CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. Philippe LÉGER
présentées le 22 novembre 2005

Table des matières

Page

Affaire C-317/04

Parlement européen
contre
Conseil de l'Union européenne

«Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Recours en annulation – Décision 2004/496/CE du Conseil – Accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR ('Passenger Name Records')»

Affaire C-318/04

Parlement européen
contre
Commission des Communautés européennes

«Recours en annulation – Décision 2004/535/CE de la Commission, 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 – Directive 95/46/CE»

1. Le Parlement européen a saisi la Cour de deux recours en annulation en vertu de l'article 230 CE. Dans l'affaire Parlement/Conseil (C-317/04), le recours vise à l'annulation de la décision 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 (2). Dans l'affaire Parlement/Commission (C-318/04), le Parlement demande l'annulation de la décision 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 (3).

2. Ces deux affaires invitent la Cour à se prononcer sur la problématique relative à la protection des données à caractère personnel des passagers aériens dès lors que, pour justifier leur transfert et leur traitement dans un pays tiers, en l'occurrence les États-Unis (4), sont invoqués des impératifs tenant à la sécurité publique et relevant du domaine pénal, tels que la prévention et le combat contre le terrorisme et d'autres crimes graves.

3. Ces deux affaires trouvent leur origine dans une série d'évènements qu'il convient dès à présent d'exposer. Nous détaillerons ensuite le cadre juridique dans lequel elles s'inscrivent.

I – Les antécédents du litige

4. Au lendemain des attaques terroristes du 11 septembre 2001, les États-Unis ont adopté une législation disposant que les transporteurs aériens assurant des liaisons à destination, au départ ou à travers le territoire des États-Unis sont tenus de fournir aux autorités douanières américaines un accès électronique aux données contenues dans leurs systèmes automatiques de réservation et de contrôle des départs, dénommées «Passenger Name Records» (ci-après les «PNR») (5). Tout en reconnaissant la légitimité des intérêts de sécurité en jeu, la Commission des Communautés européennes a informé les autorités des États-Unis, dès le mois de juin 2002, que ces dispositions pouvaient entrer en conflit avec la législation communautaire et celle des États membres en matière de protection des données à caractère personnel, ainsi qu'avec certaines dispositions du règlement sur l'utilisation de systèmes informatisés de réservation (SIR) (6). Les autorités des États-Unis ont reporté l'entrée en vigueur des nouvelles dispositions, mais ont refusé de renoncer à imposer des sanctions aux compagnies aériennes qui ne se conformeraient pas auxdites dispositions après le 5 mars 2003. Depuis lors, plusieurs grandes compagnies aériennes établies dans des États membres ont fourni aux autorités américaines l'accès à leurs PNR.

5. La Commission a entamé avec les autorités américaines des négociations qui ont donné lieu à l'élaboration d'un document contenant des engagements de la part du CBP, en vue de l'adoption d'une décision de la Commission ayant pour objet de constater le caractère adéquat du niveau de protection des données à caractère personnel offert par les États-Unis, sur la base de l'article 25, paragraphe 6, de la

directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (7).

6. Le 13 juin 2003, le groupe dit «article 29» sur la protection des données (8) a rendu un avis dans lequel il a exprimé des doutes quant au niveau de protection garanti par ces engagements pour les traitements de données envisagés (9). Il a réitéré ses doutes dans un autre avis du 29 janvier 2004 (10).

7. Le 1er mars 2004, la Commission a saisi le Parlement du projet de décision d'adéquation, assorti du projet de la déclaration d'engagement du CBP.

8. Le 17 mars 2004, la Commission a transmis au Parlement, dans la perspective de la consultation de ce dernier au titre de l'article 300, paragraphe 3, premier alinéa, CE, une proposition de décision du Conseil de l'Union européenne concernant la conclusion d'un accord entre la Communauté et les États-Unis. Par lettre du 25 mars 2004, le Conseil a demandé, en se référant à la procédure d'urgence prévue à l'article 112 du règlement du Parlement (devenu depuis article 134), l'avis du Parlement sur cette proposition pour le 22 avril 2004 au plus tard. Dans sa lettre, le Conseil souligne que «[l]a lutte contre le terrorisme, qui justifie les mesures proposées, est une priorité essentielle de l'Union européenne. Actuellement, les transporteurs aériens et les passagers sont dans une situation d'incertitude à laquelle il convient de remédier d'urgence. En plus, il est essentiel de protéger les intérêts financiers des parties concernées».

9. Le 31 mars 2004, en application de l'article 8 de la décision du Conseil, du 28 juin 1999, fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission (11), le Parlement a adopté une résolution qui exprime un certain nombre de réserves d'ordre juridique sur cette approche. En particulier, le Parlement a considéré que le projet de décision d'adéquation excédait les compétences conférées à la Commission par l'article 25 de la directive 95/46. Il a appelé à la conclusion d'un accord international approprié respectant les droits fondamentaux, et a demandé à la Commission de lui soumettre un nouveau projet de décision. Il s'est, en outre, réservé le droit de saisir la Cour pour lui demander de vérifier la légalité de l'accord international envisagé et, en particulier, la compatibilité de celui-ci avec la protection du droit au respect de la vie privée.

10. Le 21 avril 2004, le Parlement a entériné, à la demande de son président, une recommandation de la commission juridique et du marché intérieur tendant à demander à la Cour un avis sur la compatibilité de l'accord envisagé avec le traité, conformément à l'article 300, paragraphe 6, CE, procédure qui a été entamée le jour même. Le Parlement a également décidé, à la même date, le renvoi en commission du rapport sur la proposition de décision du Conseil, rejetant ainsi implicitement, à ce stade, la demande d'urgence du Conseil en date du 25 mars 2004.

11. Le 28 avril 2004, le Conseil, en se fondant sur l'article 300, paragraphe 3, premier alinéa, CE, a adressé une lettre au Parlement lui demandant de rendre son avis sur la conclusion de l'accord avant le 5 mai 2004. Pour justifier l'urgence, le Conseil a repris les motifs indiqués dans sa lettre du 25 mars 2004 (12).

12. Le 30 avril 2004, le greffier de la Cour a informé le Parlement que celle-ci avait fixé au 4 juin 2004 le délai pour le dépôt des observations des États membres, du Conseil et de la Commission dans la demande d'avis 1/04.

13. Le 4 mai 2004, le Parlement a rejeté la demande d'urgence que le Conseil lui avait soumise le 28 avril (13). Le surlendemain, le président du Parlement s'est adressé au Conseil et à la Commission pour leur demander de ne pas poursuivre dans leurs intentions tant que la Cour n'aurait pas rendu l'avis sollicité le 21 avril 2004.

14. Le 14 mai 2004, la Commission a adopté la décision relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des

passagers aériens transférés au CBP, conformément à l'article 25, paragraphe 6, de la directive 95/46.

15. Le 17 mai 2004, le Conseil a adopté la décision concernant la conclusion d'un accord entre la Communauté et les États-Unis sur le traitement et le transfert de données PNR par des transporteurs aériens au CBP.

16. Par lettre du 9 juillet 2004, le Parlement a informé la Cour du retrait de sa demande d'avis 1/04 (14). Il a ensuite décidé de donner une suite contentieuse aux différends l'opposant au Conseil et à la Commission.

II – Le cadre juridique des deux affaires

A – *Le traité UE*

17. Aux termes de l'article 6 UE:

«1. L'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et des libertés fondamentales, ainsi que de l'État de droit, principes qui sont communs aux États membres.

2. L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, en tant que principes généraux du droit communautaire.

[…]»

B – *Le traité instituant la Communauté européenne*

18. L'article 95, paragraphe 1, CE dispose:

«Par dérogation à l'article 94 et sauf si le présent traité en dispose autrement, les dispositions suivantes s'appliquent pour la réalisation des objectifs énoncés à l'article 14. Le Conseil, statuant conformément à la procédure visée à l'article 251 et après consultation du Comité économique et social, arrête les mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur

19. S'agissant de la procédure de conclusion d'accords internationaux par la Communauté, l'article 300, paragraphe 2, premier alinéa, CE, prévoit à sa première phrase que «[s]ous réserve des compétences reconnues à la Commission dans ce domaine, la signature […] ainsi que la conclusion des accords sont décidées par le Conseil, statuant à la majorité qualifiée sur proposition de la Commission».

20. L'article 300, paragraphe 3, CE est ainsi rédigé:

«Le Conseil conclut les accords après consultation du Parlement européen, sauf pour les accords visés à l'article 133, paragraphe 3, y compris lorsque l'accord porte sur un domaine pour lequel la procédure visée à l'article 251 ou celle visée à l'article 252 est requise pour l'adoption de règles internes. Le Parlement européen émet son avis dans un délai que le Conseil peut fixer en fonction de l'urgence. En l'absence d'avis dans ce délai, le Conseil peut statuer.

Par dérogation aux dispositions de l'alinéa précédent, sont conclus après avis conforme du Parlement européen les accords visés à l'article 310, ainsi que les autres accords qui créent un cadre institutionnel spécifique en organisant des procédures de coopération, les accords ayant des implications budgétaires notables pour la Communauté et les accords impliquant une modification d'un acte adopté selon la procédure visée à l'article 251.

Le Conseil et le Parlement européen peuvent, en cas d'urgence, convenir d'un délai pour l'avis conforme.»

C – *Le droit européen de la protection des données à caractère personnel*

21. L'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la «CEDH») dispose:

«1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.»

22. Le droit européen de la protection des données s'est d'abord dessiné dans le cadre du Conseil de l'Europe. La convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a ainsi été ouverte à la signature des États membres du Conseil de l'Europe, à Strasbourg, le 28 janvier 1981 (15). Son but est de garantir, sur le territoire de chaque Partie contractante, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant.

23. Pour ce qui concerne l'Union européenne, outre son article 7 qui est relatif au respect de la vie privée et familiale, l'article 8 de la charte des droits fondamentaux de l'Union européenne (16) est spécifiquement consacré à la protection des données à caractère personnel. Il est ainsi rédigé:

«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.»

24. S'agissant du droit communautaire primaire, l'article 286 CE prévoit, à son paragraphe 1, que, «[à] partir du 1er janvier 1999, les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes institués par le présent traité ou sur la base de celui-ci» (17).

25. En droit communautaire dérivé, la norme de base en la matière est la directive 95/46 (18). Sa filiation avec les textes issus du Conseil de l'Europe ressort explicitement des dixième et onzième considérants de ladite directive. Son dixième considérant énonce, en effet, que «l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et

libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la [CEDH] et dans les principes généraux du droit communautaire; […] pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté». De plus, le onzième considérant de la directive 95/46 indique que «les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention [n° 108]».

26. Adoptée sur la base de l'article 100 A du traité CE (devenu, après modification, article 95 CE), la directive 95/46 trouve son origine dans l'idée exprimée à son troisième considérant, aux termes duquel «l'établissement et le fonctionnement du marché intérieur […] nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés». Plus précisément, le législateur communautaire est parti du constat selon lequel «les différences entre États membres quant au niveau de protection des droits et libertés des personnes, notamment du droit à la vie privée, à l'égard des traitements de données à caractère personnel peuvent empêcher la transmission de ces données du territoire d'un État membre à celui d'un autre État membre» (19), ce qui peut notamment avoir pour effet de faire obstacle à l'exercice d'activités à l'échelle communautaire et de fausser la concurrence. Aussi, le législateur communautaire a-t-il considéré que «pour éliminer les obstacles à la circulation des données à caractère personnel, le niveau de protection des droits et libertés des personnes à l'égard du traitement de ces données doit être équivalent dans tous les États membres» (20). Cette approche doit avoir pour résultat que, «du fait de la protection équivalente résultant du rapprochement des législations nationales, les États membres ne pourront plus faire obstacle à la libre circulation entre eux de données à caractère personnel pour des raisons relatives à la protection des droits et libertés des personnes, notamment du droit à la vie privée» (21).

27. L'article 1er de la directive 95/46, intitulé «Objet de la directive», met en œuvre cette approche en ces termes:

«1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

2. Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.»

28. L'article 2 de ladite directive définit, notamment, les notions de «données à caractère personnel», de «traitement de données à caractère personnel» et de «responsable du traitement».

29. Ainsi, aux termes de l'article 2, sous a), de la directive 95/46, constituent des données à caractère personnel «toute information concernant une personne physique identifiée ou identifiable […]; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale».

30. Un traitement de telles données recouvre, selon l'article 2, sous b), de ladite directive, «toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction».

31. L'article 2, sous d), de la directive 95/46 définit le responsable du traitement comme étant «la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel […]».

