de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes ou des poursuites en la matière ».

260. Le caractère exhaustif de la détermination des objectifs poursuivis par la directive PNR ressort clairement du libellé de son article 1, paragraphe 2, et est corroborée, outre par son article 6, paragraphe 2, et son article 7, paragraphe 4, déjà mentionnés, par plusieurs articles et considérants de cette directive qui rattachent systématiquement chaque étape du processus d'accès, de traitement, de conservation et de partage des données PNR à ces seuls objectifs spécifiques (247).

261. Il ressort tant du libellé de l'article 1, paragraphe 2, de la directive PNR que de son interprétation à la lumière des principes de légalité et de proportionnalité, qui imposent de limiter de manière exhaustive les finalités des mesures comportant des ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, que toute extension des finalités du traitement des données PNR au-delà des objectifs de sécurité expressément mentionnés à cette disposition est contraire à la directive PNR.

262. Cette interdiction d'élargir les objectifs poursuivis par la directive vaut, à mon sens, tout particulièrement pour ce qui concerne les activités des services de sécurité et de renseignement des États membres, y inclus au motif du manque de transparence qui caractérise leur modus operandi. Sur ce point, mes vues concordent avec celles de la Commission, à savoir que ces services ne devraient en règle générale pas avoir un accès direct aux données PNR. Dans ce contexte, je considère déjà en soi critiquable la circonstance que les UIP nationales puissent, comme c'est le cas de l'UIP belge, compter parmi ses membres des fonctionnaires détachés des services de sécurité (248).

263. Sur la base des considérations qui précèdent, il y a, à mon avis, lieu de répondre à la cinquième question préjudicielle que la directive PNR, et notamment son article 1er, paragraphe 2, et son article 6, doit être interprétée en ce sens qu'elle s'oppose à une législation nationale qui admet comme finalité du traitement des données PNR le suivi de certaines activités des services de renseignement et de sécurité, dans la mesure où, dans le cadre d'une telle finalité, l'UIP nationale serait amenée à traiter lesdites données et/ou à transmettre celles-ci ou le résultat de leur traitement auxdits services à des fins autres que celles exhaustivement indiquées à l'article 1, paragraphe 2, de cette directive, ce qui incombe au juge national de vérifier.

D. **Sur la septième question préjudicielle**

264. Par sa septième question, la juridiction de renvoi demande, en substance à la Cour, si l'article 12, paragraphe 3, sous b), de la directive PNR doit être interprété en ce sens que l'UIP constitue une « autorité nationale compétente » au sens de cette disposition, pouvant autoriser la communication de l'intégralité des données PNR à l'expiration de la période initiale de six mois suivant le transfert de ces données.

265. Je rappelle que l'article 12, paragraphe 2, de la directive PNR prévoit que, à l'expiration d'un délai de six mois, les données PNR sont dépersonnalisées par le masquage de certains éléments qui pourraient servir à identifier directement le passager auquel elles se rapportent. Après ce délai, la communication de l'intégralité desdites données n'est autorisée que dans les conditions prévues au paragraphe 3 dudit article 12, et, notamment, lorsque cette communication a été préalablement approuvée par une « autorité judiciaire » [article 12, paragraphe 3, sous b), i)] ou une « autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post » [article 12, paragraphe 3, sous b), ii)].

266. La plupart des gouvernements qui ont présenté leurs observations écrites dans la présente procédure ne se sont pas prononcés sur la septième question préjudicielle. Le gouvernement tchèque considère, à l'instar de la Commission, que l'article 12, paragraphe 3, de la directive PNR ne saurait être interprété en ce sens que l'UIP peut constituer une « autorité nationale compétente ». En revanche, les gouvernements belge (249), irlandais, espagnol, français et chypriote s'opposent à une telle interprétation. Ils considèrent, en substance, qu'aucune disposition de la directive PNR ou du droit de l'Union ne fait obstacle à la désignation de l'UIP parmi les autorités nationales compétentes au sens de l'article 12, paragraphe 2, sous b), ii), de ladite directive et que l'UIP, par nature, serait une autorité suffisamment indépendante pour pouvoir procéder à l'autorisation du traitement des données PNR.

267. Pour ma part, je relève, premièrement, qu'il ressort du libellé de l'article 12, paragraphe 3, sous b), de la directive PNR et, notamment, de l'utilisation de la conjonction « ou », reliant les deux cas de figure aux points i) et ii) de cette disposition, que le législateur de l'Union a entendu mettre sur le même plan le contrôle exercé par l'autorité nationale visée au point ii) et celui opéré par l'autorité judiciaire visée au point i). Il s'ensuit que ladite autorité nationale doit présenter un niveau d'indépendance et d'impartialité tel que le contrôle qu'elle exerce puisse être considéré comme une alternative comparable au contrôle qui peut être effectué par une autorité judiciaire (250).

268. Deuxièmement, il ressort des travaux préparatoires de la directive PNR que le législateur de l'Union, d'une part, n'a pas retenu la proposition de la Commission de charger le responsable de l'UIP de la tâche d'autoriser la communication de l'intégralité des données PNR (251), et, d'autre part, a rallongé, en le portant à six mois, le délai initial de rétention de ces données proposé par cette institution, qui s'élevait à 30 jour. C'est dans ce contexte, caractérisé par la recherche d'un équilibre entre la durée de la période de rétention avant la dépersonnalisation des données PNR et les conditions auxquelles est soumis leur démasquage à la fin de cette période que se situe la décision du législateur de l'Union de soumettre l'accès intégrale aux données PNR à des conditions procédurales plus strictes que celles initialement prévues par la Commission et de charger une autorité indépendante de la tâche de vérifier que les conditions de communication sont satisfaites.

269. Troisièmement, ainsi que l'a, à juste titre, observé la Commission, il ressort de l'économie de la directive PNR que la raison d'être de la procédure d'approbation prévue à l'article 12, paragraphe 3, de la directive PNR réside dans l'attribution à une entité tierce impartiale de la tâche de procéder, dans chaque cas d'espèce, à une mise en balance des droits des personnes concernées avec la finalité répressive poursuivie par cette directive.

270. Quatrièmement, il découle de la jurisprudence de la Cour qu'une entité chargée d'effectuer le contrôle préalable requis afin d'autoriser l'accès des autorités nationales compétentes à des données à caractère personnel légitimement conservées doit disposer de toutes les attributions et présenter toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. La Cour a également précisé que cette entité doit jouir d'un statut lui permettant d'agir lors

de l'exercice de ses missions de manière objective et impartiale, et doit être, à cet effet, à l'abri de toute influence extérieure (252). En particulier, eu égard à l'exigence d'indépendance requise, surtout dans le domaine pénal, l'autorité chargée du contrôle préalable doit avoir la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte qu'elle ne doit pas être impliquée dans la conduite d'une enquête pénale et doit maintenir une position de neutralité à l'égard des parties à la procédure pénale (253).

271. Or, force est de constater que l'UIP ne présente pas toutes les garanties d'indépendance et d'impartialité auxquelles doit satisfaire l'autorité chargée d'exercer le contrôle préalable prévu à l'article 12, paragraphe 3, de la directive PNR. En effet, les UIP sont directement liées aux autorités compétentes 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. Conformément à l'article 4, paragraphe 1, de la directive PNR, l'UIP est elle-même une telle autorité ou une antenne de celle-ci. Par ailleurs, le paragraphe 3 de cet article prévoit que les membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes. Tel est le cas notamment de l'UIP belge qui, aux termes de l'article 14 de la loi PNR, est composée, notamment, de membres détachés des services de police, de la sûreté de l'État, du service général de renseignement et de sécurité, et de l'administration générale des douanes et accises.

272. Certes, de manière générale, les membres de l'UIP doivent offrir toute garantie d'intégrité, de compétence, de transparence et d'indépendance, et il incombe aux États membres de veiller, le cas échéant, à ce que, compte tenu des liens qui les unissent à leurs corps d'appartenance, ces garanties puissent concrètement être respectées, notamment afin d'éviter que les autorités compétentes dans la structure desquelles ces membres sont originairement insérés aient un accès direct non pas à la banque de données PNR, mais uniquement aux résultats des saisies effectués par les UIP. Il n'en reste pas moins que les membres des UIP qui sont détachés des autorités compétentes au sens de l'article 7, paragraphe 2, de la directive PNR gardent inévitablement un lien avec leurs services d'origine pendant la période de leur détachement, en conservant leur statut même s'ils sont placés sous l'autorité fonctionnelle et hiérarchique du fonctionnaire dirigeant l'UIP.

273. La conclusion selon laquelle l'UIP n'est pas une autorité nationale au sens de l'article 12, paragraphe 3, sous b), ii), de la directive PNR est par ailleurs corroborée par la circonstance que, conformément à cette disposition, le délégué à la protection des données de l'UIP concernée doit être « informé » de la demande de communication et exerce un « examen ex post ». En effet, dans le cas où l'UIP était habilitée, en tant qu'« autre autorité nationale », à approuver une demande de communication au titre de l'article 12, paragraphe 3, de la directive PNR, le délégué à la protection des données, qui est entre autres chargé, conformément à l'article 5, paragraphe 1, de cette directive, de mettre en œuvre les garanties pertinentes entourant le traitement des données PNR, serait informé de la demande d'accès au moment de son introduction et son contrôle interviendrait nécessairement ex ante. (254)

274. À la lumière des considérations qui précèdent, je suggère à la Cour de répondre à la septième question préjudicielle que l'article 12, paragraphe 3, sous b), de la directive PNR doit être interprété en ces sens que l'UIP ne constitue pas une « autre autorité nationale compétente » au sens de cette disposition.

E. **Sur la neuvième question préjudicielle**

275. Par sa neuvième question préjudicielle, la juridiction de renvoi demande en substance à la Cour, d'une part, si la directive API est compatible avec l'article 3, paragraphe 2, TUE et avec l'article 45 de la Charte en ce qu'elle s'appliquerait aux vols à l'intérieur de l'Union et, d'autre part,

si cette directive, lue en combinaison avec l'article 3, paragraphe 2, TUE et avec l'article 45 de la Charte, doit être interprétée en ce sens qu'elle s'oppose à une législation nationale qui, aux fins de lutter contre l'immigration illégale et d'améliorer les contrôles aux frontières, autorise un système de collecte et de traitement des données des passagers qui pourrait impliquer indirectement un rétablissement des contrôle aux frontières intérieures.

276. Il ressort de la décision de renvoi que cette question préjudicielle s'insère dans le cadre de l'examen du second moyen du recours, soulevé par la LDH à titre subsidiaire. Ce moyen, tiré de la violation de l'article 22 de la Constitution belge, lu en combinaison avec l'article 3, paragraphe 2, TUE et avec l'article 45 de la Charte est dirigé contre l'article 3, § 1, l'article 8, § 2, et le chapitre 11, notamment les articles 28 à 31, de la loi PNR. Si le premier de ces articles énonce, en des termes généraux, l'objet de cette loi, en précisant qu'elle « détermine les obligations des transporteurs et des opérateurs de voyage relatives à la transmission des données de passagers à destination du, en provenance du et transitant par le territoire national », l'article 8, § 2, de ladite loi prévoit que, « sous les conditions prévues au chapitre 11 [de celle-ci,] les données des passagers sont également traitées en vue de l'amélioration des contrôles des personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale ». Dans le cadre de cette finalité, conformément à l'article 29, § 1, de la loi PNR, seules les « données des passagers » visées à l'article 9, § 1, point 18, de celle-ci (à savoir les données API mentionnées au point 18 de la directive PNR), concernant trois catégories de passagers, sont transmises aux services de police chargés du contrôle aux frontières et à l'Office des étrangers (Belgique). Il s'agit des « passagers qui envisagent d'entrer ou sont entrés sur le territoire par les frontières extérieures de la Belgique », des « passagers qui envisagent de quitter ou ont quitté le territoire par les frontières extérieures de la Belgique » et des « passagers qui envisagent de passer par, se trouvent dans ou sont passés par une zone internationale de transit située en Belgique » (255). Il ressort de l'article 29, § 3, de la loi PNR que lesdites données sont transmises aux services de police chargés du contrôle aux frontières et à l'Office des étrangers par l'UIP « immédiatement après leur enregistrement dans la banque de données de passagers » et qu'ils sont détruits vingt-quatre heures après leur transmission. Aux termes de cette disposition, passé ce délai, l'Office des étrangers peut également adresser à l'UIP une demande motivée en vue d'obtenir l'accès à ces mêmes données lorsque cela s'avère nécessaire dans le cadre de sa mission légale. Dès lors, le cadre légal dans lequel s'insère la neuvième question préjudicielle sort de celui de la directive PNR, étant donné la finalité poursuivie par le traitement de données visé aux articles 28 et 29 de la loi PNR, pour s'insérer dans celui de la directive API. Par ailleurs, il ressort, notamment, du dossier déposé au greffe de la Cour que le second moyen de la LDH se fonde sur une interprétation des dispositions du chapitre 11 de la loi PNR selon laquelle celles-ci s'applique également en cas de franchissement des frontières intérieures de la Belgique.

277. La première partie de la neuvième question préjudicielle se fonde sur un présupposé erroné et n'appelle à mon sens pas de réponse de la part de la Cour. En effet, il ressort de manière non équivoque de l'article 3, paragraphe 1, de la directive API, lu en combinaison avec l'article 2, sous b) et d), de celle-ci que cette directive ne prévoit l'obligation pour les transporteurs aériens de transmettre les données API aux autorités chargées du contrôle des personnes aux frontières extérieures qu'en ce qui concerne les vols qui acheminent des passagers vers un point de passage autorisé pour le franchissement des frontières extérieures des États membres avec des pays tiers. De même, l'article 6, paragraphe 1, de ladite directive ne prévoit que le traitement des données API relatives à ces vols. Par ailleurs, s'il est vrai que la directive PNR prévoit la possibilité pour les États membres d'étendre l'obligation de transférer les données API recueillies également aux transporteurs aériens qui assurent des vols intra-UE, cette extension doit s'entendre sans préjudicie de la directive API (256). Dans le cadre de la directive PNR, les données API transférées ne seront traitées que dans le cadre des finalités répressives prévues par cette directive. Inversement, le considérant 34 de la directive PNR prévoit que celle-ci est sans préjudice des règles actuelles de

l'Union sur les modalités des contrôles aux frontières ou des règles de l'Union régissant l'entrée sur le territoire de l'Union et la sortie de celui-ci, et l'article 6, paragraphe 9, seconde phrase de cette directive stipule que, lorsque des évaluations au titre du paragraphe 2 de cet article sont réalisées pour des vols intra-UE entre des États membres auxquels s'applique le code frontières Schengen (257), les conséquences de ces évaluations doivent respecter ledit règlement.

278. Reformuler cette partie de la neuvième question préjudicielle, ainsi que le suggère, à titre subsidiaire, la Commission, en ce sens qu'elle vise la compatibilité avec les dispositions du traité et de la Charte non pas de la directive API, mais de la directive PNR, et notamment de son article 2, impliquerait non seulement de modifier l'acte par rapport auquel la juridiction de renvoi a demandé une appréciation en validité, mais signifierait également sortir du cadre légal dans lequel se situe cette question préjudicielle. En effet, ainsi que je l'ai expliqué, les dispositions du chapitre 11 de la loi PNR, contre lesquelles est dirigé le second moyen de recours, transposent la directive API et non pas la directive PNR.

279. Dans l'hypothèse où la Cour procéderait à une telle reformulation, je me borne aux quelques réflexions qui suivent en ce qui concerne notamment la question de savoir si l'évaluation préalable que les États membres sont autorisés à conduire sur les données PNR des passagers des vols intra-UE, conformément à la faculté dont ils disposent au sens de l'article 2 de la directive PNR, peut être considérée comme équivalente à l'exercice des « vérifications aux frontières » au sens de l'article 23, sous a), du code frontières Schengen (258). Premièrement, si l'évaluation préalable des données PNR a lieu non pas « au point de passage frontalier » ou au « moment du franchissement de la frontière », mais avant ce moment, elle est néanmoins effectuée « au motif » du franchissement imminent des frontières. Deuxièmement, conformément à l'article 2 de la directive PNR, les États membres sont autorisés à étendre l'évaluation préalable des données PNR prévue à l'article 6, paragraphe 2, sous a), de la directive PNR aux passagers de tous les vols intra-UE, indépendamment du comportement des personnes concernées et de circonstances établissant un risque d'atteinte à la sécurité publique. Cette évaluation préalable a, en outre, un caractère systématique. Or, ni l'un ni l'autre de ces éléments ne semblent satisfaire aux indices visées à l'article 23, sous a), seconde phrase, ii), iii) et iv), du code frontières Schengen (259). Troisièmement, s'agissant des indices visés au point a), seconde phrase, i) et iii), de cet article, je me demande si l'évaluation préalable au titre de l'article 6, paragraphe 2, sous a), de la directive PNR ne recoupe pas, à tout le moins en partie, la finalité des vérifications aux frontières effectuées en application de l'article 8, paragraphe 2, sous b), et paragraphe 3, sous a), vi) et sous g), iii), du code frontières Schengen, tel que modifié par le règlement 2017/458, et, surtout si elle se distingue clairement, quant à ses modalités, de ces vérifications systématiques (260). À cet égard, je relève que l'article 8, paragraphe 2, sexies et paragraphe 3, i bis), de ce code précisent que lesdites vérifications « peuvent s'effectuer au préalable sur la base des données relatives aux passagers reçues conformément à la directive API ou à d'autres dispositions du droit national ou de l'Union ». Cela étant, il est vrai que la finalité de la directive PNR n'est pas celle de « s'assurer que les personnes *peuvent être autorisées* à entrer sur le territoire de l'État membre ou à le quitter », ou celle « d'empêcher les personnes de se soustraire à ces vérifications », que la Cour a reconnu être les objectifs du « contrôle aux frontières » aux termes du code frontières Schengen (261), cette directive n'ayant qu'une finalité exclusivement répressive. En outre, l'article 23, sous a), seconde phrase, ii), dudit code prévoit explicitement que l'exercice de compétences de police ne peut être considéré comme équivalant à l'exercice de vérifications aux frontières lorsque les contrôles visent, notamment, la lutte contre la criminalité transfrontalière (262). Enfin, la Cour devrait tenir compte également dans son appréciation de la circonstance, soulignée notamment par la Commission, que l'article 2 de la directive PNR n'autorise les États membres qu'à imposer aux transporteurs aériens le transfert des données PNR qu'ils ont recueillies dans le cours normal de leurs activités et ne

prévoit dès lors pas une obligation analogue à celle prévue par la directive API pour le passage des frontières extérieures.

280. S'agissant de la seconde partie de la neuvième question préjudicielle, j'estime, à l'instar de la Commission, qu'elle doit être entendue comme se rapportant au franchissement des frontières intérieures et comme visant à obtenir de la Cour des éclaircissements permettant à la juridiction de renvoi d'apprécier la compatibilité des dispositions du chapitre 11 de la loi PNR avec l'abolition des contrôles aux frontières intérieures des États membres dans l'espace Schengen.

281. À cet égard, compte tenu du peu d'éléments dont la Cour dispose, je me borne à relever que les dispositions du chapitre 11 de la loi PNR ne sauraient être compatibles avec le droit de l'Union et, notamment, avec l'article 67, paragraphe 2, TFUE que si elles sont interprétées en ce sens qu'elles ne visent que le transfert et le traitement des données API des passagers qui franchissent les frontières extérieures de la Belgique avec des pays tiers.

282. Dans la mesure où la Cour déciderait de reformuler la seconde partie de la neuvième question préjudicielle en ce sens qu'elle porte sur l'interprétation de la directive PNR en relation avec les dispositions du chapitre 11 de la loi PNR, je me borne à relever que le traitement des données API prévu aux articles 28 et 29 de cette loi se greffe sur le système mis en place par le législateur belge afin de transposer la directive PNR. Ainsi, premièrement, les données API qui font l'objet de traitement sont celles énumérées au point 12 de l'annexe I de cette directive et non pas uniquement celles contenues dans la liste figurant à l'article 3, paragraphe 2, de la directive API. Deuxièmement, conformément à l'article 29, § 1, de la loi PNR, ces données sont transmises aux services de police chargés du contrôle aux frontières et à l'Office des étrangers par l'UIP – qui est chargé de collecter et de traiter les données PNR dans le cadre des seules finalités poursuivies par la directive PNR –, et non pas, comme prévu par la directive API, directement par les transporteurs aériens. Par ailleurs, cette transmission concerne également les données des passagers qui entendent quitter ou ont quitté le territoire belge et n'a pas pour seuls destinataires les autorités chargées des contrôles aux frontières, mais également l'Office des étrangers, qui est chargé de la gestion de la population immigrée et de la lutte contre l'immigration clandestine. Troisièmement, au titre de l'article 29, § 4, deuxième alinéa, de la loi PNR, l'Office des étrangers semblerait habilité à adresser à l'UIP des demandes d'accès aux données API même après le traitement de ces données à l'occasion du franchissement des frontières des passagers concernés. En ce sens, cet office est de facto assimilé à une autorité compétente au titre de l'article 7 de la directive PNR, tout en en revêtant pas la nature et en ne figurant pas sur la liste de ces autorités qui a été communiquée à la Commission par la Belgique. Or, un tel amalgame entre les systèmes prévus par la directive API et par la directive PNR ne sauraient, à mon sens, être admis en ce qu'il méconnaît le principe de la limitation des finalités inscrit à l'article 1, paragraphe 2, de la directive PNR (263).