32. Quant au champ d'application matériel de la directive 95/46, l'article 3, paragraphe 1, prévoit que celle-ci «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».

33. L'article 3, paragraphe 2, de ladite directive permet de connaître une des limites du champ d'application matériel de celle-ci dans la mesure où il dispose que:

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

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

[…]»

34. Le chapitre II de la directive 95/46 est consacré aux «[c]onditions générales de licéité des traitements de données à caractère personnel». À l'intérieur de ce chapitre, la section I porte sur les «[p]rincipes relatifs à la qualité des données». L'article 6 de cette directive énumère ces principes dits de loyauté, de licéité, de finalité, de proportionnalité et d'exactitude des traitements de données à caractère personnel. Il est ainsi rédigé:

«1. Les États membres prévoient que les données à caractère personnel doivent être:

a) traitées loyalement et licitement;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités […];

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

d) exactes et, si nécessaire, mises à jour […];

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement […].

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1.»

35. La section II du chapitre II de ladite directive est, quant à elle, consacrée aux «[p]rincipes relatifs à la légitimation des traitements de données». L'article 7 formant cette section se lit comme suit:

«Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si:

a) la personne concernée a indubitablement donné son consentement

ou

b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci

ou

c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis

[…]»

36. S'agissant des données à caractère personnel communément qualifiées de «sensibles», l'article 8, paragraphe 1, énonce le principe de l'interdiction de leur traitement. Il prévoit, en effet, que «[l]es États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.» Ce principe d'interdiction connaît toutefois plusieurs exceptions dont le contenu et le régime sont détaillés dans les paragraphes suivants du même article.

37. Aux termes de l'article 13, paragraphe 1, de la directive 95/46, intitulé «Exceptions et limitations»:

«Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

a) la sûreté de l'État;

b) la défense;

c) la sécurité publique;

d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;

e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;

f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);

g) la protection de la personne concernée ou des droits et libertés d'autrui.»

38. Le législateur communautaire a également souhaité que le régime protecteur ainsi établi ne soit pas mis à mal dès lors que les données à caractère personnel sortent du territoire communautaire. Il est en effet apparu que la dimension internationale des flux d'informations (22) rendrait insuffisante, sinon inutile, l'existence d'une réglementation dont l'effectivité couvrirait ce seul territoire. Le législateur communautaire a donc opté pour un système requérant, pour admettre un transfert de données à caractère personnel vers un pays tiers, que ledit pays assure à ces données un «niveau de protection adéquat».

39. Le législateur communautaire pose ainsi la règle selon laquelle «lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit» (23).

40. Dans cette perspective, l'article 25 de la directive 95/46 pose les principes auxquels sont soumis les transferts de données à caractère personnel vers des pays tiers:

«1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

3. Les États membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2.

4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause.

5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.

6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

Les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.»

41. Enfin, il convient d'indiquer que, dans le cadre du titre VI du traité UE, qui est relatif à la coopération policière et judiciaire en matière pénale, la protection des données à caractère personnel est régie par différents instruments spécifiques. Il s'agit notamment d'instruments qui instaurent des systèmes d'information communs au niveau européen, tels que la convention d'application de l'Accord de Schengen (24) qui contient des dispositions spécifiques sur la protection des données dans le cadre du système d'information Schengen (SIS) (25); la convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un office européen de police (26); la décision du Conseil créant Eurojust (27) et les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel (28); la convention établie sur la base de l'article K.3 du traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, qui contient des dispositions relatives à la protection des données à caractère personnel applicables au système d'information des douanes (29), et la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (30).

42. Le 4 octobre 2005, la Commission a présenté une proposition de décision-cadre du Conseil, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (31).

III – Les décisions attaquées

43. Nous examinerons les deux décisions attaquées dans l'ordre chronologique de leur adoption.

A – *La décision d'adéquation*

44. La décision d'adéquation a été adoptée par la Commission sur la base de l'article 25, paragraphe 6, de la directive 95/46, qui, rappelons-le, lui confère le pouvoir de constater qu'un pays tiers assure un niveau de protection adéquat des données à caractère personnel (32). Ainsi que le mentionne le deuxième considérant de cette décision, «[s]ur la base de ce constat, des données à caractère personnel peuvent être transférées à partir des États membres sans qu'aucune garantie supplémentaire ne soit nécessaire».

45. Au onzième considérant de ladite décision, la Commission indique que «[l]e traitement par le CBP des données à caractère personnel contenues dans les PNR des passagers aériens qui lui sont transférés est régi par les dispositions figurant dans la 'Déclaration d'engagement du Bureau des douanes et de la protection des frontières du ministère de la Sécurité intérieure du 11 mai 2004' et par la législation américaine dans les conditions prévues par la déclaration d'engagement». Aussi, la Commission constate-t-elle au quatorzième considérant de la même décision que «[l]es normes en vertu desquelles le CBP traite les données PNR des passagers sur la base de la législation américaine et de la déclaration d'engagement respectent les principes essentiels nécessaires pour assurer un niveau de protection adéquat des personnes physiques».

46. En conséquence, l'article 1er de la décision d'adéquation dispose:

«Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, [le CBP] est considéré comme assurant un niveau de protection adéquat des données de dossiers passagers [...] transférées depuis la Communauté en ce qui concerne les vols à destination ou au départ des États-Unis, conformément à la déclaration d'engagement figurant en annexe».

47. En outre, l'article 3 de la décision d'adéquation prévoit que le transfert de données vers le CBP peut être suspendu à l'initiative des autorités compétentes des États membres dans les conditions suivantes:

«1. Sans préjudice des pouvoirs leur permettant de prendre des mesures pour assurer le respect des dispositions nationales adoptées conformément aux dispositions autres que l'article 25 de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent actuellement pour suspendre le transfert de données vers le CBP afin de protéger les personnes physiques à l'égard du traitement des données à caractère personnel qui les concernent dans l'un des deux cas suivants:

a) lorsqu'une autorité américaine compétente a constaté que le CBP ne respecte pas les normes applicables en matière de protection;

b) lorsqu'il est probable que les normes de protection établies en annexe ne sont pas respectées, qu'il y a tout lieu de croire que le CBP ne prend pas ou ne prendra pas, en temps voulu, les mesures qui s'imposent pour régler l'affaire en question, que la poursuite du transfert entraînerait un risque imminent de grave préjudice pour les personnes concernées et que les autorités compétentes de l'État membre se sont raisonnablement efforcées, dans ces circonstances, d'avertir le CBP et de lui donner la possibilité de répondre.

2. La suspension du transfert cesse dès que les normes de protection sont assurées et que les autorités compétentes dans les États membres concernés en sont averties.»

48. Les États membres sont tenus d'informer la Commission des mesures prises conformément à l'article 3 de la décision d'adéquation. Par ailleurs, les États membres et la Commission doivent, en vertu de l'article 4, paragraphe 2, de cette décision, s'informer mutuellement de tout changement dans les normes de protection et des cas dans lesquels ces normes apparaîtraient insuffisamment respectées. Suite à ces échanges, l'article 4, paragraphe 3, de la décision d'adéquation prévoit que «[s]i les informations recueillies conformément à l'article 3 et aux paragraphes 1 et 2 du présent article montrent que les principes essentiels nécessaires pour assurer un niveau de protection adéquat des personnes physiques ne sont plus respectés, ou qu'un quelconque organisme chargé de veiller au respect par le CBP des normes de protection établies en annexe ne remplit pas efficacement sa mission, le CBP sera informé et, si nécessaire, la procédure prévue à l'article 31, paragraphe 2, de la directive 95/46/CE sera applicable en vue d'annuler ou de suspendre la présente décision».

49. Par ailleurs, l'article 5 de la décision d'adéquation pose la règle selon laquelle la mise en œuvre de cette dernière fera l'objet d'une évaluation et prévoit que «toute constatation pertinente sera rapportée au comité institué par l'article 31 de la directive 95/46/CE».

50. En outre, l'article 7 de la décision d'adéquation indique que celle-ci «vient à échéance trois ans et six mois à compter de sa notification, à moins qu'elle ne soit prolongée conformément à la procédure prévue à l'article 31, paragraphe 2, de la directive 95/46/CE».

51. En annexe de ladite décision est jointe la déclaration d'engagement du CBP, laquelle précise dans son introduction qu'elle a pour objet de «soutenir le projet» de la Commission tendant à reconnaître l'existence d'un niveau de protection adéquat des données transférées au CBP. Selon ses termes, cette déclaration, qui comporte au total 48 paragraphes, «ne crée ni ne confère aucun droit ni aucun avantage pour toute personne ou partie, qu'elle soit privée ou publique» (33).

52. Nous indiquerons, en substance, au fil de nos développements, le contenu des engagements pertinents pour la solution du litige.

53. Enfin, la décision d'adéquation contient une annexe «A» qui procède à l'énumération des 34 rubriques des données PNR demandées par le CBP aux compagnies aériennes (34).

54. Cette décision de la Commission est complétée par la décision du Conseil de conclure un accord international entre la Communauté européenne et les États-Unis.

B – *La décision du Conseil*

55. La décision du Conseil a été adoptée sur le fondement de l'article 95, en liaison avec l'article 300, paragraphe 2, premier alinéa, première phrase, CE.

56. Son premier considérant indique que «[l]e Conseil a autorisé la Commission, le 23 février 2004, à négocier, au nom de la Communauté, un accord avec les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au [CBP]» (35). Le deuxième considérant de cette décision mentionne, quant à lui, que «[l]e Parlement européen n'a pas émis son avis dans le délai fixé, en vertu de l'article 300, paragraphe 3, premier alinéa, du traité, par le Conseil en vue de la nécessité urgente de remédier à la situation d'incertitude dans laquelle se trouvent les compagnies aériennes et les passagers et de protéger les intérêts financiers des parties concernées».

57. En vertu de l'article 1er de la décision du Conseil, l'accord est approuvé au nom de la Communauté. En outre, l'article 2 de ladite décision autorise le président du Conseil à désigner les personnes habilitées à signer l'accord au nom de la Communauté.

58. Le texte de l'accord est annexé à la décision du Conseil. L'article 7 dudit accord prévoit qu'il entre en vigueur dès sa signature. Conformément à cet article, l'accord, signé à Washington le 28 mai 2004, est entré en vigueur ce même jour (36).

59. Dans le préambule de l'accord, la Communauté et les États-Unis reconnaissent «qu'il importe de respecter les droits et libertés fondamentaux, et notamment le droit au respect de la vie privée, et de respecter ces valeurs, tout en prévenant et en combattant le terrorisme et les délits qui y sont liés, ainsi que d'autres délits graves de nature transnationale, notamment la criminalité organisée».

60. Les textes suivants sont visés dans le préambule de l'accord: la directive 95/46, et notamment son article 7, sous c), les engagements pris par le CBP ainsi que la décision d'adéquation (37).

61. Les Parties contractantes notent également que «les transporteurs aériens disposant de systèmes de contrôle des réservations et des départs et établis sur le territoire des États membres de la Communauté européenne doivent faire le nécessaire pour que les données PNR soient transmises au CBP dès que cela sera techniquement possible, mais que, d'ici-là, les autorités américaines devront pouvoir accéder directement aux données, en vertu des dispositions du présent accord» (38).

62. C'est ainsi que le paragraphe 1 de l'accord prévoit que «[l]e CBP peut accéder, par voie électronique, aux données PNR provenant des systèmes de contrôle des réservations et des départs des transporteurs aériens […] situés sur le territoire des États membres de la Communauté européenne, en application stricte de la décision [(39)] et aussi longtemps que cette dernière sera applicable, c'est-à-dire jusqu'à ce qu'un système satisfaisant soit mis en place pour permettre la transmission de ces données par les transporteurs aériens».

63. En complément du pouvoir ainsi accordé au CBP d'accéder directement aux données PNR, le paragraphe 2 de l'accord impose aux transporteurs aériens assurant un service de transport international de passagers à destination ou au départ des États-Unis de traiter les données PNR stockées dans leurs systèmes informatiques de réservation «comme demandé par le CBP en vertu de la législation américaine, en application stricte de la décision [(40)] et aussi longtemps que cette dernière est applicable».

64. Par ailleurs, au paragraphe 3 de l'accord, il est précisé que le CBP «prend note» de la décision d'adéquation et «déclare qu'il met en œuvre les engagements annexés à ladite décision». De plus, le paragraphe 4 dudit accord prévoit que «[l]e CBP traite les données PNR reçues et les personnes concernées par ce traitement conformément aux lois et exigences constitutionnelles américaines, sans discrimination, en particulier sur la base de la nationalité et du pays de résidence».

65. En outre, le CBP et la Communauté s'engagent à examiner conjointement et régulièrement la mise en œuvre de l'accord (41). Ce dernier prévoit également que «[e]n cas de mise en œuvre, dans l'Union européenne, d'un système d'identification des passagers aériens, dans le cadre duquel elle impose aux transporteurs aériens de donner aux autorités l'accès aux données PNR des passagers dont le voyage en cours inclut un vol à destination ou au départ de l'Union européenne, [le] DHS [Department of Homeland Security] encourage activement, autant que possible et dans le strict respect du principe de réciprocité, les compagnies aériennes relevant de sa compétence à coopérer» (42).

66. De plus, outre qu'il prévoit que l'accord entre en vigueur dès sa signature, le paragraphe 7 de celui-ci précise que chaque partie peut le dénoncer à tout moment.

Dans ce cas, l'accord cesse d'être applicable 90 jours après la date de la notification de la dénonciation à l'autre partie. Par ailleurs, il est prévu, dans le même paragraphe, que l'accord peut être modifié à tout moment d'un commun accord écrit.

67. Enfin, le paragraphe 8 de l'accord dispose que «[l]e présent accord n'a pas pour objet de déroger à la législation des parties ni de la modifier; il ne crée ni ne confère aucun droit ou avantage sur toute autre personne ou entité, privée ou publique».

IV – Les moyens soulevés par le Parlement dans les deux affaires

68. Dans l'affaire C-317/04, le Parlement soulève six moyens à l'encontre de la décision du Conseil:

– le choix erroné de l'article 95 CE comme base juridique;

– la violation de l'article 300, paragraphe 3, deuxième alinéa, CE, en raison d'une modification de la directive 95/46;

– la violation du droit à la protection des données à caractère personnel;

– la violation du principe de proportionnalité;

– l'insuffisante motivation de la décision litigieuse;

– la violation du principe de coopération loyale prévu à l'article 10 CE.

69. Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord ainsi que la Commission ont été admis à intervenir à l'appui des conclusions du Conseil (43). Par ailleurs, le contrôleur européen de la protection des données (ci-après le «CEPD») a été admis à intervenir au soutien des conclusions du Parlement (44).

70. Dans l'affaire C-318/04, le Parlement soulève quatre moyens à l'encontre de la décision d'adéquation:

– l'excès de pouvoir;

– la violation des principes essentiels de la directive 95/46;

– la violation des droits fondamentaux;

– la violation du principe de proportionnalité.

71. Le Royaume-Uni a été admis à intervenir à l'appui des conclusions de la Commission (45). En outre, le CEPD a été admis à intervenir au soutien des conclusions du Parlement (46).

72. Nous analyserons les deux recours dans l'ordre selon lequel les décisions attaquées ont été adoptées. Nous examinerons donc, en premier lieu, le recours visant à l'annulation de la décision d'adéquation (affaire C-318/04) puis, en second lieu, celui visant à l'annulation de la décision du Conseil (affaire C-317/04).

V – Sur le recours visant à l'annulation de la décision d'adéquation (affaire C-318/04)

A – *Sur le moyen tiré de ce que la Commission aurait commis un excès de pouvoir en adoptant la décision d'adéquation*

1. Arguments des parties

73. À l'appui de ce moyen, le Parlement soutient, en premier lieu, que la décision d'adéquation, en tant qu'elle vise la réalisation d'un but qui relève de la sécurité publique et du droit pénal, viole la directive 95/46 puisqu'elle concerne un domaine exclu du champ d'application ratione materiae de ladite directive. Cette exclusion serait prévue de manière expresse à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 et ne se prêterait à aucune interprétation pouvant en réduire la portée. Le fait que les données à caractère personnel aient été collectées lors de l'exercice d'une activité économique, à savoir la vente d'un ticket d'avion donnant droit à une prestation de services, ne pourrait pas justifier l'application de ladite directive, et notamment de son article 25, dans un domaine exclu de son champ d'application.

74. En deuxième lieu, le Parlement fait valoir que le CBP n'est pas un pays tiers au sens de l'article 25 de la directive 95/46. Or, cet article, à son paragraphe 6, prescrirait qu'une décision de la Commission constatant un niveau adéquat de protection des données à caractère personnel ait trait à un «pays tiers», c'est-à-dire un État ou une entité assimilée, et non une unité ou composante administrative faisant partie du pouvoir exécutif d'un État.

75. En troisième lieu, le Parlement considère que l'adoption par la Commission de la décision d'adéquation constitue un excès de pouvoir dans la mesure où la déclaration d'engagement qui y est annexée permet expressément la transmission par le CBP de données PNR à d'autres autorités gouvernementales américaines ou étrangères.

76. En quatrième lieu, le Parlement estime que la décision d'adéquation implique certaines limitations et exceptions aux principes figurant dans la directive 95/46 alors que l'article 13 de celle-ci réserve ce pouvoir uniquement aux États membres. Ainsi, en adoptant la décision d'adéquation, la Commission se serait substituée aux États membres et aurait méconnu, de ce fait, l'article 13 de ladite directive. Par un acte d'exécution de la directive 95/46, la Commission se serait arrogé des compétences strictement réservées aux États membres.

77. En cinquième lieu, le Parlement développe l'argument selon lequel la mise à disposition des données effectuée par le biais du système «pull» (extraction) ne constituerait pas un «transfert» au sens de l'article 25 de la directive 95/46, et ne pourrait donc pas être admise.

78. En dernier lieu, compte tenu de l'interdépendance entre la décision d'adéquation et l'accord, ladite décision devrait, selon cette institution, être considérée comme une mesure non appropriée en vue d'imposer les transferts de données PNR.

79. À la différence du Parlement, le CEPD estime que le fait de donner accès aux données à une personne ou à une institution d'un pays tiers peut être considéré comme étant constitutif d'un transfert et que, dès lors, l'article 25 de la directive 95/46 est applicable. Il considère, en effet, que limiter la notion à un transfert réalisé par l'envoyeur permettrait d'éluder les conditions posées par cet article et porterait ainsi préjudice à la protection des données prévue audit article.

80. La Commission, soutenue par le Royaume-Uni, est d'avis que les activités des transporteurs aériens entrent dans le champ d'application du droit communautaire et que, en conséquence, la directive 95/46 reste entièrement applicable. Le régime mis en place dans le cadre du transfert de données PNR n'aurait pas pour objet les activités d'un État membre ou d'autorités publiques tombant hors du champ d'application du droit communautaire.

81. En outre, la Commission relève que l'accord a été signé au nom des États-Unis et non pas au nom d'un service gouvernemental. En ce qui concerne les transferts

ultérieurs des données PNR par le CBP, la Commission estime que la protection des données à caractère personnel n'est pas incompatible avec l'autorisation de tels transferts à condition que ceux-ci soient soumis aux restrictions appropriées et nécessaires.

82. Enfin, la Commission observe que l'article 13 de la directive 95/46 n'est pas pertinent dans la présente affaire et que le «transfert», au sens de l'article 25 de cette directive, consiste, pour les transporteurs aériens, à mettre activement les données PNR à la disposition du CBP. Le système examiné comporterait donc bien un transfert de données au sens de la directive 95/46.

2. Appréciation

83. Par ce premier moyen, le Parlement soutient que la décision d'adéquation constitue une violation de la directive 95/46, et particulièrement des articles 3, paragraphe 2, 13 et 25 de celle-ci. Il fait notamment valoir que cette décision ne pouvait pas être valablement fondée sur l'acte de base que constitue ladite directive.

84. Comme nous l'avons déjà exposé, la directive 95/46 a pour but, en vue de l'établissement et du fonctionnement du marché intérieur, d'éliminer les obstacles à la libre circulation des données à caractère personnel en rendant équivalent dans les États membres le niveau de protection des droits et libertés des personnes à l'égard du traitement de telles données.

85. Le législateur communautaire a également souhaité que le régime protecteur ainsi instauré ne soit pas mis en péril dès lors que les données à caractère personnel sortent du territoire communautaire. Il a donc opté pour un système requérant, pour admettre qu'un transfert de données à caractère personnel vers un pays tiers puisse être réalisé, que ledit pays assure à ces données un niveau de protection adéquat. Ainsi, la directive 95/46 contient le principe selon lequel lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit.

86. L'article 25 de ladite directive impose une série d'obligations aux États membres et à la Commission visant à contrôler les transferts de données à caractère personnel vers des pays tiers compte tenu du niveau de protection accordé à de telles données dans chacun de ces pays. Il prévoit également la méthode et les critères permettant de considérer qu'un pays tiers assure un niveau de protection adéquat des données à caractère personnel qui lui sont transférées.

87. La Cour a qualifié le régime relatif au transfert de données à caractère personnel vers des pays tiers de «régime spécial, comportant des règles spécifiques, qui vise à assurer un contrôle par les États membres des transferts de données à caractère personnel vers les pays tiers». Elle a également précisé qu'il s'agit d'«un régime complémentaire au régime général mis en place par le chapitre II de ladite directive concernant la licéité de traitements de données à caractère personnel» (47).

88. La spécificité des règles qui encadrent le transfert de données à caractère personnel vers les pays tiers s'explique en grande partie par le rôle clé que joue la notion de protection adéquate. Afin de cerner la portée de cette notion, il convient de clairement la distinguer de la notion de protection équivalente qui, elle, exigerait que le pays tiers reconnaisse et applique effectivement l'ensemble des principes contenus dans la directive 95/46.

89. La notion de protection adéquate signifie que le pays tiers doit être en mesure de garantir une protection adaptée, selon un modèle qui est jugé acceptable en termes de degré de protection des données à caractère personnel. Un tel système fondé sur le caractère adéquat de la protection assurée par un pays tiers laisse une marge d'appréciation importante aux États membres et à la Commission dans leur évaluation des garanties mises en place dans le pays de destination des données. Cette appréciation est guidée par l'article 25, paragraphe 2, de la directive 95/46, qui

énumère certains des facteurs pouvant entrer en considération aux fins de cette évaluation (48). Dans cette perspective, la règle posée par le législateur communautaire est que «[l]e caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données».

90. Ainsi que la Cour l'a déjà constaté, la directive 95/46 ne définit pas la notion de «transfert vers un pays tiers» (49). Elle ne précise notamment pas si la notion recouvre seulement l'action par laquelle un responsable de traitement communique activement des données à caractère personnel vers un pays tiers ou bien si elle s'étend au cas dans lequel une entité d'un pays tiers est autorisée à avoir accès à des données situées dans un État membre. Cette directive est donc muette sur le point de savoir selon quelle méthode un transfert de données vers un pays tiers peut être effectué.

91. Contrairement au Parlement, nous estimons que, dans la présente affaire, l'accès aux données PNR dont bénéficie le CBP relève de la notion de «transfert vers un pays tiers». En effet, ce qui est déterminant pour caractériser un tel transfert est, selon nous, la circulation des données depuis un État membre à destination d'un pays tiers, en l'occurrence les États-Unis (50). Peu importe à cet égard que le transfert soit effectué par l'envoyeur ou par le récepteur. En effet, ainsi que le précise le CEPD, si la portée de l'article 25 de la directive 95/46 était limitée aux transferts réalisés par l'envoyeur, il serait aisé d'éluder les conditions posées par cet article.

92. Ceci étant précisé, il convient toutefois d'insister sur le fait que le chapitre IV de ladite directive, dans lequel figure ledit article 25, n'est pas destiné à régir *tous* les transferts de données à caractère personnel, de quelque nature qu'ils soient, vers des pays tiers. Il ne couvre, aux termes de l'article 25, paragraphe 1, de la directive, que le transfert de données à caractère personnel «*faisant l'objet d'un traitement*, ou destinées *à faire l'objet d'un traitement* après leur transfert».

93. Nous rappelons à cet égard que, aux termes de l'article 2, sous b), de la directive 95/46, est constitutif d'un traitement de données à caractère personnel «toute opération ou ensemble d'opérations [...] appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, [...] la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition [...]» (51).

94. Quelle que soit sa spécificité, laquelle repose largement, comme nous l'avons vu, sur la notion d'adéquation, le régime relatif au transfert de données à caractère personnel vers des pays tiers est soumis au respect des règles relatives au champ d'application de la directive 95/46 dont il fait partie (52).

95. Aussi, pour être couvert par les dispositions de l'article 25 de la directive 95/46, un transfert vers un pays tiers doit-il concerner des données à caractère personnel dont le traitement, qu'il soit actuellement mis en œuvre au sein de la Communauté ou seulement envisagé dans le pays tiers, entre dans le champ d'application de ladite directive. C'est seulement à cette condition qu'une décision d'adéquation peut valablement constituer un acte d'exécution de la directive 95/46.