283. Sur la base de l'ensemble des considérations qui précèdent, je propose à la Cour de répondre à la neuvième question préjudicielle que l'article 3, paragraphe 1, de la directive API, au titre duquel les États membres prennent les mesures nécessaires afin d'établir l'obligation, pour les transporteurs aériens, de transmettre, à la demande des autorités chargées du contrôle des personnes aux frontières extérieures, avant la fin de l'enregistrement, les renseignements relatifs aux passagers visés au paragraphe 2 de cet article, lu en combinaison avec l'article 2, sous b) et d) de cette directive, ne concerne que les passagers transportés vers un point de passage autorisé pour le franchissement des frontières extérieures des États membres avec des pays tiers. Une législation nationale qui, dans le seul but d'améliorer des contrôles aux frontières et de lutter contre l'immigration illégale, étendrait cette obligation aux données des personnes qui franchissent les frontières intérieures de l'État membre concerné par avion ou par d'autres moyens de transport serait contraire à l'article 67, paragraphe 2, TFUE et à l'article 22 du code frontières Schengen.

F. **Sur la dixième question préjudicielle**

284. Par sa dixième question préjudicielle, la juridiction de renvoi demande en substance à la Cour si, au cas où elle devrait arriver à la conclusion que la loi PNR méconnaît les articles 7 , 8, et l'article 52, paragraphe 1, de la Charte, elle pourrait maintenir provisoirement les effets de cette loi afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisés aux fins visées par la loi PNR.

285. La Cour a répondu à une question ayant la même teneur dans l'arrêt La Quadrature du Net concernant le stockage des métadonnées des communications électroniques, prononcé après l'introduction de la présente demande préjudicielle. Dans cet arrêt, la Cour a, d'abord, rappelé sa jurisprudence selon laquelle il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire. Elle a ensuite rappelé que, dans l'arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen (264), où était en cause la légalité de mesures adoptées en méconnaissance de l'obligation édictée par le droit de l'Union d'effectuer une évaluation préalable des incidences d'un projet sur l'environnement et sur un site protégé, elle a admis qu'une juridiction nationale peut, si le droit interne le permet, exceptionnellement maintenir les effets de telles mesures lorsque ce maintien est justifié par des considérations impérieuses liées à la nécessité d'écarter une menace réelle et grave de rupture de l'approvisionnement en électricité de l'État membre concerné pour le temps strictement nécessaire afin de remédier à cette illégalité. Elle a néanmoins conclu que, contrairement à l'omission d'une obligation procédurale telle que l'évaluation préalable des incidences d'un projet dans le domaine spécifique de la protection de l'environnement, une méconnaissance des droits fondamentaux garantis aux articles 7 et 8 de la Charte ne saurait faire l'objet d'une régularisation par la voie d'une procédure comparable à celle prévue dans l'arrêt susmentionné (265). La même réponse doit à mon sens être donnée à la dixième question préjudicielle dans la présente procédure.

286. Dans la mesure où tant la juridiction de renvoi que le gouvernement belge ainsi que la Commission et le Conseil s'interrogent sur le point de savoir si le droit de l'Union s'oppose à une exploitation, dans le cadre d'une procédure pénale, des renseignements ou des éléments de preuve obtenus en utilisant les données PNR recueillies, traitées et/ou conservées de manière incompatible avec le droit de l'Union, je rappelle que, au point 222 de l'arrêt La Quadrature du Net, la Cour a précisé que, en l'état actuel du droit de l'Union, il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, d'informations et d'éléments de preuve qui ont été obtenus par une conservation de données contraire au droit de l'Union, sous réserve du respect du principe d'équivalence et d'effectivité. S'agissant de ce dernier, la Cour a jugé que ce principe impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits. Ces principes sont également transposables mutatis mutandis aux circonstances de la procédure au principal.

IV. **Conclusion**

287. Sur la base de l'ensemble des considérations qui précèdent, je suggère à la Cour de répondre comme suit aux questions préjudicielles posées par la Cour constitutionnelle (Belgique) :

1) L'article 23 du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), lu en combinaison avec l'article 2, paragraphe 2, sous d), de ce règlement, doit être interprété en ce sens :

– qu'il s'applique à une législation nationale transposant la directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, dans la mesure où cette législation régit les traitements des données PNR effectués par les transporteurs aériens et par d'autres opérateurs économiques, y inclus le transfert de données PNR aux unités d'informations passagers (UIP) visées à l'article 4 de cette directive, prévu à l'article 8 de celle-ci ;

– qu'il ne s'applique pas à une législation nationale transposant la directive 2016/681 dans la mesure où celle-ci régit les traitements de données effectués pour les finalités prévues à l'article 1, paragraphe 2, de cette directive par les autorités nationales compétentes, y incluses les UIP et, le cas échéant, les services de sécurité et de renseignement de l'État membre intéressé ;

– qu'il s'applique à une législation nationale transposant la directive 2004/82/CE du Conseil, du 29 avril 2004, concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, et la directive 2010/65/UE du Parlement européen et du Conseil, du 20 octobre 2010, concernant les formalités applicables aux navires à l'entrée et/ou à la sortie des portes des États membres et abrogeant la directive 2002/6/CE, en vue de l'amélioration des contrôles de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale.

2) Le point 12 de l'annexe I de la directive 2016/681 est invalide dans la mesure où il inclut les « remarques générales » parmi les catégories de données que les transporteurs aériens sont tenus de transmettre aux UIP, conformément à l'article 8 de cette directive.

3) L'examen des deuxième, troisième, quatrième, sixième et huitième question n'a pas révélé d'autres éléments de nature à affecter la validité de la directive 2016/681.

4) Le point 12 de l'annexe I de la directive 2016/681, pour la partie qui n'est pas déclarée invalide, doit être interprété comme couvrant les seuls renseignements concernant les mineurs qui y sont expressément mentionnés et qui ont un rapport direct avec le vol.

5) Le point 18 de l'annexe I de la directive 2016/681 doit être interprété en ce sens qu'il ne couvre que les informations préalables sur les passagers qui sont expressément énumérées à ce point ainsi qu'à l'article 3, paragraphe 2, de la directive 2004/82 et qui ont été recueillies par les transporteurs aériens dans le cours normal de leurs activités.

6) La notion de « bases de données utiles » visée à l'article 6, paragraphe 3, sous a), de la directive 2016/681 doit être interprétée en ce sens qu'elle ne vise que les bases de données nationales gérées par les autorités compétentes au titre de l'article 7, paragraphe 1, de cette directive, ainsi que les bases de données de l'Union et internationales directement exploitées par ces autorités dans le cadre de leur mission. Lesdites bases de données doivent être en rapport direct et étroit avec les finalités de lutte contre le terrorisme et la criminalité grave poursuivies par ladite

directive, ce qui implique qu'elles aient été développées pour ces finalités. Dans le cadre de la transposition dans leur droit national de la directive 2016/681, les États membres sont tenus de publier une liste desdites bases de données et de la tenir à jour.

7) L'article 6, paragraphe 3, sous b), de la directive 2016/681 doit être interprété en ce sens qu'il s'oppose à l'utilisation, dans le cadre du traitement automatisé prévu à cette disposition, de systèmes algorithmiques pouvant aboutir à une modification, sans intervention humaine, des critères préétablis sur la base desquels ce traitement a été effectué et qui ne permettent pas d'identifier de manière claire et transparente les motifs ayant conduit à une concordance positive à la suite dudit traitement.

8) L'article 12, paragraphe 1, de la directive 2016/681, lu en conformité avec les articles 7, 8, et l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que la conservation des données PNR fournies par les transporteurs aériens à l'UIP 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 n'est permise, après que l'évaluation préalable au titre de l'article 6, paragraphe 2, sous a), de cette directive a été effectuée, que dans la mesure où il est établi, sur la base de critères objectifs, un rapport entre ces données et la lutte contre le terrorisme ou la criminalité grave. Une conservation généralisée et indifférenciée de ces données PNR sous une forme non anonymisée ne saurait se justifier que face à une menace grave pour la sécurité des États membres qui s'avère réelle et actuelle ou prévisible, liée, par exemple, à des activités de terrorisme, et à la condition que la durée de cette conservation soit limitée au strict nécessaire.

9) L'article 6, paragraphe 2, sous b), de la directive 2016/681 doit être interprété en ce sens que la communication des données PNR ou du résultat du traitement de ces données au titre de cette disposition, qui intervient au cours de la période initiale de six mois prévue à l'article 12, paragraphe 2, de cette directive, doit respecter les conditions énoncées à l'article 12, paragraphe 3, sous b), de ladite directive.

10) La directive 2016/681, et notamment son article 1er, paragraphe 2, et son article 6, doit être interprétée en ce sens qu'elle s'oppose à une législation nationale qui admet comme finalité du traitement des données PNR le suivi de certaines activités des services de renseignement et de sécurité, dans la mesure où, dans le cadre d'une telle finalité, l'UIP nationale serait amenée à traiter lesdites données et/ou à transmettre celles-ci ou le résultat de leur traitement auxdits services à des fins autres que celle exhaustivement indiquée à l'article 1, paragraphe 2, de ladite directive, ce qui incombe au juge national de vérifier.

11) L'article 12, paragraphe 3, sous b), de la directive 2016/681 doit être interprété en ce sens que l'UIP ne constitue pas une « autre autorité nationale compétente » au sens de cette disposition.

12) L'article 3, paragraphe 1, de la directive 2004/82, au titre duquel les États membres prennent les mesures nécessaires afin d'établir l'obligation, pour les transporteurs aériens, de transmettre, à la demande des autorités chargées du contrôle des personnes aux frontières extérieures, avant la fin de l'enregistrement, les renseignements relatifs aux passagers visés au paragraphe 2 de cet article, lu en combinaison avec l'article 2, sous b) et d), de cette directive, ne concerne que les passagers transportés vers un point de passage autorisé pour le franchissement des frontières extérieures des États membres avec des pays tiers. Une législation nationale qui, dans le seul but de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration illégale, étendrait cette obligation aux données des personnes qui franchissent les frontières intérieures de l'État membre concerné par avion ou par d'autres moyens de transport serait contraire à l'article 67, paragraphe 2, TFUE et à

l'article 22 du règlement (UE) 2016/399 du Parlement européen et du Conseil, du 9 mars 2016, concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen).

13) Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux transporteurs aériens, terrestres et maritimes ainsi qu'aux opérateurs de voyage, en vue de la lutte contre le terrorisme et la criminalité grave, un transfert des données PNR et prévoyant un traitement et une conservation généralisés et indifférenciés de ces données incompatibles avec les articles 7, 8, et l'article 52, paragraphe 1, de la charte des droits fondamentaux. En application du principe d'effectivité, le juge pénal national est tenu d'écarter des informations et des éléments de preuve qui ont été obtenus en application d'une telle législation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de terrorisme ou de criminalité grave, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

---

1 Langue originale : le français.

---

2 JO 2016, L 119, p. 1.

---

3 JO 2016, L 119, p. 132.

---

4 JO 2004, L 261, p. 24.

---

5 *Moniteur belge* du 25 janvier 2017, p. 12905.

---

6 Aux termes de l'article 3, point 2, de la directive PNR, est un « vol extra-UE » « tout vol, régulier ou non, effectué par un transporteur aérien en provenance d'un pays tiers et devant atterrir sur le territoire d'un État membre ou en provenance du territoire d'un État membre et devant atterrir dans un pays tiers, y compris, dans les deux cas, les vols comportant d'éventuelles escales sur le territoire d'États membres ou de pays tiers ».