96. À cet égard, nous rappelons que, d'un point de vue ratione materiae, ladite directive ne s'applique pas à tous les traitements de données à caractère personnel susceptibles d'entrer dans l'une des catégories d'opérations visées à son article 2, sous b). En effet, l'article 3, paragraphe 2, premier tiret, de la directive 95/46 dispose que celle-ci ne s'applique pas aux traitements de données à caractère personnel qui sont «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*» (53).

97. Or, nous considérons que la consultation, l'utilisation par le CBP et la mise à la disposition de ce dernier des données des passagers aériens provenant des systèmes de réservation des transporteurs aériens situés sur le territoire des États membres constituent des traitements de données à caractère personnel qui ont pour objet la sécurité publique et qui concernent des activités étatiques relatives à des domaines du droit pénal. Ces traitements sont, par conséquent, exclus du champ d'application matériel de la directive 95/46.

98. Les termes utilisés dans la décision d'adéquation démontrent l'objet des traitements auxquels sont soumises les données à caractère personnel des passagers aériens. Ainsi, après avoir indiqué que les exigences de transfert vers le CBP des données à caractère personnel contenues dans les PNR des passagers aériens se fondent sur une loi promulguée par les États-Unis en novembre 2001 et sur des règlements de mise en œuvre adoptés par le CBP en vertu de cette loi (54), la Commission précise qu'un des objets de la législation américaine est «le renforcement de la sécurité» (55). Il est également indiqué que «[l]a Communauté soutient entièrement les États-Unis dans leur lutte contre le terrorisme, dans les limites imposées par le droit de la Communauté» (56).

99. De plus, le quinzième considérant de la décision d'adéquation dispose que «les données des PNR doivent être utilisées dans le but unique de prévenir et de combattre le terrorisme et les crimes liés au terrorisme, d'autres crimes graves, y compris la criminalité organisée, qui, par nature, revêtent un caractère transnational et la fuite en cas de mandat d'arrêt ou de mise en détention pour l'un des crimes susmentionnés».

100. La directive 95/46, et notamment son article 25, paragraphe 6, ne saurait, selon nous, constituer un fondement approprié pour l'adoption par la Commission d'un acte d'exécution tel qu'une décision relative au niveau de protection adéquat de données à caractère personnel faisant l'objet de traitements qui sont expressément exclus de son champ d'application. Autoriser, sur la base de ladite directive, les transferts de telles données reviendrait en effet à étendre, de façon détournée, le champ d'application de celle-ci.

101. Or, il convient d'avoir à l'esprit que la directive 95/46, adoptée sur le fondement de l'article 100 A du traité CE, définit des principes de protection qui doivent s'appliquer aux traitements de données à caractère personnel dès lors que les activités du responsable de traitement relèvent du champ d'application du droit communautaire, mais que, en raison même du choix de sa base juridique, elle n'est pas apte à régir des activités étatiques, telles que celles qui concernent la sécurité publique ou qui poursuivent des fins répressives, qui ne relèvent pas du champ d'application du droit communautaire (57).

102. Il est vrai que le traitement que constituent la collecte et l'enregistrement de données des passagers aériens par les compagnies aériennes a, en général, une finalité commerciale dans la mesure où il est directement lié au déroulement du vol assuré par le transporteur aérien. Aussi, est-il juste de considérer que les données PNR sont initialement collectées par les compagnies aériennes dans le cadre d'une activité qui relève du droit communautaire, à savoir la vente d'un billet d'avion qui donne droit à une prestation de services. Toutefois, le traitement des données qui est pris en compte dans la décision d'adéquation possède une nature tout autre, dans la mesure où il couvre un stade ultérieur à la collecte initiale des données. Il porte en effet, comme nous l'avons vu, sur la consultation, l'utilisation par le CBP et la mise à la disposition de ce dernier des données des passagers aériens provenant des systèmes de réservation des transporteurs aériens situés sur le territoire des États membres.

103. En réalité, la décision d'adéquation ne vise pas un traitement de données nécessaire à la réalisation d'une prestation de services, mais considéré comme nécessaire pour sauvegarder la sécurité publique et à des fins répressives. Telle est bien la finalité du transfert et du traitement dont font l'objet les données PNR. Par conséquent, le fait que les données à caractère personnel aient été collectées lors de l'exercice d'une activité économique ne peut pas, selon nous, justifier l'application de

la directive 95/46, et notamment l'article 25 de celle-ci, dans un domaine exclu de son champ d'application.

104. Ces éléments suffisent, selon nous, à considérer que, comme le pense le Parlement, la Commission ne disposait pas, en vertu de l'article 25 de la directive 95/46, du pouvoir d'adopter une décision relative au niveau de protection adéquat de données à caractère personnel transférées *dans le cadre* et *en vue* d'un traitement exclu expressément du champ d'application de ladite directive (58).

105. Cette décision d'adéquation est donc constitutive d'une violation de l'acte de base que constitue la directive 95/46, et notamment de son article 25 qui n'en est pas le fondement approprié. Nous estimons qu'elle doit, pour cette raison, être annulée

106. En outre, dans la mesure où nous considérons que la décision d'adéquation tombe hors du champ d'application de la directive 95/46, il ne nous paraît pas pertinent d'analyser, ainsi que l'invite le Parlement dans son deuxième moyen, cette décision au regard des principes essentiels contenus dans ladite directive (59). Nous estimons donc qu'il n'y a pas lieu d'examiner ce deuxième moyen.

107. Quant aux troisième et quatrième moyens du présent recours, que nous n'envisagerons qu'à titre subsidiaire, ils ne peuvent pas, à notre avis, faire l'objet d'une analyse séparée, car la vérification d'une violation éventuelle des droits fondamentaux par la décision d'adéquation comprend nécessairement une évaluation du respect du principe de proportionnalité par cet acte au regard de l'objectif qu'il poursuit. Nous proposons donc à la Cour d'examiner ensemble ces troisième et quatrième moyens.

B – *Sur les moyens tirés d'une violation des droits fondamentaux et d'une violation du principe de proportionnalité*

108. Le Parlement soutient que la décision d'adéquation ne respecte pas le droit à la protection des données à caractère personnel tel qu'il est garanti à l'article 8 de la CEDH. Plus précisément, au regard des conditions posées par cet article, il estime que ladite décision constitue une ingérence dans la vie privée qui ne peut être considérée comme prévue par la loi, car il s'agit d'une mesure qui n'est pas accessible et prévisible. En outre, le Parlement estime que cette mesure n'est pas proportionnée au but qu'elle poursuit, eu égard notamment au nombre excessif de rubriques des PNR demandées et à la durée de conservation excessivement longue des données.

109. Dans le recours qu'il a introduit dans l'affaire C-317/04, qui vise à l'annulation de la décision du Conseil, le Parlement invoque également ces deux moyens et développe à leur appui des arguments qui se recoupent en grande partie. Nous estimons que ces moyens soulevés dans les deux affaires soumises à la Cour doivent faire l'objet d'un examen unique qu'il nous paraît pertinent d'effectuer dans le cadre de nos développements consacrés à l'affaire C-317/04.

110. Il ressort en effet de l'argumentation développée par les parties dans leurs mémoires qu'il est impossible d'appréhender séparément, au regard du droit au respect de la vie privée, les composantes du régime relatif au traitement des données PNR par le CBP (60) que constituent l'accord tel qu'approuvé par la décision du Conseil, la décision d'adéquation et les engagements du CBP qui sont annexés à ladite décision de la Commission. Les parties renvoient d'ailleurs à maintes reprises à l'un ou à l'autre de ces actes afin d'asseoir leur démonstration.

111. L'interdépendance entre ces trois composantes du régime PNR ressort expressément des termes mêmes de l'accord. En effet, tant les engagements du CBP que la décision d'adéquation sont visés dans le préambule de l'accord. Ensuite, le paragraphe 1 de cet accord précise que le CBP peut accéder aux données PNR «en application stricte de la décision [d'adéquation] et aussi longtemps que cette dernière sera applicable […]». De même, si, selon le paragraphe 2 dudit accord, les transporteurs aériens qui y sont désignés doivent traiter les données PNR «comme

demandé par le CBP en vertu de la législation américaine», c'est encore «en application stricte de la décision [d'adéquation] et aussi longtemps que cette dernière est applicable». Enfin, le paragraphe 3 de l'accord dispose que «[l]e CBP prend note de la décision [d'adéquation] et déclare qu'il met en œuvre les engagements annexés à ladite décision».

112. Il résulte de ces éléments que le droit d'accès aux données PNR conféré par l'accord au CBP ainsi que l'obligation de traitement desdites données qui incombe aux transporteurs aériens désignés dans ledit accord sont soumis à l'application stricte et effective de la décision d'adéquation.

113. L'interdépendance entre les trois composantes du régime PNR, ainsi que le fait que les moyens tirés de la violation des droits fondamentaux et du principe de proportionnalité soient soulevés par le Parlement dans les deux affaires soumises au jugement de la Cour, nous conduisent à comprendre ces moyens comme visant à faire constater par cette dernière l'incompatibilité du régime PNR, dans ses trois composantes, avec le droit au respect de la vie privée garanti à l'article 8 de la CEDH. À notre avis, il serait en effet artificiel d'examiner la décision d'adéquation sans tenir compte de l'accord, qui fait peser certaines obligations sur les compagnies aériennes et, en sens inverse, d'examiner cet accord sans prendre en considération les autres textes applicables auxquels cet instrument fait expressément référence.

114. Compte tenu du fait que le système est composé de plusieurs éléments indissociables, l'analyse ne doit donc pas être artificiellement scindée.

115. L'ingérence dans la vie privée est, sous cet angle, constituée par l'ensemble que forment l'accord tel qu'approuvé par la décision du Conseil, la décision d'adéquation et les engagements du CBP. Afin d'examiner si cette ingérence est prévue par la loi, poursuit un but légitime et est nécessaire dans une société démocratique, il est également nécessaire de prendre en compte l'ensemble du mécanisme «à trois vitesses» ainsi mis sur pied, comme le fait le Parlement dans ses deux requêtes. Pour avoir une vue globale du régime PNR, nous procéderons à cet examen dans le cadre du recours visant à l'annulation de la décision du Conseil.

VI – Sur le recours visant à l'annulation de la décision du Conseil (affaire C-317/04)

A – *Sur le moyen tiré du choix erroné de l'article 95 CE comme base juridique de la décision du Conseil*

1. Arguments des parties

116. Le Parlement européen fait valoir que l'article 95 CE ne constitue pas la base juridique appropriée de la décision du Conseil. Celle-ci n'aurait pas, en effet, pour but et contenu l'établissement et le fonctionnement du marché intérieur. La décision du Conseil aurait plutôt pour objectif de légaliser le traitement de données à caractère personnel imposé par la législation américaine aux compagnies aériennes établies sur le territoire de la Communauté. Cette décision ne préciserait pas dans quelle mesure cette légalisation des transferts des données vers un pays tiers contribuerait à l'établissement ou au fonctionnement du marché intérieur.

117. Selon le Parlement, le contenu de la décision du Conseil ne justifierait pas non plus le recours à l'article 95 CE comme base juridique. Cette décision consisterait à établir le droit d'accès du CBP au système des réservations des compagnies aériennes sur le territoire de la Communauté, et ce en vue de la réalisation des vols entre les États-Unis et les États membres, conformément à la législation américaine, afin de prévenir et de lutter contre le terrorisme. Or, la réalisation de ces buts ne tomberait pas sous le coup de l'article 95 CE.

118. Enfin, le Parlement ajoute que l'article 95 CE ne serait pas susceptible de fonder la compétence de la Communauté pour conclure l'accord concerné dans la mesure où

celui-ci vise des traitements de données effectués à des fins de sécurité publique et donc exclus du champ d'application de la directive 95/46, basée sur ledit article du traité.

119. En revanche, le Conseil estime que sa décision a été correctement fondée sur l'article 95 CE. Selon lui, cet article peut fonder des mesures visant à assurer que les conditions de concurrence ne sont pas faussées dans le marché intérieur. Il soutient à cet égard que l'accord vise à supprimer toute distorsion de concurrence entre les compagnies aériennes des États membres et entre celles-ci et les compagnies des pays tiers, pouvant se produire, en raison des exigences américaines, pour des raisons relatives à la protection des droits et libertés des personnes. Les conditions de concurrence entre les compagnies des États membres assurant un service de transport international de passagers à destination ou au départ des États-Unis auraient pu être faussées si seulement certaines d'entre elles accordaient aux autorités américaines un accès à leurs bases de données.

120. Dans le même ordre d'idées, le Conseil souligne, d'une part, que les compagnies aériennes ne se conformant pas aux exigences américaines auraient pu se voir imposer le paiement d'amendes par les autorités américaines, subir des retards de leurs vols et perdre des passagers au profit d'autres compagnies aériennes ayant conclu des arrangements avec les États-Unis. D'autre part, certains États membres auraient pu sanctionner des compagnies aériennes transférant les données personnelles en cause, alors que d'autres États membres n'auraient pas nécessairement agi de la même manière.

121. Dans ces conditions, et en l'absence d'une réglementation commune concernant l'accès par les autorités américaines aux données PNR, le Conseil estime que les conditions de concurrence risquaient d'être faussées et qu'une atteinte grave aurait été portée à l'unicité du marché intérieur. Il était donc, selon lui, nécessaire d'établir des conditions harmonisées régissant l'accès par les autorités américaines auxdites données, tout en sauvegardant les exigences communautaires en ce qui concerne le respect des droits fondamentaux. Il s'agirait de l'imposition à toutes les compagnies concernées d'obligations harmonisées et de l'aspect externe de l'établissement et du fonctionnement du marché intérieur.

122. Enfin, le Conseil remarque que l'accord a été conclu après la décision d'adéquation, adoptée en vertu de l'article 25, paragraphe 6, de la directive 95/46. Selon lui, il était donc normal et correct de fonder la décision de conclusion de l'accord sur la même base juridique que celle de ladite directive, à savoir l'article 95 CE.

123. Dans son mémoire en intervention, la Commission souligne que les dispositions du préambule de l'accord démontrent que, pour les États-Unis, l'objectif primordial est la lutte contre le terrorisme, tandis que pour la Communauté le but principal est le maintien des éléments principaux de sa législation sur la protection des données à caractère personnel.

124. Elle remarque que, tout en critiquant le choix de l'article 95 CE comme base juridique de la décision du Conseil, le Parlement ne présente pas d'alternative crédible. Selon la Commission, cet article serait la base juridique «naturelle» de la décision du Conseil dans la mesure où la dimension externe de la protection des données à caractère personnel devrait être fondée sur l'article du traité qui soutient la mesure interne que constitue la directive 95/46, et ce d'autant plus que cet aspect externe serait explicitement prévu aux articles 25 et 26 de ladite directive. De plus, compte tenu du lien étroit et de l'interdépendance entre l'accord, la décision d'adéquation et les engagements du CBP, l'article 95 CE s'avérerait être la base juridique appropriée. En tout état de cause, la Commission soutient que le Conseil avait le pouvoir de conclure l'accord sur la base de cet article car la directive 95/46 aurait été affectée, au sens de la jurisprudence AETR (61), si les États membres avaient, séparément ou conjointement, conclu un tel accord en dehors du cadre communautaire.

125. Enfin, la Commission fait valoir que le traitement initial des données en cause par les compagnies aériennes est effectué dans un but commercial. Aussi, l'utilisation

qu'en font les autorités américaines ne les ferait-elle pas échapper à l'incidence de la directive 95/46.

2. Appréciation

126. Par son premier moyen, le Parlement invite la Cour à juger si l'article 95 CE constitue la base juridique appropriée pour fonder la décision du Conseil concernant la conclusion par la Communauté d'un accord international tel que celui en cause dans la présente affaire. Afin de répondre à cette question, il convient de faire application de la jurisprudence constante de la Cour en vertu de laquelle le choix de la base juridique d'un acte communautaire doit se fonder sur des éléments objectifs susceptibles de contrôle juridictionnel, parmi lesquels figurent, notamment, le but et le contenu de l'acte (62). En effet, «dans le cadre du système des compétences de la Communauté, le choix de la base juridique d'un acte ne peut pas dépendre seulement de la conviction d'une institution quant au but poursuivi […]» (63).

127. Nous rappelons que la Cour a jugé que «le choix de la base juridique appropriée revêt une importance de nature constitutionnelle. En effet, la Communauté ne disposant que de compétences d'attribution, elle doit rattacher [l'accord international concerné] à une disposition du traité qui l'habilite à l'effet d'approuver un tel acte». Selon la Cour, «[l]e recours à une base juridique erronée est donc susceptible d'invalider l'acte de conclusion lui-même et, partant, de vicier le consentement de la Communauté à être liée par l'accord auquel cette dernière a souscrit» (64).

128. Conformément à la méthode d'analyse appliquée par la Cour, nous examinerons donc si le but et le contenu de l'accord autorisaient le Conseil à adopter, sur le fondement de l'article 95 CE, une décision ayant pour objet, aux termes de son article 1er, d'approuver au nom de la Communauté ledit accord.

129. S'agissant du but de l'accord, il ressort expressément du paragraphe 1 de son préambule qu'il poursuit deux objectifs, à savoir, d'une part, la prévention et le combat du terrorisme et des délits qui y sont liés, ainsi que d'autres délits graves de nature transnationale, notamment la criminalité organisée (65), et, d'autre part, le respect des droits et libertés fondamentaux, et notamment le droit au respect de la vie privée.

130. La poursuite de l'objectif de lutte contre le terrorisme et d'autres crimes graves est attestée par la référence, au paragraphe 2 du préambule de l'accord, aux lois et règlements américains, adoptés à la suite des attentats terroristes du 11 septembre 2001, qui exigent de tout transporteur aérien assurant un service de transport international de passagers à destination ou au départ des États-Unis qu'il fournisse au CBP un accès électronique aux données PNR qui sont recueillies et stockées dans son système informatique de contrôle des réservations et des départs.

131. Quant à l'objectif tendant au respect des droits fondamentaux, et notamment le droit au respect de la vie privée, il apparaît à travers la référence à la directive 95/46. Il s'agit ainsi de garantir aux personnes physiques transportées la protection de leurs données à caractère personnel.

132. Cette garantie est recherchée tant dans le cadre des engagements pris par la CBP le 11 mai 2004, dont le paragraphe 4 du préambule de l'accord indique qu'ils seront publiés dans le *Federal Register*, que dans celui de la décision d'adéquation dont il est fait mention au paragraphe 5 du même préambule.

133. Ces deux objectifs doivent, selon le paragraphe 1 du préambule de l'accord, être poursuivis de façon simultanée. L'accord, conclu entre la Communauté et les États-Unis, tente donc de concilier ces deux objectifs, c'est-à-dire qu'il repose sur l'idée selon laquelle la lutte contre le terrorisme et d'autres crimes graves doit être menée dans le respect des droits fondamentaux, notamment du droit au respect de la vie privée, et plus précisément du droit à la protection des données à caractère personnel

134. Le contenu de l'accord confirme cette analyse. En effet, son paragraphe 1 prévoit que le CBP peut accéder, par voie électronique, aux données PNR provenant des systèmes de contrôle des réservations des transporteurs aériens situés sur le territoire des États membres «en application stricte» de la décision d'adéquation «et aussi longtemps que cette dernière sera applicable». Nous en déduisons que le moyen de lutter contre le terrorisme et d'autres crimes graves que constitue l'accès aux données PNR des passagers aériens n'est autorisé par l'accord que tant qu'il est reconnu que ces données bénéficient aux États-Unis d'un niveau de protection adéquat. Le contenu de cette disposition de l'accord traduit ainsi la poursuite simultanée des objectifs de lutte contre le terrorisme et d'autres crimes graves et de protection des données à caractère personnel.

135. Le même constat s'impose lors de l'examen du paragraphe 2 de l'accord qui oblige les transporteurs aériens assurant un service de transport international de passagers à destination ou au départ des États-Unis à traiter les données PNR stockées dans leurs systèmes informatiques de réservation «comme demandé par le CBP en vertu de la législation américaine, en application stricte de la décision [d'adéquation] et aussi longtemps que cette dernière est applicable». Là aussi, l'obligation qui pèse désormais sur les transporteurs aériens dans un but de lutte contre le terrorisme et d'autres crimes graves est étroitement liée à une protection adéquate des données à caractère personnel des passagers aériens.

136. D'autres dispositions de l'accord ont pour objet de traduire les buts de lutte contre le terrorisme et d'autres crimes graves et de protection des données personnelles des passagers aériens.

137. Ainsi, concernant spécifiquement l'objectif de protection des données à caractère personnel de ces passagers, il est indiqué au paragraphe 3 de l'accord que «[l]e CBP prend note de la décision [d'adéquation] et déclare qu'il met en œuvre les engagements annexés à ladite décision».

138. En outre, le paragraphe 6 de l'accord envisage l'hypothèse où l'Union européenne mettrait à son tour en œuvre un système d'identification des passagers aériens, dans le cadre duquel elle imposerait aux transporteurs aériens de donner aux autorités compétentes l'accès aux données PNR des passagers dont le voyage inclurait un vol à destination ou au départ de l'Union européenne. Dans le cas où elle mettrait en application cette mesure, l'accord prévoit que le Department of Homeland Security «encourage activement, autant que possible et dans le strict respect du principe de réciprocité, les compagnies aériennes relevant de sa compétence à coopérer». Il s'agit là d'une disposition qui traduit encore une fois l'objectif de lutte contre le terrorisme et d'autres crimes graves.

139. Nous précisons à cet égard, en réponse à certains arguments exposés par la Commission, qu'il nous paraît ainsi difficile de soutenir que l'objectif de lutte contre le terrorisme et d'autres crimes graves serait unilatéralement et seulement poursuivi par les États-Unis, la Communauté ayant uniquement pour but de protéger les données à caractère personnel des passagers aériens (66). En vérité, nous sommes d'avis que l'accord a, du point de vue de chaque Partie contractante et dans le même temps, pour but et contenu de concilier l'objectif de lutte contre le terrorisme et d'autres crimes graves avec celui de protection des données à caractère personnel des passagers aériens. Ce faisant, l'accord institue une coopération entre les Parties contractantes précisément destinée à atteindre ce double objectif de façon simultanée.

140. Au regard du but et du contenu de l'accord ainsi décrits, nous considérons que l'article 95 CE ne constitue pas une base juridique appropriée pour la décision du Conseil.

141. Il convient, à cet égard, de rappeler que l'article 95, paragraphe 1, CE, vise l'adoption par le Conseil de mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur.

142. La compétence attribuée à la Communauté par cet article du traité a un caractère horizontal, c'est-à-dire qu'elle n'est pas limitée à un domaine particulier. L'étendue de la compétence communautaire est donc définie «sur la base d'un critère *fonctionnel*, s'étendant de manière horizontale à l'ensemble des mesures destinées à la réalisation du 'marché intérieur'» (67).

143. De plus, il résulte de la jurisprudence de la Cour que les mesures visées à l'article 95, paragraphe 1, CE sont destinées à améliorer les conditions de l'établissement et du fonctionnement du marché intérieur et doivent effectivement avoir cet objet, en contribuant à l'élimination d'entraves à la libre circulation des marchandises ou à la libre prestation des services ou encore à la suppression de distorsions de concurrence (68). Il découle également de cette jurisprudence que, si le recours à l'article 95 CE comme base juridique est possible en vue de prévenir l'apparition d'obstacles futurs aux échanges résultant de l'évolution hétérogène des législations nationales, l'apparition de tels obstacles doit être vraisemblable et la mesure en cause doit avoir pour objet leur prévention (69).

144. Ainsi que nous l'avons déjà exposé, le Conseil soutient que sa décision a valablement été adoptée sur le fondement de l'article 95 CE dans la mesure où, en supprimant toute distorsion de concurrence entre les compagnies aériennes des États membres et entre celles-ci et les compagnies des pays tiers, l'accord avec les États-Unis aurait contribué à éviter qu'une atteinte grave soit portée à l'unicité du marché intérieur.

145. Certes, il convient de noter que le deuxième considérant de la décision du Conseil fait état de «la nécessité urgente de remédier à la situation d'incertitude dans laquelle se trouvent les compagnies aériennes et les passagers et de protéger les intérêts financiers des parties concernées». Cette phrase pourrait être comprise comme faisant allusion aux sanctions pouvant être infligées par les autorités américaines compétentes aux compagnies aériennes qui refuseraient de fournir un accès aux données PNR de leurs passagers, sanctions qui pourraient avoir des conséquences financières sur lesdites compagnies. Il serait possible de concevoir que, dans un tel cas de figure, ces sanctions ayant des implications financières défavorables pour certaines compagnies puissent être à l'origine de distorsions de concurrence entre l'ensemble des compagnies aériennes établies sur le territoire des États membres.

146. Par ailleurs, nous pouvons également concevoir qu'une attitude différente de la part des États membres, certains interdisant sous peine de sanctions aux compagnies aériennes établies sur leur territoire d'autoriser le transfert des données PNR de leurs passagers, alors que d'autres n'agiraient pas de la sorte, soit susceptible d'avoir un effet, même indirect, sur le fonctionnement du marché intérieur, du fait des éventuelles distorsions de concurrence qui pourraient naître entre les compagnies aériennes.