---

7 Aux termes de l'article 3, point 3), de la directive PNR, constitue un « vol intra-UE » « tout vol, régulier ou non, effectué par un transporteur aérien en provenance du territoire d'un État

membre et devant atterrir sur le territoire d'un ou de plusieurs États membres, sans escale sur le territoire d'un pays tiers ».

---

8 L'article 7, paragraphe 1, de la directive PNR prévoit que chaque État membre arrête une liste des autorités compétentes habilitées à demander aux UIP ou à recevoir de celles-ci des données PNR ou le résultat du traitement de telles données en vue de procéder à un examen plus approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. Cette liste a été publiée par la Commission en 2018 (JO 2018, C 194, p. 1 ; rectificatif JO 2020, C 366, p. 55).

---

9 Décision-cadre du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO 2008, L 350, p. 60).

---

10 JO 2016, L 119, p. 89. L'article 25 de la décision-cadre 2008/977/JAI a été remplacé par l'article 41 de la directive police.

---

11 Voir article 15, paragraphe 2, de la directive PNR.

---

12 Voir article 15, paragraphe 3, sous a) et b), de la directive PNR.

---

13 Directive du Parlement européen et du Conseil du 20 octobre 2010 concernant les formalités applicables aux navires à l'entrée et/ou à la sortie des portes des États membres et abrogeant la directive 2002/6/CE (JO 2010, L 283, p. 1).

---

14 *Moniteur belge* du 18 décembre 1998, p. 40312.

---

15 C-203/15 et C-698/15, ci-après l'« arrêt Tele2 Sverige », EU:C:2016:970.

---

16 Ci-après l'« avis 1/15 », .EU:C:2017:592.

---

17 Voir, en ce sens, arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504, point 61).

---

18 Aux termes de l'article 2, paragraphe 1, du RGPD « [l]e présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».

---

19 Voir arrêt du 16 juillet 2020, Facebook Ireland et Schrems (C-311/18, EU:C:2020:559, point 84), ainsi que arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504, point 62).

---

20 Voir, en ce sens, arrêt du 6 octobre 2020, Privacy International (C-623/17, ci-après l'« arrêt Privacy International », EU:C:2020:790, point 41 et jurisprudence citée). Aux termes de l'article 4, point 2, du RGPD constitue un « traitement » « toute opération [...] appliquée [...] à des données ou des ensembles de données à caractère personnel, telles que [...] la communication par transmission ».

---

21 Voir, en ce sens, arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504, point 69). Aux termes de l'article 3, point 7, sous a) et b), de la directive police, est une « autorité compétente » « a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; ou b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique » à ces mêmes fins.

---

22 Aucun indice en ce sens ne ressort de la décision de renvoi.

---

23 Un tel opérateur ne saurait non plus être qualifié de « sous-traitant » au sens de l'article 4, point 8, du RGPD ou de l'article 3, point 9, de la directive police, s'agissant plutôt du « responsable du traitement » au sens de l'article 4, point 7, seconde phrase, du RGPD. Aux termes de l'article 4, point 8, du RGPD et de l'article 3, point 9, de la directive police, qui sont rédigés de manière identique, le « sous-traitant » est la « personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ». Au sens de l'article 4, point 7, première phrase, du RGPD, le « responsable du traitement », est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui [...] détermine les finalités et les moyens du traitement », la deuxième phrase de cette disposition précise que « lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les

critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

---

24 Directive du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31). Cette directive a été abrogée et remplacée par le RGPD, voir article 94 de ce règlement.

---

25 C-317/04 et C-318/04, ci-après l'« arrêt Parlement/Conseil », EU:C:2006:346. Dans les affaires ayant donné lieu à cet arrêt, le Parlement avait demandé, d'une part, l'annulation de la décision 2004/496/CE du Conseil, du 17 mai 2004, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (JO 2004, L 183, p. 83, et rectificatif JO 2005, L 255, p. 168) et, d'autre part, l'annulation de la décision 2004/535/CE de la Commission, du 14 mai 2004, relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique (JO 2004, L 235, p. 11).

---

26 Aux termes de l'article 3, paragraphe 2, premier tiret, de la directive 95/46 , cette directive ne s'appliquait pas au traitement de données à caractère personnel « mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, *en tout état de cause*, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal » (mise en italique par mes soins).

---

27 Sur l'« approche téléologique » et « contextuelle » de la Cour dans l'arrêt Parlement/Conseil, voir conclusions de l'avocat général Campos Sánchez-Bordona dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6, points 47 et 62).

---

28 C-511/18, C-512/18 et C-520/18, ci-après l'arrêt « La Quadrature du Net », EU:C:2020:791.

---

29 Voir arrêt La Quadrature du Net, points 100 à 102.

---

30 Voir, dans le même sens, arrêt Privacy International, point 47.

31 C-207/16, ci-après l'« arrêt Ministerio Fiscal », EU:C:2018:788, point 34.

32 Voir, par analogie, arrêts Tele2 Sverige, points 72 à 74, et Ministerio fiscal, point 34. Ces arrêts portaient sur l'interprétation de l'article 15, paragraphe 1, première phrase, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), qui prévoit une clause de limitation analogue à celle contenue à l'article 23, paragraphe 1, sous a) à d), RGPD.

33 Une référence à l'article 15, paragraphe 1, de la directive 2002/58 était justifiée dans le contexte de cette directive, au vu du libellé de la clause d'exclusion prévue à l'article 1, paragraphe 3, de celle-ci, qui se réfère, de manière générale, aux « activités de l'État dans le domaine relevant du droit pénal ».

34 Voir, par analogie, arrêt Privacy International, points 38 et 39.

35 Il s'agit des traitements régis par les chapitres 7 à 10 et 12 de la loi PNR.

36 Voir, en ce sens, arrêts La Quadrature du Net, point 103, et Privacy International, point 48.

37 Voir, notamment, arrêt La Quadrature du Net.

38 Voir arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504, point 66).

39 Voir arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504).

40 Voir arrêt La Quadrature du Net, point 99 et jurisprudence citée.

41 Les conditions entourant ces traitements de données sont prévues au chapitre 11 de la loi PNR.

42 Voir considérants 8, 9 et 12, et article 6 de la directive API, et article 8, paragraphe 2, de la directive 2010/65.

43 L'utilisation des informations préalables sur les passagers (ci-après les « données API ») par des services répressifs est expressément prévue à l'article 6, paragraphe 1, dernier alinéa, de la directive API.

44 Voir, en ce sens, notamment, arrêt du 16 juillet 2020, Facebook Ireland et Schrems (C-311/18, EU:C:2020:559, point 170 et jurisprudence citée).

45 Voir, notamment, arrêt du 16 juillet 2020, Facebook Ireland et Schrems (C-311/18, EU:C:2020:559, point 172 et jurisprudence citée).

46 Voir, en ce sens, arrêt La Quadrature du Net, point 122.

47 Voir arrêt La Quadrature du Net, point 123.

48 Voir arrêt La Quadrature du Net, point 124 et jurisprudence citée.

49 Voir arrêt du 18 juin 2020, Commission/Hongrie (Transparence associative) (C-78/18, EU:C:2020:476, point 122 et jurisprudence citée).

50 Voir, notamment, Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie (CE:ECHR:2015:1204JUD004714306, § 227) ; Cour EDH, 18 mai 2010, Kennedy c. Royaume-Uni (CE:ECHR:2010:0518JUD002683905, § 130), et Cour EDH, 25 mai 2021, Centrum för Rättvisa c. Suède (CE:ECHR:2021:0525JUD003525208, § 246).

51 Voir Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie, (CE:ECHR:2015:1204JUD004714306, § 228) ; Cour EDH, 4 mai 2000, Rotaru c. Roumanie (CE:ECHR:2000:0504JUD002834195, § 52) ; Cour EDH, 4 décembre 2008, S. et Marper c. Royaume-Uni (CE:ECHR:2008:1204JUD003056204, § 95) ; Cour EDH, 18 mai 2021, Kennedy c. Royaume-Uni (CE:ECHR:2010:0518JUD002683905, § 151), et Cour EDH, 25 mai 2021, Centrüm för Rättvisa c. Suède (CE:ECHR:2021:0525JUD003525208, § 246).

---

52 Voir, entre autres, arrêt du 18 juin 2020, Commission/Hongrie (C-78/18, EU:C:2020:476, points 124 et 126, ainsi que jurisprudence citée) ; voir, également, Cour EDH, 4 mai 2000, Rotaru c. Roumanie (CE:ECHR:2000:0504JUD002834195, § 48) ; Cour EDH, 26 mars 1987, Leander c. Suède (CE:ECHR:1987:0326JUD000924881, § 46), et Cour EDH, 29 juin 2006, Weber et Saravia c. Allemagne (CE:ECHR:2006:0629DEC005493400, § 79).

---

53 Voir, entre autres, arrêt Ministerio Fiscal, point 51 et jurisprudence citée.

---

54 Voir, entre autres, arrêt du 18 juin 2020, Commission/Hongrie (C-78/18, EU:C:2020:476, point 126), ainsi que arrêt Ministerio Fiscal, point 51 et jurisprudence citée.

---

55 Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, ci-après l'« arrêt Digital Rights », EU:C:2014:238, point 34).

---

56 Voir avis 1/15, points 121 à 123.

---

57 Voir, par analogie, arrêt Privacy International, points 79 et 80, ainsi que jurisprudence citée.

---

58 Voir article 2, paragraphes 1 à 3, de la directive PNR.

---

59 Voir article 2, paragraphe 3, de la directive PNR.

---

60 Conformément aux articles 1er et 2 du protocole (nº 22) sur la position du Danemark, cet État membre ne participant pas à l'adoption de la directive PNR, il n'est ni lié par celle-ci, ni soumis à son application (voir considérant 40 de cette directive). Il ressort néanmoins des observations écrites déposées par le gouvernement danois que le Royaume de Danemark a adopté en 2018 une loi

portant sur la collecte, l'utilisation et la conservation des données PNR, dont les dispositions concordent largement avec celles de la directive PNR. Quant à l'Irlande, il ressort du considérant 39 de la directive PNR que cet État membre a notifié, conformément à l'article 3 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au TUE et au TFUE, son souhait de participer à l'adoption et à l'application de cette directive.

---

61 La Commission a publié une liste mise à jour des États membres qui ont décidé d'appliquer la directive PNR aux vols intra-UE visés à l'article 2 de la directive [PNR] (JO 2020, C 358, p. 7), rectifiée en septembre 2021 avec l'ajout de la Slovénie et la suppression de la référence au Royaume-Uni (JO 2021, C 360, p. 8). L'Irlande et l'Autriche ne figurent pas sur cette liste. Le rapport de la Commission au Parlement européen et au Conseil portant sur le réexamen de la directive [PNR], du 24 juillet 2020 [COM(2020)305 final, p. 11 (ci-après le « rapport de la Commission de 2020 »)] mentionne que tous les États membres, à une exception près, ont étendu la collecte des données PNR aux vols intra-UE.

---

62 Voir, notamment, points 4) et 18) de l'annexe I relatifs aux noms, au sexe, à la date de naissance, à la nationalité et aux documents d'identité du passager.