147. Toutefois, force est de constater qu'un tel objectif tendant à éviter des distorsions de concurrence, pour autant qu'il soit effectivement poursuivi par le Conseil, présente *un caractère accessoire* par rapport aux deux objectifs principaux de lutte contre le terrorisme et d'autres crimes graves et de protection des données à caractère personnel des passagers qui, comme nous l'avons vu, sont expressément mentionnés et effectivement mis en œuvre dans les dispositions de l'accord.

148. L'objectif tendant à éviter les distorsions de concurrence, que ce soit, ainsi que l'affirme le Conseil, entre les compagnies aériennes des États membres ou entre celles-ci et les compagnies des pays tiers, ne figure, quant à lui, explicitement nulle part dans les dispositions de l'accord. Il présente un caractère implicite, et donc nécessairement accessoire par rapport aux deux autres.

149. Or, nous rappelons que, ainsi que la Cour l'a déjà jugé, «le seul fait qu'un acte puisse avoir des incidences sur l'établissement et le fonctionnement du marché intérieur ne suffit pas pour justifier le recours à cette disposition comme base juridique de cet acte» (70).

150. Et surtout, il ressort d'une jurisprudence constante de la Cour que lorsque l'examen d'un acte communautaire démontre qu'il poursuit plusieurs finalités ou qu'il a plusieurs composantes, et si l'une de celles-ci est identifiable comme principale ou prépondérante, tandis que l'autre n'est qu'accessoire, l'acte en question doit être fondé sur une seule base juridique, à savoir celle exigée par la finalité ou composante principale ou prépondérante (71). Ce n'est qu'à titre exceptionnel, s'il est établi que l'acte poursuit à la fois plusieurs objectifs qui sont liés d'une façon indissociable, sans que l'un soit second et indirect par rapport à l'autre, qu'un tel acte devra être fondé sur les différentes bases juridiques correspondantes (72). Tel n'est pas, selon nous, le cas en l'espèce.

151. Nous remarquerons encore que, même si les trois objectifs devaient être considérés comme poursuivis d'une façon indissociable par l'accord, il n'en resterait pas moins que le choix du Conseil de fonder juridiquement sa décision sur le seul article 95 CE devrait, en vertu de cette jurisprudence, être considéré comme inapproprié.

152. En vérité, il ressort de la lecture du deuxième considérant de la décision du Conseil dans son entier que la «nécessité urgente» dont il est fait état par ce dernier a pour objet principal d'expliquer qu'un délai a été fixé au Parlement pour rendre son avis, conformément à l'article 300, paragraphe 3, premier alinéa, CE, qui prévoit que, dans le cadre de la procédure de conclusion des accords, «[l]e Parlement européen émet son avis dans un délai que le Conseil peut fixer en fonction de l'urgence». Cet article dispose également que, «[e]n l'absence d'avis dans ce délai, le Conseil peut statuer». Tel a été le cas dans la procédure qui a été suivie en vue de l'adoption de la décision du Conseil.

153. Autrement dit, si «la nécessité urgente de remédier à la situation d'incertitude dans laquelle se trouvent les compagnies aériennes et les passagers et de protéger les intérêts financiers des parties concernées» a pu effectivement entrer en ligne de compte dans le processus visant à établir un régime des données PNR, il nous semble que cette prise en compte a davantage joué un rôle dans le cadre de la procédure suivie que dans la définition du but et du contenu de l'accord.

154. Quant à l'argument du Conseil et de la Commission selon lequel un acte relatif à la dimension externe de la protection des données à caractère personnel devrait être fondé sur une base juridique identique à celle de la mesure interne que constitue la directive 95/46, il convient de relever que la Cour a déjà jugé que le fait qu'une disposition particulière du traité ait été choisie comme base juridique pour l'adoption d'actes internes ne suffit pas à démontrer que cette même base doit également être retenue pour l'approbation d'un accord international ayant un objet similaire (73). De plus, nous avons démontré que l'accord n'a ni pour but principal ni pour contenu d'améliorer les conditions de fonctionnement du marché intérieur, alors que la directive 95/46, adoptée en vertu de l'article 95 CE, «vise à assurer la libre circulation entre États membres des données à caractère personnel par l'harmonisation des règles nationales protégeant les personnes physiques à l'égard du traitement de telles données» (74).

155. Compte tenu des éléments qui précèdent, nous estimons que l'examen du but et du contenu de l'accord démontre que l'article 95 CE ne constitue pas la base juridique appropriée de la décision du Conseil.

156. Nous proposons par conséquent à la Cour de juger que le premier moyen soulevé par le Parlement est fondé. Il s'ensuit que la décision du Conseil doit être annulée en raison du choix erroné de sa base juridique.

157. Il serait certes intéressant à ce stade de s'interroger sur la question tendant à savoir quelle devrait être la base juridique appropriée d'une telle décision. Toutefois, il importe de noter que la Cour n'est pas saisie de cette question délicate dans le cadre de la présente affaire. Nous formulerons donc seulement quelques remarques sur ce problème et, de façon plus générale, sur la nature du régime PNR tel qu'il a été négocié avec les États-Unis.

158. D'abord, contrairement à une idée défendue par le Conseil, la circonstance que le régime PNR n'ait pas été mis en place dans le cadre des dispositions du traité UE n'est pas, selon nous, de nature à démontrer la validité juridique de l'approche retenue par le Conseil et la Commission.

159. Ensuite, de manière plus générale, nous estimons qu'un acte qui prévoit la consultation et l'utilisation de données à caractère personnel par une entité ayant pour fonction d'assurer la sécurité intérieure d'un État, ainsi que la mise à disposition de ces données à une telle entité, est assimilable à un acte de coopération entre autorités publiques (75).

160. De plus, le fait d'imposer à une personne morale d'exécuter un tel traitement de données et de l'obliger à effectuer un transfert de ces données ne nous paraît pas fondamentalement éloigné d'un échange direct de données entre autorités publiques (76). C'est la communication obligatoire de données à des fins sécuritaires et répressives qui importe, et non ses modalités spécifiques à telle ou telle situation. Notre affaire concerne en réalité une problématique nouvelle, qui est relative à l'utilisation de données commerciales à des fins répressives (77).

161. Enfin, il convient de noter que le Tribunal a jugé que «la lutte contre le terrorisme international […] ne peut être rattachée à aucun des objets explicitement assignés à la Communauté par les articles 2 CE et 3 CE» (78).

162. Compte tenu du fait que notre analyse du premier moyen nous conduit à proposer à la Cour d'annuler la décision du Conseil en raison du choix erroné de la base juridique de celle-ci, nous n'examinerons qu'à titre subsidiaire les autres moyens invoqués par le Parlement à l'appui du présent recours.

B – *Sur le moyen tiré de la violation de l'article 300, paragraphe 3, deuxième alinéa, CE, en raison d'une modification de la directive 95/46*

1. Arguments des parties

163. Par ce deuxième moyen, le Parlement soutient que l'accord entre la Communauté et les États-Unis ne pouvait être approuvé au nom de celle-ci qu'en respectant la procédure prévue à l'article 300, paragraphe 3, deuxième alinéa, CE. En effet, cet article prévoit que «sont conclus après avis conforme du Parlement européen […] les accords impliquant une modification d'un acte adopté selon la procédure visée à l'article 251». Or, selon cette institution, l'accord en question impliquerait une modification de la directive 95/46, qui a été adoptée selon la procédure visée à l'article 251 CE.

164. De l'avis du Parlement, les engagements que les autorités américaines ont acceptés d'appliquer conformément à l'accord resteraient en deçà des conditions de traitement des données imposées par la directive 95/46. Partant, l'accord aurait pour effet de déroger à certains principes essentiels de ladite directive et de rendre licites des traitements de données qui ne sont pas autorisés par celle-ci. En ce sens, l'accord modifierait la directive 95/46. En particulier, le Parlement identifie les modifications suivantes.

165. En premier lieu, l'accord viserait la prévention et la lutte contre le terrorisme et d'autres crimes graves, alors que l'article 3, paragraphe 2, premier tiret, de la directive 95/46 exclurait du champ d'application de celle-ci le transfert de données à destination d'autorités publiques d'un État tiers pour des raisons liées à la sécurité publique de cet État. Le Parlement note que les États membres ont prévu à cet effet des dispositions spécifiques dans la convention Europol et que l'on peut dès lors estimer qu'il y a une complémentarité dans ce domaine entre les deux instruments, qui sont fondés sur des bases juridiques différentes.

166. En deuxième lieu, la possibilité accordée aux autorités américaines compétentes d'accéder directement aux données à caractère personnel à l'intérieur du territoire de

la Communauté (système «pull») constituerait également une modification de la directive 95/46. En effet, les articles 25 et 26 de celle-ci ne contiendraient aucune disposition autorisant qu'un pays tiers soit en droit d'accéder directement à ces données.

167. En troisième lieu, l'accord, en se référant aux engagements, autoriserait que le CBP, à sa discrétion et au cas par cas, transmette des données PNR à des autorités gouvernementales de répression ou de lutte contre le terrorisme étrangères aux États-Unis. Cette discrétion laissée aux autorités américaines violerait la directive 95/46, et notamment son article 25, paragraphe 1, aux termes duquel «le transfert vers un pays tiers de données à caractère personnel […] ne peut avoir lieu que si […] le pays tiers en question assure un niveau de protection adéquat». Le Parlement estime, en effet, que le système de protection mis au point dans ladite directive serait réduit à néant si le pays tiers faisant l'objet d'une décision d'adéquation positive était ensuite libre de transférer les données à caractère personnel vers d'autres pays qui, eux, n'ont fait l'objet d'aucune évaluation de la part de la Commission.

168. En quatrième lieu, l'accord contiendrait une modification de la directive 95/46 dans la mesure où le CBP, même s'il décidait de ne pas utiliser les données à caractère personnel «sensibles», serait juridiquement autorisé à procéder à leur collecte, ce qui constituerait déjà un traitement au sens de l'article 2, sous b), de cette directive.

169. En cinquième lieu, le Parlement considère que l'accord modifie ladite directive dans la mesure où le recours juridictionnel en cas de violation des droits qui sont garantis à toute personne par les dispositions nationales applicables au traitement en question, tel que prévu à l'article 22 de la directive 95/46, n'est pas suffisamment assuré. Notamment, une personne concernée par le transfert de ses données PNR ne disposerait d'aucun recours juridictionnel, par exemple en cas de données incorrectes la concernant ou d'utilisation de données sensibles ou encore de transmission des données à une autre autorité.

170. En sixième et dernier lieu, le Parlement souligne le caractère excessif de la durée de conservation des données PNR transférées au CBP, ce qui constituerait une modification de la directive 95/46, et plus particulièrement de son article 6, paragraphe 1, sous e), qui prévoit une durée de conservation des données «n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement».

171. Le CEPD soutient les conclusions du Parlement en ce sens que, selon lui, l'accord a une incidence sur la directive 95/46. Il est d'avis que l'accord ne pouvait être conclu que sous le contrôle démocratique du Parlement dans la mesure où il affecte le niveau d'harmonisation des législations nationales tel qu'il est prévu par cette directive, et même le respect des droits fondamentaux. Selon lui, l'atteinte au niveau de protection des données à caractère personnel prévu par ladite directive résulte notamment du fait que, tant dans le système «pull» que dans le système «push», les transporteurs aériens sont obligés d'agir en violation de la directive, en particulier de son article 6, paragraphe 1, sous b) et c). Dans la mesure où cette atteinte au niveau de protection des données implique une modification de la directive 95/46, le CEPD considère que les garanties de procédure prévues à l'article 300, paragraphe 3, deuxième alinéa, CE n'ont pas été respectées. Il estime, en outre, que les «garanties de substance» ne sont pas non plus respectées, en particulier parce que les engagements du CBP ont un caractère non contraignant.

172. En revanche, le Conseil, soutenu par la Commission, estime que l'accord n'implique pas une modification de la directive 95/46. À l'appui de cette opinion, il cite le paragraphe 8 dudit accord aux termes duquel celui-ci «n'a pas pour objet de déroger à la législation des parties ni de la modifier». Il soutient également que cette directive donne à la Commission un large pouvoir discrétionnaire pour apprécier le caractère adéquat de la protection assurée par un pays tiers. À cet égard, selon le Conseil, la question de savoir si la Commission a dépassé les limites de sa marge d'appréciation constituerait plutôt l'objet du recours en annulation de la décision d'adéquation dans l'affaire C-318/04.

173. Le Conseil rappelle également que, selon lui, les motivations (sécurité, lutte contre le terrorisme ou autre) qui ont amené le CBP à exiger la transmission des données PNR ne constituent, du point de vue de la Communauté, ni l'objet ni le contenu de l'accord. En outre, la directive 95/46 autoriserait que, dans le champ d'application du marché intérieur, les données à caractère personnel puissent être utilisées à des fins légitimes telles que la protection de la sécurité d'un État.

174. En tout état de cause, selon le Conseil, même à supposer que la Communauté n'avait pas de compétence pour conclure l'accord, il ne s'ensuivrait pas pour autant que le Parlement aurait dû donner son avis conforme, au prétendu motif que l'accord modifierait la directive 95/46. En effet, le Conseil précise que l'avis conforme du Parlement ne pourrait en aucun cas avoir pour effet d'élargir le champ des compétences de la Communauté.

175. Quant à la possibilité pour le CBP d'accéder directement aux données PNR (système «pull» actuellement applicable, dans l'attente de la mise en place d'un système «push»), si le Conseil reconnaît que la directive 95/46 ne mentionne pas explicitement une telle possibilité, elle ne l'interdirait pas non plus. Du point de vue de la Communauté, ce sont les conditions d'accès aux données qui importeraient.

176. La Commission ajoute à cette argumentation que, quel que soit le but pour lequel les données personnelles sont utilisées par le CBP, il n'en resterait pas moins que celles-ci sont et demeurent, pour les transporteurs aériens dans la Communauté, des données commerciales tombant sous le coup de la directive 95/46 et qui doivent, par conséquent, être protégées et traitées conformément à celle-ci.

2. Appréciation

177. En matière de conclusion d'accords internationaux par la Communauté, la consultation du Parlement apparaît comme la procédure de droit commun, en dehors du domaine de la politique commerciale commune. Cette consultation du Parlement intervient, en vertu de l'article 300, paragraphe 3, premier alinéa, CE, y compris lorsque l'accord porte sur un domaine pour lequel la procédure de codécision de l'article 251 CE est requise pour l'adoption de règles internes.

178. Par dérogation à cette procédure de droit commun, l'article 300, paragraphe 3, deuxième alinéa, CE, impose l'avis conforme du Parlement dans quatre cas, dont, pour ce qui nous intéresse dans la présente affaire, celui dans lequel l'accord implique «une modification d'un acte adopté selon la procédure visée à l'article 251». Il s'agit de garantir au Parlement colégislateur un contrôle sur une modification éventuelle par un accord international d'un acte adopté par lui.

179. La directive 95/46 a été adoptée selon la procédure de codécision. Le Parlement soutient donc que, l'accord impliquant une modification de ladite directive, la décision du Conseil portant approbation dudit accord au nom de la Communauté exigeait, pour être adoptée dans le respect des règles prévues par le traité, son avis conforme.

180. Afin d'apprécier le bien-fondé de ce moyen, nous précisons avant tout qu'il importe peu à nos yeux que l'accord précise, aux termes de son paragraphe 8, qu'il «n'a pas pour objet de déroger à la législation des parties ni de la modifier». En effet, ce qui importe aux fins de rendre opératoire l'article 300, paragraphe 3, deuxième alinéa, CE, c'est de vérifier si l'accord international *implique* une modification de l'acte communautaire interne, c'est-à-dire s'il a *pour effet* de modifier ledit acte, et ce indépendamment du fait que tel n'est pas son objet.

181. Ceci étant précisé, il semble que la Cour ne se soit pas encore prononcée sur le sens à donner à l'expression relativement vague de «modification d'un acte adopté selon la procédure visée à l'article 251» (79). Certains auteurs se sont interrogés à cet égard sur le point de savoir si le terme «modification» signifiait «une modification contrariant le texte» de l'acte interne ou si «n'importe quelle modification, même

allant dans le sens du texte» de l'acte interne était suffisante pour exiger le respect de la procédure de l'avis conforme (80).

182. L'expression utilisée à l'article 300, paragraphe 3, deuxième alinéa, CE invite également à se demander si, pour que l'avis conforme soit exigé, le champ d'application de l'accord projeté doit recouvrir, au moins partiellement, celui de l'acte interne adopté ou si le seul fait qu'un acte interne soit intervenu sur la base juridique utilisée pour la conclusion dudit accord suffit (81).

183. D'une manière générale, nous sommes d'avis que pour qu'il y ait «modification» par un accord international d'un acte communautaire interne adopté selon la procédure de codécision, l'une des conditions est que le champ d'application de l'accord recoupe celui couvert par cet acte interne. Dans ce cas, en effet, une modification de l'acte interne par l'accord international est susceptible d'intervenir, soit dans la mesure où l'accord comporte une disposition qui contredit l'une de celles de l'acte interne, soit parce que l'accord ajoute au contenu de l'acte interne, y compris sans contrariété directe.

184. Dans la présente affaire, nous estimons que l'accord n'a pas pu modifier le contenu de la directive 95/46.

185. Notre opinion est fondée, en premier lieu, sur le fait que, ainsi qu'il ressort de notre analyse du premier moyen, l'accord a principalement pour objectif de lutter contre le terrorisme et d'autres crimes graves tout en assurant, dans le même temps, une protection aux données à caractère personnel des passagers aériens. En revanche, la directive 95/46 vise à assurer la libre circulation entre les États membres des données à caractère personnel par l'harmonisation des dispositions nationales protégeant les personnes physiques à l'égard du traitement de telles données. Les deux actes ont donc deux objectifs bien distincts, et ce quand bien même ils concernent tous deux le domaine de la protection des données à caractère personnel (82).

186. En second lieu, et en cohérence avec le constat selon lequel leurs objectifs sont distincts, il s'avère que l'accord et la directive 95/46 ont des champs d'application différents. En effet, alors que l'accord s'applique à des traitements de données à caractère personnel mis en œuvre pour l'exercice d'activités relatives à la sécurité intérieure des États-Unis et, dans le même temps et plus précisément, à des activités relatives à la lutte contre le terrorisme et d'autres crimes graves, nous rappelons que l'article 3, paragraphe 2, premier tiret, de ladite directive exclut expressément de son champ d'application les traitements de données à caractère personnel qui sont «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 UE, 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*» (83).

187. Compte tenu du fait que, en l'espèce, les deux actes présentent des objectifs et des champs d'application différents, nous ne voyons pas comment le contenu de l'un serait susceptible de modifier celui de l'autre. À vrai dire, l'accord concerne des traitements de données à caractère personnel dont le législateur communautaire a clairement exclu qu'ils puissent être couverts par le système de protection mis en place par la directive 95/46. Cette approche retenue par le législateur communautaire est d'ailleurs cohérente avec le choix de la base juridique de ladite directive, à savoir l'article 95 CE.

188. Cette analyse ne nous paraît pas pouvoir être contredite par l'argument de la Commission en vertu duquel, quel que soit le but pour lequel les données personnelles sont utilisées par le CBP, il n'en resterait pas moins que celles-ci sont et demeurent, pour les transporteurs aériens dans la Communauté, des données commerciales tombant sous le coup de la directive 95/46 et qui doivent être protégées et traitées conformément à cette dernière.

189. Nous rappelons à cet égard que, s'il est vrai que le traitement que constituent la collecte et l'enregistrement de données des passagers aériens par les compagnies aériennes a, en général, une finalité commerciale dans la mesure où il est directement lié au déroulement du vol assuré par le transporteur aérien, le traitement des données que régit l'accord possède toutefois une nature tout autre, dans la mesure où, d'une part, il couvre un stade ultérieur à la collecte des données et, d'autre part, il poursuit une finalité sécuritaire.

190. Eu égard à l'ensemble de ces considérations, nous estimons que le deuxième moyen soulevé par le Parlement n'est pas fondé et doit donc être rejeté.

191. Pour les mêmes raisons que celles évoquées dans le cadre de notre examen de l'affaire C-318/04 (84), nous allons à présent examiner ensemble les troisième et quatrième moyens soulevés par le Parlement, à savoir la violation du droit à la protection des données à caractère personnel et la violation du principe de proportionnalité.

192. Nous rappelons également que, compte tenu de l'interdépendance entre l'accord tel qu'approuvé par la décision du Conseil, la décision d'adéquation et les engagements du CBP qui sont annexés à ladite décision de la Commission, c'est l'ensemble du régime PNR que nous estimons devoir être analysé au regard de ces moyens (85).

C – *Sur les moyens tirés de la violation du droit à la protection des données à caractère personnel et de la violation du principe de proportionnalité*

1. Arguments des parties

193. Le Parlement soutient que le régime PNR viole le droit à la protection des données à caractère personnel, tel qu'il est reconnu notamment par l'article 8 de la CEDH.

194. Selon lui, en prévoyant que le CBP peut accéder, par voie électronique, aux données PNR provenant des systèmes de réservation des transporteurs aériens situés sur le territoire des États membres, et en stipulant que lesdits transporteurs, lorsqu'ils assurent un service de transport international de passagers à destination ou au départ des États-Unis, traiteront les données PNR en cause comme demandé par le CBP en vertu de la législation américaine, l'accord serait relatif à un traitement de données à caractère personnel constitutif d'une ingérence dans la vie privée, au sens de l'article 8 de la CEDH. De même, la décision d'adéquation ne respecterait pas cet article.

195. Le Parlement précise que, pour ne pas enfreindre l'article 8 de la CEDH, pareille ingérence doit être prévue par la loi, poursuivre un but légitime et être nécessaire dans une société démocratique afin d'atteindre ce but. Il considère que l'accord et la décision d'adéquation ne remplissent pas ces conditions.

196. S'agissant, en premier lieu, de la condition selon laquelle l'ingérence doit être prévue par la loi, la Parlement relève que tant l'accord que la décision d'adéquation ne répondent pas aux exigences d'accessibilité et de prévisibilité de la loi qui sont requises par la jurisprudence de la Cour européenne des droits de l'homme. D'une part, quant à l'exigence d'accessibilité de la loi, le Parlement estime que, en renvoyant de façon générale et imprécise à la législation américaine applicable, l'accord et la décision d'adéquation ne contiennent pas eux-mêmes les droits et obligations qui incombent aux passagers et aux compagnies aériennes européennes. Or, l'impératif de sécurité juridique exigerait qu'un acte communautaire qui crée des obligations juridiques permette aux intéressés de connaître avec exactitude l'étendue des obligations qu'il leur impose (86). En outre, contrairement à ce que requiert l'exigence d'accessibilité de la loi, les lois américaines applicables ne seraient pas disponibles dans toutes les langues officielles de la Communauté. Le Parlement constate également le caractère erroné, dans le préambule de l'accord, de la référence et de la date d'adoption de la décision d'adéquation. D'autre part, quant à l'exigence de prévisibilité de la loi, elle ferait défaut car l'accord et la décision d'adéquation ne

contiendraient pas avec suffisamment de précision les droits et obligations des entreprises aériennes et des citoyens établis dans la Communauté. Par ailleurs, les passagers recevraient seulement une information générale, ce qui serait contraire à l'obligation d'information, telle qu'elle est prévue aux articles 10 et 11 de la directive 95/46 et 8, sous a), de la convention n° 108. Enfin, l'accord et les engagements du CBP contiendraient une série d'imprécisions incompatibles avec l'article 8 de la CEDH.

197. Concernant, en deuxième lieu, la condition selon laquelle, en vertu de l'article 8, paragraphe 2, de la CEDH, l'ingérence dans le droit au respect de la vie privée doit poursuivre un but légitime, le Parlement admet qu'elle est remplie. Il rappelle à cet égard le soutien qu'il a exprimé à de multiples reprises au Conseil dans la lutte contre le terrorisme.