---

63 Voir, notamment, points 2), 3), 7), 13) et 18) de l'annexe I de la directive PNR mentionnant, notamment, le numéro de vol, les aéroports de départ et d'arrivée, ainsi que les dates et heures de départ et d'arrivée.

---

64 Voir points 5), 6), 9), 12) et 16) de l'annexe I.

---

65 Voir, en ce sens, avis 1/15, point 131.

---

66 SWD(2020)128 final.

---

67 Le document de travail de 2020 (p. 28 et note de bas de page 55), mentionne un taux de concordances positives de 0,59 % pour l'année 2019, desquelles seulement 0,11 % ont fait l'objet d'un transfert aux autorités compétentes. Pour l'année 2018, les pourcentages correspondants étaient respectivement de 0,25 % et de 0,4 %.

---

68 Voir avis 1/15, point 132.

69 Le système établi par la directive PNR était susceptible de couvrir, avant la crise sanitaire, jusqu'à un milliard de passagers par un, données accessibles sur https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table ?lang=fr.

70 À savoir toute personne qui répond à la notion de « passager », telle que définie à l'article 3, point 4, de la directive PNR et qui emprunte un « vol extra-UE », ainsi que, de facto, un « vol intra-UE ».

71 Dans une étude adoptée par la Commission européenne pour la démocratie par le droit (Commission de Venise) en 2015, de telles mesures sont considérées relever de la notion de « surveillance stratégique » et suivre une « tendance générale » au recours à une « surveillance proactive » de la population ; voir étude *Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique*, adopté par la Commission de Venise lors de sa 102e session plénière (Venise, 20 et 21 mars 2015), https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)006-f, point 61.

72 S'agissant de l'article 8 de la CEDH, voir arrêt de la Cour EDH, 25 mai 2021, Big Brother Watch e.a. c. Royaume-Uni (CE:ECHR:2021:0525JUD005817013, § 325, ci-après l'« arrêt Big Brother Watch ») sur les mesures d'interception en masse, où la Cour EDH affirme que l'intensité de l'ingérence dans l'exercice du droit au respect de la vie privée de ces mesures augmente au fur et à mesure que sont franchies les différentes étapes du processus, à savoir l'interception et la rétention initiale des communications et des données associées, le traitement automatisé par l'application de sélecteurs, l'examen par des analystes et la rétention subséquente des données ainsi que l'utilisation du « produit final ».

73 Voir, en ce sens, considérants 6 et 7 de la directive PNR ; voir, pour une analyse approfondie de la finalité et des implications pour la protection de la vie privée et des données à caractère personnel, rapport intitulé *Passenger Name Records (PNR), data mining and data protection : the need for strong safeguards*, préparé par Korff, D., avec la contribution de Georges, M., http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/TPD(2015)11_PNR %20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15 %2006 %202015.pdf (ci-après le « rapport Korff »).

74 Comme cela est indiqué dans le rapport Korff, « PNR is not an isolated issue, but a new symptom of a much wider disease ».

75 Voir, entre autres, arrêts du 16 juillet 2020, Facebook Ireland et Schrems (C-311/18, EU:C:2020:559, point 175) ; du 8 septembre 2020, Recorded Artists Actors Performers (C-265/19, EU:C:2020:677, point 86 et jurisprudence citée), ainsi que arrêt Privacy international, point 65.

---

76 Voir, entre autres, arrêts de la Cour EDH du 8 juin 2006, Lupsa c. Roumanie, (CE:ECHR:2006:0608JUD001033704, §§ 32 et 33), et du 15 décembre 2020, Pişkìn c. Turquie (CE:ECHR:2020:1215JUD003339918, § 206) ; voir, également, arrêt Big Brother Watch, § 333. Sur la nécessité de reconnaître à l'expression « prévue par la loi » à l'article 52, paragraphe 1, de la CEDH la même interprétation que celle retenue par la Cour EDH, voir conclusions de l'avocat général Wathelet dans l'affaire WebMindLicenses (C-419/14, EU:C:2015:606, points 134 à 143).

---

77 Voir, en dernier lieu, arrêt Big Brother Watch., § 333.

---

78 Voir arrêt du 17 décembre 2015, WebMindLicenses (C-419/14, EU:C:2015:832, point 81) ; voir, également, Cour EDH, 1er juillet 2008, Liberty e.a. c. Royaume-Uni (CE:ECHR:2008:0701JUD005824300, § 69), ainsi que arrêt Big Brother Watch, § 333.

---

79 Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée à Strasbourg le 28 janvier 1981 et ratifiée par tous les États membres, plus connue comme la « convention 108 ». Un protocole d'amendement de cette convention a été élaboré en 2018 en vue de sa modernisation. Par décision (UE) 2019/682 du Conseil du 9 avril 2019 (JO 2019, L 115, p. 7), les États membres ont été autorisés à ratifier, dans l'intérêt de l'Union, ledit protocole d'amendement pour autant que ses dispositions relèvent de la compétence exclusive de l'Union. Dans la suite des présentes conclusions, je me référerai également au texte de la convention 108 modernisée, qui bien que non encore ratifiée par tous les États membres et non encore entrée en vigueur prévoit, ainsi que cela ressort de la décision 2019/682, des garanties reposant sur les mêmes principes que ceux énoncés dans le RGPD et dans la directive police.

---

80 https://rm.coe.int/t-pd-201618rev-avis-pnr-fr/16807b6c09, p. 3 et 5. Le rapport explicatif accompagnant le protocole d'amendement de la convention 108 (ci-après le « rapport explicatif sur la convention 108 modernisée ») met aussi l'accent sur l'exigence que la mesure prévoyant des ingérences dans les droits au respect de la vie privée et à la protection des données personnelles soit « accessible », « prévisible », « suffisamment détaillée » et « clairement formulée » ; voir point 91 de ce rapport explicatif, https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

---

81 Voir, a contrario, arrêt du 3 décembre 2019, République tchèque/Parlement et Conseil (C-482/17, EU:C:2019:1035, point 135).

82 Voir, entre autres, arrêt La Quadrature du Net, point 132 et jurisprudence citée ; voir, également, Cour EDH, arrêt Big Brother Watch, § 334.

83 Voir, à cet égard, Tridimas, T., Gentile, G. « The essence of Rights : an unreliable Boundary ? », *German Law Journal*, 2019, p. 796 ; Lenaerts, K., « Limits on limitations : The Essence of Fundamental Rights in the EU », *German Law Journal*, 2019, 20, p. 779 et suiv..

84 À partir de l'arrêt de la Cour EDH du 24 octobre 1979, Winterwerp c. Pays-Bas, (CE:ECHR:1979:1024JUD000630173, § 60).

85 Voir Explications relatives à la Charte des droits fondamentaux (JO 2007, C 303, p. 17, en particulier « Explications ad article 52 », p. 32, ci-après les « explications relatives à la Charte »).

86 Voir, déjà en ce sens, notamment, arrêts du 14 mai 1974, Nold/Commission (4/73, EU:C:1974:51, point 14), et du 13 décembre 1979, Hauer (44/79, EU:C:1979:290, point 23).

87 C-362/14, ci-après l'arrêt « Schrems I », EU:C:2015:650, points 94 à 98.

88 Voir Lenaerts, K., op. cit., p. 781 ; Tridimas, T., Gentile, G., op. cit., p. 803.

89 Les explications relatives à la Charte reconnaissent expressément que « la dignité de la personne humaine fait partie de la substance des droits inscrits dans [la] Charte » et qu'« [i]l ne peut donc y être porté atteinte, même en cas de limitation d'un droit ».

90 Je renvoie à cet égard aux considérations contenues dans l'opinion en partie concordante commune aux juges Lemmens, Vehabović et Bošniak dans l'arrêt Big Brother Watch, §§ 3 à 10.

91 Directive du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54).

92 Voir arrêt Digital Rights, point 39 ; voir, également, s'agissant de la directive 2002/58, arrêt Tele2 Sverige, point 101.

93 Voir avis 1/15, point 150.

94 Voir en ce sens, notamment, arrêt Digital Rights, point 40.

95 Voir, en ce même sens, avis 1/15, point 128.

96 Voir avis 1/15, points 164 et 165.

97 Voir avis 1/15, point 150.

98 Voir, notamment, considérants 5, 6, 15 et 22 de la directive PNR.

99 Proposition de la Commission du 2 février 2011, relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière [COM(2011) 32 final, p. 4].

100 Pour des raisons de simplification, dans les présentes conclusions, j'utiliserai les expressions « services répressifs » ou « autorités répressives » pour indiquer, de manière générale, toute autorité investie de pouvoirs dans les domaines de la détection, de la prévention, de la poursuite ou de l'enquête en matière de terrorisme ou de criminalité grave, couverts par la directive PNR.

101 Voir considérant 7 de la directive PNR. Voir, également, proposition de directive PNR, p. 5.

102 Voir, en ce sens, avis 1/15, ainsi que arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, ci-après l'« arrêt Prokuratuur », EU:C:2021:152, point 33 et jurisprudence citée).

---

103 Voir, en ce sens, avis 1/15, point 149 et jurisprudence citée, ainsi que arrêt La Quadrature du Net.

---

104 Voir, ci-après, analyse sur la proportionnalité de l'ingérence.

---

105 Voir arrêt La Quadrature du Net, point 125.

---

106 Voir arrêt La Quadrature du Net, point 126 et jurisprudence citée.

---

107 Voir arrêt La Quadrature du Net, point 136.

---

108 Voir arrêt Digital Rights, point 46 et jurisprudence citée.

---

109 Voir avis 1/15, point 140, ainsi que arrêt La Quadrature du Net, point 130 et jurisprudence citées. L'exigence que le traitement de données à caractère personnel reflète, à chaque étape, un « juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu » est également énoncée à l'article 5 de la convention 108.

---

110 Voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, point 55 et jurisprudence citée), ainsi que arrêts La Quadrature du Net, point 131, et Prokuratuur, point 32.

---

111 Voir, en ce sens, arrêts Digital Rights, point 54, et Schrems I, point 91, ainsi que avis 1/15, point 141.

---

112 Voir avis 1/15, point 141 et jurisprudence citée.

113 Voir, en ce sens, arrêt Digital Rights, point 48.

114 Voir, en ce sens, points 201 à 203 des présentes conclusions.

115 Je renvoie, à cet égard, aux données contenus dans le document de travail de 2020.

116 Voir, en ce sens, avis du 19 août 2016, p. 5.

117 Sur l'importance des statistiques aux fins de l'évaluation de l'efficacité du système établi par la directive PNR, voir, notamment, avis 1/2011 du 14 juin 2011, sur la proposition de directive PNR, https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_FR.pdf, point 2.1.2.1 (ci-après l'« avis 1/2011 de la FRA »).

118 Cette question est, en revanche, clairement posée par le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden, Allemagne), dans l'affaire pendante C-215/20.

119 La Commission a été invitée à présenter ses observations à ce propos dans le cadre d'une question pour réponse écrite. Les autres intéressés ont pu prendre position lors de l'audience.

120 Voir point 107, in fine, des présentes conclusions.

121 Directive du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO 2017, L 88, p 6).

122 Je relève, à cet égard, que la notion de « crime de nature transnationale » telle que définie, par exemple, dans le projet d'accord PNR Canada-UE était suffisamment large pour inclure également des infractions commises dans un seul pays et où l'auteur « se trouve dans un autre pays ou a l'intention de se rendre dans un autre pays » ; voir article 3, paragraphe 3, sous e), du projet d'accord PNR Canada-UE, dont le libellé est repris au point 30 de l'ais 1/15. J'observe également que, dans son avis 1/2011 (points 2.2.3.1 et 3.7), la FRA avait suggéré de limiter le système PNR de

l'Union aux seules infractions transnationales graves. La proposition de directive PNR envisageait en revanche un traitement automatisé différencié pour les infractions transnationales et pour celles ne revêtant pas ce caractère (voir article 4, paragraphe 2, sous a), de cette proposition.

---

123 Je relève, par ailleurs, qu'une partie des infractions visées à l'annexe II relèvent de domaines de criminalité qualifiée de « particulièrement grave » par l'article 83, paragraphe 1, premier alinéa, TFUE et énumérés au second alinéa de ce paragraphe. Il s'agit notamment de la traite des êtres humains, de l'exploitation sexuelle des enfants, du trafic illicite de drogues, du trafic illicite d'armes, du blanchiment d'argent, de la corruption, de la contrefaçon de moyens de paiement, de la criminalité informatique et de la criminalité organisée. Dans plusieurs de ces domaines, le législateur de l'Union a adopté, sur la base de l'article 83, paragraphe 1, TFUE des directives établissant « des règles minimales relatives à la définition des infractions pénales et des sanctions » ; voir, notamment, directive 2011/36/UE du Parlement européen et du Conseil, du 5 avril 2011, concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes et remplaçant la décision-cadre 2002/629/JAI du Conseil (JO 2011, L 101, p. 1) ; directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO 2011, L 335, p. 1) ; directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO 2013, L 218, p. 8) ; directive (UE) 2019/713 du Parlement européen et du Conseil, du 17 avril 2019, concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil (JO 2019, L 123, p. 18) ; directive (UE) 2017/1371 du Parlement européen et du Conseil, du 5 juillet 2017, relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal (JO 2017, L 198, p. 29), et directive (UE) 2018/1673 du Parlement européen et du Conseil, du 23 octobre 2018, visant à lutter contre le blanchiment de capitaux au moyen du droit pénal (JO 2018, L 284, p. 22).

---

124 Je relève, cependant, que toutes les infractions visées à l'annexe I, à l'exception de l'« espionnage industriel », figurent à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil, du 13 juin 2002, relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO 2002, L 190, p. 1). Si elles ne sont pas explicitement qualifiées de graves, elles donnent néanmoins lieu, lorsqu'elles atteignent le même seuil de peine privative de liberté prévu à l'article 3, point 9, de la directive PNR, à la remise sur la base d'un mandat d'arrêt européen, sans contrôle de la double incrimination du fait. La presque totalité desdites infractions, à l'exception du « sabotage », du « détournement d'avion » et de l'« espionnage industriel » figure également à l'annexe I du règlement (UE) 2018/1727 du Parlement européen et du Conseil, du 14 novembre 2018, relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil (JO 2018, L 295, p. 138), qui énumère la liste des « formes graves de criminalité » relevant de la compétence d'Eurojust.

---

125 Il s'agit, notamment, des points 7, 8, 10 et 16.

---

126 C’est le cas, par exemple, de la « fraude » (point 7), de la « corruption » (point 6), de la « cybercriminalité » (point 9) et des « infractions contre l’environnement » (point 10). C’est au sujet, en particulier, des infractions frauduleuses que s’interroge le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden), dans l’affaire pendante C-215/20.

---

127 Cette directive précise d’ailleurs, à son article 9, la durée minimale de la peine d’emprisonnement maximale dont doivent être passible lesdites infractions, seuil qui seulement dans certaines circonstances atteint trois ans.

---

128 Directive du Parlement et du Conseil du 19 novembre 2008 (JO 2008, L 328, p. 28).

---

129 Directive du Conseil du 28 novembre 2002 définissant l’aide à l’entrée, au transit et au séjour irréguliers (JO 2002, L 328, p. 17).

---

130 Décision-cadre du Conseil du 28 novembre 2002 visant à renforcer le cadre pénal pour la répression de l’aide à l’entrée, au transit et au séjour irréguliers (JO 2002, L 328, p. 1).

---

131 Décision-cadre du Conseil du 22 juillet 2003 relative à la lutte contre la corruption dans le secteur privé (JO 2003, L 192, p. 54).

---

132 Décision-cadre du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée (JO 2008, L 300, p. 42).

---

133 Voir, notamment, considérants 7 et 22 de la directive PNR.

---

134 Voir considérant 35 de la directive PNR.

---

135 Voir, par analogie, arrêts du 16 décembre 2008, Arcelor Atlantique et Lorraine e.a. (C-127/07, EU:C:2008:728, points 61 et 62), ainsi que du 17 octobre 2013, Schaible (C-101/12, EU:C:2013:661, points 91 et 94).

---

136 Voir document 9944, approuvé par le Secrétaire général de l'OACI et publié sous son autorité. La version en langue française de ce document est accessible sur le site https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_fr.pdf. Conformément au point 9.22 de l'annexe 9 (Facilitations) à la convention relative à l'aviation civile internationale, signée à Chicago le 7 décembre 1944) (ci-après la « convention de Chicago »), les États contractants de cette convention qui exigent les données PNR sont tenus d'aligner leurs besoins en matière de données et le traitement de ces données, entre autres, sur ces lignes directrices.

---

137 Dans le même sens, voir avis 1/15, point 160.

---

138 Voir points 2.1.2 et 2.1.5 des lignes directrices de l'OACI.

---

139 La seule référence aux lignes directrices de l'OACI dans la directive PNR est contenue au considérant 17 de celle-ci et ne concerne que les « formats de données reconnus pour les transferts des données PNR par les transporteurs aériens aux États membres ».

---

140 Ainsi, le point 2.1.5 desdites lignes directrices mentionne des « renseignements supplémentaires » ou « relatifs à des services demandés », pouvant porter « sur des demandes de soins médicaux ou de repas spéciaux, des "mineurs voyageant seuls", des demandes d'assistance, etc. ». Le point 2.1.6 précise, quant à lui que le « champ "remarques générales" » peut également contenir « certains renseignements, tels que les correspondances ou communications internes entre le personnel des compagnies aériennes et les agents de réservation ».

---

141 Voir points 2.1.5 et 2.1.6 des lignes directrices de l'OACI.

---

142 Voir arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, point 32), concernant le cas du demandeur de passeport tenu de se soumettre au prélèvement de ses empreintes digitales afin de pouvoir disposer d'un document lui permettant d'effectuer des déplacements à destination d'un pays tiers.

---

143 Je reviendrai sur cette catégorie de données plus loin dans les présentes conclusions.

---

144 La FRA s'est exprimée en ce sens dans son avis 1/2011, p. 13. Dans son avis du 25 mars 2011 sur la proposition de directive PNR, (https://edps.europa.eu/sites/edp/files/publication/110325_pnr_en.pdf, point 47) (ci-après l'« avis du

CEPD du 25 mars 2011 »), le CEPD a proposé d'exclure la rubrique « Remarques générales » de la liste de l'annexe I.

---

145 Voir, notamment, arrêts du 19 novembre 2009, Sturgeon e.a. (C-402/07 et C-432/07, EU:C:2009:716, point 47 et jurisprudence citée) ; du 19 septembre 2013, Réexamen Commission/Strack (C-579/12 RX-II, EU:C:2013:570, point 40), ainsi que du 14 mai 2019, M e.a. (Révocation du statut de réfugié) (C-391/16, C-77/17 et C-78/17, EU:C:2019:403, point 77 et jurisprudence citée).

---

146 Voir, notamment, considérants 5, 7, 11, 15, 16, 20, 22, 23, 25, 27, 28, 31, 36 et 37 de la directive PNR.

---

147 Voir arrêts du 26 juin 2007, Ordre des barreaux francophones et germanophone e.a. (C305/05, EU:C:2007:383, point 28), ainsi que du 14 mai 2019, M e.a. (Révocation du statut de réfugié) (C-391/16, C-77/17 et C-78/17, EU:C:2019:403, point 77).

---

148 Pour ce qui importe ici, le considérant 9 prévoit que « [l]'utilisation combinée des données PNR et des données API présente une valeur ajoutée en ce qu'elle aide les États membres à vérifier l'identité d'une personne, renforçant ainsi la valeur du résultat en termes de prévention, de détection et de répression des infractions et réduisant au minimum le risque de soumettre des personnes innocentes à des vérifications et à des enquêtes ».

---

149 En ce sens, voir, également, proposition de directive PNR, p. 7, point 1. Ces mêmes données figurent dans les directives relatives aux renseignements préalables concernant les voyageurs (RPCV) élaborées par l'Organisation mondiale des douanes (OMD), l'Association du transport aérien international (IATA) et l'OACI, http://www.wcoomd.org/~/media/wco/public/fr/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/api-guidelines-_f.pdf ?db=web) [(ci-après les « directives RPCV »), point 8.1.5, sous a)], comme « principaux éléments de données susceptibles de figurer dans la zone lisible à la machine des documents de voyage officiels ».

---

150 L'article 3, paragraphe 2, de la directive API est rédigé comme suit : « Parmi ces renseignements figurent : le numéro et le type du document de voyage utilisé ; la nationalité ; le nom complet ; la date de naissance ; le point de passage frontalier utilisé pour entrer sur le territoire des États membres ; le code de transport ; les heures de départ et d'arrivée du transport ; le nombre total des personnes transportées ; le point d'embarquement initial ». Je souligne que, dans son programme de travail pour 2022, COM(2021) 645 final, p. 9, la Commission a envisagé une mise à jour de la directive API. En septembre 2020, elle a publié une évaluation de cette directive constituant la base pour sa future révision, SWD(2020), 174 final (ci-après le « document de travail

de 2020 sur la directive API »). Dans ledit document, la Commission souligne notamment le fait que la liste de données contenue à l'article 3, paragraphe 2, de la directive API n'est pas en conformité avec les normes internationales sur les données API, notamment en ce qu'elle n'inclut pas toutes les données figurant la partie lisible à la machine des documents d'identité (voir, notamment, p. 48).

---

151 Voir directives RPCV, points 8.1.5, sous b) et c).

---

152 Une interprétation analogue de la rubrique correspondante du projet d'accord PNR Canada-UE figure au point 161 de l'avis 1/15.

---

153 Je relève que la Cour est actuellement saisie d'une série de questions préjudicielles portant spécifiquement sur le caractère suffisamment précis de plusieurs points de l'annexe I, et notamment des points 4, 8, 12, 18 (voir affaire pendante C-215/20).

---

154 Voir avis 1/15, point 158.

---

155 Je relève que les informations relatives à l'agence ou à l'agent de voyages sont déjà visées à l'annexe I, point 5.

---

156 Voir définition de données PNR à l'article 3, point 5, de la directive PNR.

---

157 En ce sens, voir, également, conclusions de l'avocat général Mengozzi dans l'avis 1/15, [(Accord PNR UE-Canada), EU:C:2016:656], point 218.

---

158 Voir rubrique correspondante de l'appendice I aux lignes directrices de l'OACI.

---

159 Voir, notamment, en ce sens, arrêt Digital Rights, point 57. Sur l'exigence que les catégories de données visées par une mesure d'accès soient limitées à ce qui est strictement nécessaire à l'objectif poursuivi, voir, en dernier lieu, arrêt Prokuratuur, point 38. Le principe de minimisation des données est entre autres prévu à l'article 5, paragraphe 1, sous c), du RGPD et à l'article 4, paragraphe 1, sous c), de la directive police.

160 Voir, notamment, Cour EDH, 18 avril 2013, M. K. c. France (CE:ECHR:2013:0418JUD001952209, § 35).

161 Voir rapport explicatif de la convention 108 de 1981 (https://rm.coe.int/16800ca471), article 5, point 40, ainsi que rapport explicatif sur la convention 108 modernisée, article 5, point 51.

162 Voir points 154 à 158 et 162 à 164 des présentes conclusions.

163 Voir points 133 à 153 des présentes conclusions.

164 Le droit de l'enfant au respect de sa vie privée est notamment consacré à l'article 16 de la convention de New York relative aux droits de l'enfant, adoptée le 20 novembre 1989 et entrée en vigueur le 2 septembre 1990.

165 Voir point 2.7.3 des lignes directrices de l'OACI.

166 Voir point 2.7.4 des lignes directrices de l'OACI.

167 L'exigence de garantir la sécurité et la fiabilité du transfert des données aux UIP est d'ailleurs rappelée à l'article 16, paragraphe 1, de la directive PNR concernant les moyens électroniques utilisés pour ce transfert et a été l'un des critères auxquels la Commission s'est conformée aux fins de l'adoption, requise au paragraphe 3 de cet article, des protocoles communs et des formats de données devant être utilisés par les transporteurs aériens lors dudit transfert ; voir décision d'exécution (UE) 2017/759 de la Commission, du 28 avril 2017, sur les protocoles communs et formats de données devant être utilisés par les transporteurs aériens lors d'un transfert de données PNR aux unités d'information passagers (JO 2017, L 113, p. 48).

168 Voir considérant 37 de la directive PNR.

169 Les catégories de données à caractère personnel énumérées à l'article 13, paragraphe 4, de la directive PNR sont toutes comprises dans celles répondant à la notion de « catégories particulières de données à caractère personnel » visée à l'article 9, paragraphe 1, du RGPD.

---

170 À cet égard, sont, à mon sens, privées de pertinence les allégations avancées par plusieurs États membres ayant présenté des observations sur la deuxième question préjudicielle, tirées de l'existence de moyens techniques permettant d'effacer aisément les données sensibles transmises par les transporteurs aériens.

---

171 Conclusions de l'avocat général Mengozzi dans l'avis 1/15 (Accord PNR UE-Canada), EU:C:2016:656.

---

172 Je relève que même les lignes directrices de l'OACI, tout en n'excluant pas que les données sensibles qui peuvent être extraites des rubriques « texte libre » puissent être utiles pour l'évaluation du risque qu'un passager peut représenter, recommandent néanmoins aux États contractants de faire en sorte qu'elle ne soient prises en considération que s'il existe des indications concrètes appelant leur utilisation aux fins poursuivi par leurs régimes PNR.

---

173 Je rappelle qu'une telle exclusion avait été déjà suggérée par le CEPD dans son avis du 25 mars 2011, point 47.

---

174 Il s'agit de données susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise.

---

175 Voir, en ce sens, arrêts La Quadrature du Net, points 141 à 145, et Tele2 Sverige, points 105 et 106, rendus dans le cadre de l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte, ainsi que arrêt Digital Rights, points 57 et 58, dans lequel la Cour a déclaré l'invalidité de la directive 2006/24.

---

176 Voir arrêt La Quadrature du Net, point 177.

---

177 Voir arrêt La Quadrature du Net, points 134 à 139 et 177. Selon la Cour, la responsabilité qui incombe aux États membres en matière de sécurité nationale « correspond à l'intérêt primordial

de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme » ; voir arrêts La Quadrature du Net, point 135, et Privacy International, point 74.

---

178 Voir arrêt La Quadrature du Net, points 138 et 178.

---

179 Voir, notamment, arrêt La Quadrature du Net, points 141 à 145.

---

180 Voir arrêt La Quadrature du Net, points 115 et 116 ; voir, également, conclusions de l'avocat général Campos Sanchéz-Bordona dans les affaires jointes SpaceNet et Telekom Deutschland (C-793/19 et C-794/19, EU:C:2021:939, points 74 et 75).

---

181 Voir arrêt Tele2 Sverige, point 119.

---

182 Voir, en ce sens, arrêt Tele2 Sverige, points 103 à 107 et 119, ainsi que jurisprudence citée.

---

183 Voir avis 1/15, points 186 et 187.

---

184 Dans les arrêts Digital Rights (point 59) et Tele2 Sverige (point 111), comme dans la jurisprudence postérieure (voir, notamment, arrêt La Quadrature du Net, points 143 à 150), c'est précisément le fait que la réglementation en cause ne se fondait pas sur des « éléments objectifs » du type de ceux mentionnés par la Cour au point 187 de l'avis 1/15, permettant de viser un public dont les données étaient susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, qui rend cette réglementation non proportionnée.

---

185 Voir arrêt La Quadrature d Net (point 117 et jurisprudence citée) ; voir également arrêt Prokuratuur (point 36).

---

186 Arrêt La Quadrature du Net, point 142.

187 Voir avis 1/15, points 128 et 150.

188 Voir avis 1/15, point 150.

189 Sur la difficulté d'une telle appréciation s'agissant des métadonnées, voir arrêt Prokuratuur, point 40.

190 Un effort en ce sens a été fait par le législateur allemand dans la réglementation faisant l'objet des affaires jointes C-793/19 et C-794/19, SpaceNet et Telekom Deutschland, dans lesquelles l'avocat général Campos Sánchez-Bordona a présenté ses conclusions (EU:C:2021:939, points 60 et 61).

191 Je renvoie à cet égard au point 93 des présentes conclusions.

192 Voir arrêt La Quadrature du Net, point 118 et jurisprudence citée.

193 Voir arrêt Tele2 Sverige, point 93.

194 Conclusions de l'avocat général Mengozzi dans l'avis 1/15 [(Accord PNR UE-Canada), EU:C:2016:656].

195 Voir, notamment, Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie (CE:ECHR:2015:1204JUD004714306, § 260).

196 Voir arrêts La Quadrature du Net (points 146 à 151), et Tele2 Sverige (point 119).

197 En ce sens, s'agissant des mesures d'interception de masse, voir arrêt Big Brother Watch, § 348.

198 Voir, par analogie, arrêt du 3 octobre 2019, A e.a. (C-70/18, EU:C:2019:823, point 61).

199 Voir, récemment, communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité [COM(2020) 605 final, p. 28], ainsi que communication de la Commission : programme de lutte antiterroriste pour l'UE : anticiper, prévenir, protéger et réagir [COM(2020) 795 final, p. 15 et suiv.].

200 Résolution du 21 décembre 2017 [ci-après la « résolution 2396 (2017 »)], https://undocs.org/fr/S/RES/2396(2017).

201 Voir résolution 2396 (2017), point 12 ; dans ce même point 12, le Conseil de sécurité des Nations unies « exhortel'OACI à travailler avec ses États membres en vue d'établir une norme pour la collecte, l'utilisation, le traitement et la protection des données PNR ». À la suite d'une telle invitation, le 23 juin 2020, l'OACI a adopté l'amendement nº 28 de l'annexe 9 de la convention de Chicago qui, comme cela a déjà été indiqué, établit des normes internationales en matière de facilitation et dont le chapitre 9, section D, porte spécifiquement sur les PNR. Le 12 janvier 2021, la Commission a adopté une proposition de décision du Conseil relative à la position à prendre, au nom de l'Union européenne, au sein de [l'OACI] en ce qui concerne cet amendement [COM(2021) 16 final].

202 Résolution du 19 juillet 2019, point 15, c), https://undocs.org/fr/S/RES/2482(2019).

203 Il existe actuellement deux accords internationaux conclus par l'Union avec respectivement l'Australie [accord entre l'Union européenne et l'Australie sur le traitement et le transfert de [données PNR] par les transporteurs aériens au service australien des douanes et de la protection des frontières (JO 2012, L 186, p. 4)] et les États-Unis d'Amérique [accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des [données PNR] et leur transfert au ministère américain de la sécurité intérieure (JO 2012, L 215, p. 5)]. Une évaluation conjointe de ces deux accords, en vue de la conclusion de nouveaux accords est en cours. Le 18 février 2020, le Conseil a en outre autorisé la Commission à ouvrir des négociations avec le Japon.

204 Voir résolution 2396 (2017), p. 4.

205 Y inclus les personnes jouissant du droit à la libre circulation en vertu du droit de l'Union ; voir règlement (UE) 2017/458 du Parlement européen et du Conseil, du 15 mars 2017, modifiant le

règlement (UE) 2016/399 en ce qui concerne le renforcement des vérifications dans les bases de données pertinentes aux frontières extérieures (JO 2017, L 74, p. 7).

---

206 En ce sens, voir, également, avis 1/15, point 187. Voir, également, Communication de la Commission relative à la démarche globale en matière de transfert des données des dossiers [PNR] aux pays tiers [COM(2010) 492 final, p. 6, point 2.2].

---

207 C'est, en quelques sorte, ce qu'implique la Commission dans sa proposition de directive PNR, p. 3.

---

208 Voir, en ce sens, arrêt Prokuratuur, point 49 et jurisprudence citée.

---

209 Voir article 4, paragraphe 2, sous a), de la proposition de directive PNR.

---

210 Si dans sa version en langue française, l'article 6, paragraphe 3, sous a), mentionne des « bases de données utiles », dans la plupart des autres versions linguistiques, cette disposition vise plutôt des « bases de données pertinentes » : voir, notamment, les versions en langues espagnole (« pertinentes »), allemande (« massgeblich »), anglaise (« relevant »), italienne (« pertinenti »), néerlandaise (« relevant »), et portugaise (« relevantes »).

---

211 Tel qu'il est rédigé, l'article 6, paragraphe 3, sous a), de la directive PNR semble permettre des analyses prenant la forme d'une exploration de données par recoupement avec des données très variées, pour autant que cette exploration soit finalisée à la poursuite des objectifs visés par cette directive. Sur les risques liés au « data mining » en matière de données PNR, voir rapport Korff, p. 77. Le CEPD a souligné avec force le manque de précision et de prévisibilité de l'identification des bases de données auxquelles les données PNR peuvent être confrontées dans son avis du 25 mars 2011, point 18.

---

212 Le caractère vague et ouvert du libellé de l'article 6, paragraphe 3, sous a), de la directive PNR se traduit par une transposition en droit national très variée, qui va d'une interprétation stricte de la notion de « base de données utiles », qui limite l'analyse prévue à la seule confrontation avec les bases de données explicitement mentionnées dans cette disposition (c'est le cas de la République fédérale d'Allemagne, ainsi que cela ressort des observations présentées par son gouvernement devant la Cour) à une interprétation plus large qui couvre toute base de données disponibles ou accessibles aux autorités compétentes dans le cadre de leur mission (en ce sens est rédigé notamment l'article 24, § 1, point 1), de la loi PNR.

213 En aucun cas, à mon sens, un État membre ne devra se considérer tenu, sur la base de l'article 6, paragraphe 3, sous a), de la directive PNR, d'autoriser son UIP à confronter systématiquement les données PNR avec des « bases de données utiles », au sens de cette disposition, gérées par ses services de renseignement.

---

214 L'article 3, point 4, de la directive police définit le « profilage » comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne ». La même définition figure à l'article 4, point 4, du RGPD et au point 1, sous c), de l'annexe à la recommandation CM/Rec(2021)8 du 3 novembre 2021 du Comité des ministres du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, https://search.coe.int/cm/pages/result_details.aspx ?ObjectId=0900001680a46148, (ci-après la « recommandation de 2021 sur le profilage »).

---

215 Le point 1, sous j, i), de la recommandation de 2021 sur le profilage définit en tant que « traitements de profilage à risque élevé », le « profilage dont le fonctionnement entraîne des effets juridiques ou qui ont un impact significatif pour la personne concernée ou pour le groupe de personnes identifié par le traitement de profilage ».

---

216 Voir avis 1/15, point 272.

---

217 Aux termes du point 1.1, sous d), de l'annexe de la recommandation de 2021 sur le profilage, le terme « profil » désigne « un ensemble de données attribué à une personne, qui caractérise une catégorie de personnes ou qui est destiné à être appliqué à une personne ». Ainsi que l'explique le rapport sur l'évolution de la situation après l'adoption de la recommandation (2010)13 sur le profilage (https://rm.coe.int/t-pd-201907fin-fr-rapport-profilage-2770287889931-final-clean-2755/1680a0925b, p. 21), ayant précédé l'adoption de la recommandation de 2021 sur le profilage, la notion de « profil » garde tout son sens dans des systèmes qui, comme la directive PNR, distinguent les opérations de création de profils [voir, notamment, article 6, paragraphe, 2 sous b), de cette directive] de celles qui l'appliquent et permet « une transparence des critères qui sont appliqués dans un second temps par l'opération de profilage ».

---

218 Voir article 6, paragraphe 4, de la directive PNR, ainsi que avis 1/15, point 172.

---

219 Voir article 6, paragraphe 4, de la directive PNR.

---

220 Voir avis 1/15, point 172.

---

221 Voir considérant 7 de la directive PNR.

---

222 Voir avis 1/15, point 174.

---

223 La même exigence figure au point 174 de l'avis 1/15.

---

224 Je relève que l'ensemble des motifs de discrimination figurant à l'article 21 de la Charte est reproduit au considérant 20 de la directive PNR. Un alignement sur la liste des motifs de discrimination prohibés visée à l'article 21 avait été proposé par la FRA dans son avis 1/2011, p. 8.

---

225 Aux termes du point 1.1, sous g), de l'annexe à la recommandation de 2021 sur le profilage, l'expression « machine learning » désigne « un traitement utilisant des méthodes particulières d'intelligence artificielle fondé sur des approches statistiques pour donner aux ordinateurs la capacité d'"apprendre" à partir de données, c'est-à-dire d'améliorer leurs performances à résoudre des tâches sans être explicitement programmés pour chacune ».

---

226 Concernant les effets de l'opacité des systèmes algorithmiques sur la possibilité d'un contrôle humain visant à prévenir les effets préjudiciables de ces systèmes et leurs impacts négatifs sur les droits de l'hommes, voir recommandation CM/Rec(2020)1 du Comité des ministres du Conseil de l'Europe aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme.

---

227 Cette définition figure au considérant 25 de la directive PNR.

---

228 L'énoncé du considérant 37 de la directive PNR, selon lequel « la conservation des données PNR dans les UIP est autorisée pendant une période *n'excédant pas cinq ans* au terme de laquelle les données devraient être effacées » (italique ajouté par mes soins), ne permet pas, à mon sens, de remettre en cause le libellé clair de l'article 12, paragraphe 1, de cette directive.

229 Voir, s'agissant du traitement des données à caractère personnel à des fins de détection, prévention, poursuite et enquête en matière d'infractions pénales, directive police, article 4, sous e), et considérant 26. Voir, plus en général, article 5, paragraphe 1, sous e), du RGPD, et article 5, paragraphe 4, sous e), de la convention 108 modernisée.

230 Voir, arrêts Schrems I (point 93) ; Tele2 Sverige (point 110) ; avis 1/15 (point 191), ainsi que arrêt La Quadrature du Net, (point 133).

231 Voir avis 1/15, point 197.

232 Voir avis 1/15, point 205.

233 Voir avis 1/15, point 207.

234 Il s'agirait là d'une application par analogie des points 187 et suiv. de l'avis 1/15, puisque ce dernier ne visait que l'hypothèse des données PCR recueillies à l'entrée sur le territoire du Canada.

235 Voir avis 1/15, point 209.

236 Voir avis 1/15, point 205.

237 Le projet d'accord PNR Canada-UE prévoyait un masquage des noms de tous les passagers trente jours après leur réception par le Canada et un masquage d'autres informations expressément énumérées deux ans après cette réception : voir article 16, point 3, du projet d'accord PNR Canada-UE examiné par la Cour, et avis 1/15, point 30.

238 Voir avis du 19 août 2016, p. 9.

239 Voir, notamment, arrêt La Quadrature du Net, points 148 et 149.

240 Il en va de même des demandes de communication des données PNR avancées par les UIP d'autres États membres au titre de l'article 9, paragraphe 2, de la directive PNR.

241 Voir avis 1/15, point 192 et jurisprudence citée. Plus récemment, voir arrêts Privacy international, point 77, et, par analogie, Prokuratuur, point 49 et jurisprudence citée.

242 Voir avis 1/15, point 200.

243 Voir avis 1/15, point 200.

244 Voir avis 1/15, point 201.

245 Voir avis 1/15, point 202.

246 Voir, en ce sens, avis 1/15, point 201.

247 Voir, notamment, article 4, article 7, paragraphes 1 et 2, article 9, paragraphe 2, article 10, paragraphe 2, article 12, paragraphe 4, de la directive PNR ; voir, notamment, considérants 6, 9, 10, 11, 15, 23, 25, 35 et 38 de cette directive. Je rappelle par ailleurs que la proposition de directive PNR précisait, à son considérant 28, que « [l]a présente directive ne porte pas atteinte à la possibilité offerte aux États membres de prévoir, en vertu de leur législation nationale, un système de collecte et de traitement des données PNR à des fins autres que celles visées dans la présente directive ». Or, cette précision n'a pas été reprise dans le texte final de la directive PNR.

248 Cette possibilité est cependant admise à l'article 4, paragraphe 3, de la directive PNR, au titre duquel « [l]es membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes », à tout le moins dans la mesure où les services de renseignement et de sécurité de l'État membre concerné peuvent être qualifiés d'« autorités compétentes », au sens de l'article 7, paragraphe 2, de cette directive.

249 S’agissant des doutes émis par le gouvernement belge quant à la compétence de la Cour pour répondre à la septième question préjudicielle, il convient de noter que, selon les termes de cette question, la juridiction de renvoi interroge la Cour sur l’interprétation de l’article 12, paragraphe 3, de la directive PNR et non pas sur la compatibilité de la législation nationale avec cette disposition. En tout état de cause, il est de jurisprudence constante que la Cour peut fournir des indications aux juridictions nationales, permettant à celles-ci d’apprécier cette compatibilité (voir, notamment, arrêt du 7 septembre 2016, ANODE, C-121/15, EU:C:2016:637, point 54 et jurisprudence citée).

---

250 Voir, à cet égard, arrêt du 5 novembre 2019, Commission/Pologne (Indépendance des juridictions de droit commun) (C-192/18, EU:C:2019:924, points 108 à 110).

---

251 L’article 9, paragraphe 2, quatrième phrase, de la proposition de directive PNR disposait que « [l’]accès à l’intégralité des données PNR n’est autorisé que par le responsable de l’unité de renseignements passager ».

---

252 Arrêt Prokuratuur, points 52 et 53.

---

253 Arrêt Prokuratuur, points 53 et 54. Dans le même sens, voir arrêt Big Brother Watch , § 349 à 352.

---

254 L’article 9, paragraphe 2, quatrième phrase, de la proposition de directive PNR disposait que « [l’]accès à l’intégralité des données PNR n’est autorisé que par le responsable de l’unité de renseignements passager ».

---

255 Loi PNR, article 29, § 1 et 2.

---

256 Voir considérant 10 de la directive PNR.

---

257 Règlement (UE) 2016/399 du Parlement européen et du Conseil, du 9 mars 2016, concernant un code de l’Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO 2016, L 77, p. 1, ci-après le « code frontières Schengen »).

---

258 L’article 23, sous a), du code frontières Schengen prévoit que l’exercice des compétences de police ne peuvent être considérées comme équivalant à l’exercice des vérifications aux frontières lorsque les mesures de police « i) n’ont pas pour objectif le contrôle aux frontières ; ii) sont fondées sur des informations générales et l’expérience des services de police relatives à d’éventuelles menaces pour la sécurité publique et visent, notamment, à lutter contre la criminalité transfrontalière ; iii) sont conçues et exécutées d’une manière clairement distincte des vérifications systématiques effectuées sur les personnes aux frontières extérieures ; iv) sont réalisées sur la base de vérifications réalisées à l’impro ».

---

259 Voir, par analogie, arrêt du 13 décembre 2018, Touring Tours und Travel et Sociedad de transportes (C-412/17 et C-474/17, EU:C:2018:1005, point 61 et jurisprudence citée), ainsi que ordonnance du 4 juin 2020, FU (C-554/19, non publiée, EU:C:2020:439, points 51 à 56).

---

260 À cet égard, je relève que, au point 188 de l’avis 1/15, la Cour a affirmé que « l’identification, au moyen des données PNR, des passagers susceptibles de présenter un risque pour la sécurité publique fait partie des contrôles aux frontières ».

---

261 Voir arrêt du 13 décembre 2018, Touring Tours und Travel et Sociedad de transportes (C-412/17 et C-474/17, EU:C:2018:1005, point 51 et jurisprudence citée).

---

262 Voir, en ce sens, notamment, ordonnance du 4 juin 2020, FU (C-554/19, non publiée, EU:C:2020:439, point 46).

---

263 Dans son document de travail de 2020 sur la directive API (p. 20), la Commission souligne également le caractère problématique d’une superposition des systèmes de traitement des données PNR et API au niveau national.

---

264 C-411/17, EU:C:2019:622, points 175, 176, 179 et 181.

---

265 Voir arrêt La Quadrature du Net, points 217 à 219.