198. S'agissant, en troisième lieu, de la condition selon laquelle l'ingérence doit constituer une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui, le Parlement considère qu'elle n'est pas remplie pour les raisons suivantes:

– il ressortirait du paragraphe 3 des engagements du CBP que le traitement des données n'est pas limité à la seule fin de lutter contre le terrorisme, mais a également pour but de prévenir et de combattre d'autres crimes graves, y compris la criminalité organisée, et la fuite en cas de mandat d'arrêt ou de mise en détention pour l'un des crimes susmentionnés. Dans la mesure où le traitement des données dépasse la seule lutte contre le terrorisme, il ne serait pas nécessaire pour la réalisation du but légitime poursuivi;

– l'accord prévoirait le transfert d'un nombre excessif de données (34), ce faisant il ne respecterait pas le principe de proportionnalité. Sous l'angle du respect d'un niveau adéquat de protection des données à caractère personnel, 19 de ces 34 données paraîtraient acceptables. Le Parlement estime qu'il existe un «décalage considérable» entre le nombre de données prévu par des instruments juridiques comparables applicables au niveau de l'Union européenne, et celui requis en vertu de l'accord (87). Par ailleurs, certaines des rubriques des PNR demandées pourraient contenir des données sensibles;

– les données seraient stockées trop longtemps par les autorités américaines eu égard au but poursuivi. En effet, il résulte des engagements du CBP que, suite à l'accès en ligne aux données pour les personnes autorisées du CBP qui est ouvert pendant sept jours, toutes les données sont conservées pendant une période de trois ans et demi, puis les données qui ont été consultées manuellement au cours de ladite période sont transférées par le CBP vers un fichier de dossiers supprimés, sous forme de données brutes, où elles sont conservées pendant une période de huit ans avant leur destruction. La comparaison avec les systèmes d'information érigés, par exemple, dans le cadre de la convention d'application de l'Accord de Schengen, de la convention Europol et de la décision Eurojust, qui prévoiraient une durée de conservation de un à trois ans, démontrerait le caractère excessif de la durée mentionnée dans les engagements;

– l'accord ne prévoirait pas de contrôle juridictionnel concernant le traitement des données par les autorités américaines. De plus, dans la mesure où l'accord et les engagements ne créent pas de droits pour les personnes dont les données à caractère personnel sont traitées, le Parlement ne voit pas comment ces personnes pourraient s'en prévaloir devant les juridictions américaines;

– l'accord permettrait le transfert des données à d'autres autorités publiques; il irait ainsi au-delà de ce qui est nécessaire pour combattre le terrorisme.

199. Le CEPD défend la thèse selon laquelle le traitement de six catégories de données constitue à l'évidence une atteinte au droit à la vie privée (88). Cette atteinte

résulterait également de la possibilité de composer des profils personnels à partir de ces données. Le CEPD soutient les arguments du Parlement tendant à démontrer que l'ingérence n'est pas justifiée au regard de l'article 8, paragraphe 2, de la CEDH. Il estime également que le niveau de protection offert par le CBP n'est pas adéquat, au sens de l'article 25 de la directive 95/46, notamment parce que l'article 8 de la CEDH n'est pas respecté.

200. En revanche, le Conseil et la Commission considèrent que le régime PNR respecte les conditions posées à l'article 8, paragraphe 2, de la CEDH, telles qu'interprétées par la Cour européenne des droits de l'homme.

201. S'agissant, en premier lieu, de la condition selon laquelle l'ingérence doit être prévue par la loi, le Conseil estime qu'il n'est pas nécessaire, pour satisfaire à l'exigence d'accessibilité de la loi, que le texte de l'accord contienne lui-même toutes les dispositions qui pourraient éventuellement affecter les personnes concernées. Il ne serait pas contraire au droit de prévoir dans l'accord un renvoi à la décision d'adéquation et aux engagements du CBP qui figurent en annexe de cette décision, dans la mesure où tous ces textes ont été publiés au *Journal officiel de l'Union européenne*. Par ailleurs, ce dernier n'aurait pas vocation à publier des lois des pays tiers. À propos de la référence erronée à la décision d'adéquation qui figure dans le préambule de l'accord, le Conseil indique qu'il prendra les dispositions nécessaires pour qu'un rectificatif soit publié au Journal officiel, mais il considère que ces erreurs de nature technique n'affectent pas l'accessibilité des actes en cause, au sens de la jurisprudence de la Cour européenne des droits de l'homme. Quant à la condition relative à la prévisibilité de la loi, le Conseil estime que ne constitue pas une violation de cette exigence le fait que les engagements du CBP ainsi que les lois et exigences constitutionnelles américaines n'aient pas été reprises in extenso dans l'accord lui-même. En outre, les engagements du CBP, rédigés avec suffisamment de précision, permettraient aux personnes concernées de régler leur conduite.

202. S'agissant, en deuxième lieu, de la condition selon laquelle l'ingérence doit poursuivre un but légitime, le Conseil relève que la lutte contre des crimes graves autres que le terrorisme entre dans plusieurs des catégories d'intérêts légitimes mentionnés à l'article 8, paragraphe 2, de la CEDH (notamment la sûreté publique, la défense de l'ordre et la prévention des infractions pénales). Dès lors, l'accord et les engagements du CBP poursuivraient un but légitime également dans la mesure où ils visent ces autres crimes graves.

203. Le Conseil estime, en troisième lieu, que l'ingérence est proportionnée au but recherché. Plus précisément, il fait valoir que les catégories de données PNR requises par le CBP sont utiles aux fins de prévenir des actes terroristes ou la criminalité organisée, ainsi que pour éclairer les enquêtes qui suivent les attentats, en facilitant la tâche d'identification des personnes associées à des groupes terroristes ou à la criminalité organisée. Quant au nombre de données PNR à transférer, la comparaison avec les systèmes d'information érigés au sein de l'Union européenne ne serait pas pertinente car, outre que ces systèmes ont un autre but et contenu que ceux du régime PNR, la nécessité de tracer le profil de terroristes potentiels exigerait d'avoir accès à un nombre plus élevé de données. S'agissant des trois rubriques des données PNR qui pourraient, selon le Parlement, contenir des données sensibles (89), le Conseil remarque que l'accès du CBP à ces trois rubriques a été strictement limité en vertu du paragraphe 5 des engagements pris par le CBP (90). De plus, selon les engagements n^{os} 9, 10 et 11, il serait en tout état de cause exclu que le CBP puisse utiliser des données sensibles (91). Quant à la durée de conservation des données PNR, le Conseil estime que, compte tenu du fait que les enquêtes suivant les attentats durent parfois plusieurs années, une durée normale de conservation fixée à trois ans et demi, sauf dans des cas spécifiques où cette durée peut être plus longue, constitue une solution équilibrée. En outre, il n'y aurait pas de raison de considérer qu'un système de contrôle indépendant fait défaut. Enfin, le transfert des données à d'autres autorités publiques serait entouré de garanties suffisantes; en particulier, le CBP ne pourrait transférer des données à d'autres autorités publiques qu'au cas par cas, et seulement aux fins de prévenir ou de combattre le terrorisme ou d'autres crimes graves.

204. Aux yeux de la Commission, il ne fait pas de doute que l'ensemble que forment l'accord, la décision d'adéquation et les engagements du CBP admet qu'une certaine ingérence dans la vie privée, de gravité variable selon les données transmises, puisse prendre place. Cette ingérence serait prévue par la loi, c'est-à-dire ledit ensemble, poursuivrait un but légitime, à savoir la réconciliation d'un conflit entre la loi américaine de nature sécuritaire et les normes communautaires relatives à la protection des données à caractère personnel, et serait nécessaire dans une société démocratique afin d'atteindre ce but.

205. Le Royaume-Uni estime que, dans le cadre de l'analyse d'une éventuelle violation du droit à la protection des données à caractère personnel, la décision du Conseil, l'accord, la décision d'adéquation et les engagements du CBP doivent être examinés ensemble, car ils constituent des instruments juridiques étroitement liés. Il considère également que c'est l'accessibilité et la prévisibilité du droit communautaire applicable qui doivent être examinées, et non celles des lois qui s'appliquent sur le territoire des États-Unis. Si l'on met en relation l'accord, la décision d'adéquation et les engagements du CBP, le droit communautaire contiendrait, de l'avis du Royaume-Uni, un exposé clair et complet de la position juridique de toutes les parties affectées. En outre, il ne partage pas l'opinion selon laquelle les engagements du CBP seraient unilatéraux par nature et pourraient être modifiés ou rétractés par les autorités américaines avec impunité.

206. Sur la nécessité de l'ingérence, le Royaume-Uni souligne d'abord que le combat contre d'autres crimes graves est clairement annoncé comme étant un objectif de l'accord et représente un but d'ordre public qui serait tout aussi légitime que la lutte contre le terrorisme. Le Royaume-Uni considère ensuite que la gamme des données qui peuvent être transférées, la durée de leur rétention et la possibilité de leur transfert à d'autres autorités correspondent et sont proportionnées à ces objectifs, étant donné en particulier les nombreuses garanties qui seraient incluses dans les engagements et la décision d'adéquation afin de limiter le risque encouru pour la vie privée des passagers. Il précise enfin que, selon lui, le critère de proportionnalité doit être appliqué, en vertu à la fois de la jurisprudence de la Cour et de celle de la Cour européenne des droits de l'homme, à la lumière de la nature et de l'importance des objectifs en cause.

2. Appréciation

207. Par ces moyens, le Parlement soutient que la décision du Conseil ainsi que la décision d'adéquation violent le droit à la protection des données à caractère personnel, tel qu'il est garanti notamment à l'article 8 de la CEDH.

208. Il est de jurisprudence constante que les droits fondamentaux font partie intégrante des principes généraux du droit dont la Cour assure le respect (92). À cet effet, la Cour s'inspire des traditions constitutionnelles communes aux États membres ainsi que des indications fournies par les instruments internationaux concernant la protection des droits de l'homme auxquels les États membres ont coopéré ou adhéré. Elle estime que la CEDH revêt, à cet égard, «une signification particulière» (93). Ne sauraient donc être admises dans la Communauté des mesures incompatibles avec le respect des droits de l'homme ainsi reconnus et garantis (94). Ces principes ont été repris à l'article 6, paragraphe 2, UE.

209. Au fil de cette jurisprudence, la Cour a été conduite à incorporer dans la légalité communautaire le droit au respect de la vie privée (95). Le droit à la protection des données à caractère personnel constitue l'un des aspects du droit au respect de la vie privée, et est donc protégé par l'article 8 de la CEDH, y compris dans l'ordre juridique communautaire, par le prisme des principes généraux du droit.

210. Nous examinerons si le régime PNR est constitutif d'une violation du droit au respect de la vie privée en suivant la grille d'analyse qui découle du libellé de l'article 8 de la CEDH. Ainsi, après avoir vérifié si ledit régime constitue une ingérence dans la vie privée des passagers aériens, nous déterminerons si cette ingérence est dûment justifiée.

a) Sur l'existence d'une ingérence dans la vie privée

211. L'existence d'une ingérence dans la vie privée réalisée par l'ensemble que forment la décision du Conseil approuvant l'accord, la décision d'adéquation et les engagements du CBP ne fait, à notre avis, guère de doute. Il nous paraît en effet clair que la consultation, l'utilisation par le CBP et la mise à la disposition de ce dernier des données des passagers aériens provenant des systèmes de réservation des transporteurs aériens situés sur le territoire des États membres constituent une immixtion de la part d'autorités publiques dans la vie privée de ces passagers.

212. Nous précisons également que l'ingérence dans la vie privée des passagers aériens nous paraît établie quand bien même certaines rubriques des données PNR, prises isolément, pourraient être analysées comme ne portant pas individuellement atteinte à la vie privée des passagers concernés. Il nous semble en effet nécessaire d'appréhender globalement la liste des rubriques des données PNR demandées par le CBP, et ce dans la mesure où le recoupement de ces données est susceptible de permettre la constitution de profils personnels.

213. Une ingérence dans la vie privée méconnaît le droit au respect de la vie privée sauf si elle est dûment justifiée.

b) Sur la justification de l'ingérence dans la vie privée

214. Pour être admissible, l'ingérence dans la vie privée est subordonnée à la vérification de trois conditions: elle doit être prévue par la loi, viser un but légitime et présenter un caractère de nécessité dans une société démocratique.

i) L'ingérence est-elle prévue par la loi?

215. Selon une jurisprudence constante de la Cour européenne des droits de l'homme, cette condition implique que la mesure incriminée ait une base légale et concerne également la qualité de la loi en cause (96). L'examen de la qualité de la loi implique que celle-ci soit accessible aux citoyens, précise et prévisible dans ses conséquences. Cela suppose qu'elle définisse avec une précision suffisante les conditions et modalités de la limitation du droit garanti, afin de permettre au citoyen de régler sa conduite et de bénéficier d'une protection adéquate contre l'arbitraire (97).

216. Le Parlement fait valoir que la mesure qui prévoit l'ingérence n'est ni accessible ni prévisible dans ses conséquences. Nous ne partageons pas cette opinion.

217. Nous estimons au contraire que la lecture de la décision du Conseil et de l'accord qui y est annexé ainsi que celle de la décision d'adéquation, qui contient en annexe les engagements du CBP, permettent aux personnes concernées, à savoir les compagnies aériennes et les passagers aériens, d'être informées de manière suffisamment précise aux fins de régler leur conduite.

218. Nous observons à cet égard le caractère relativement détaillé des 48 paragraphes de la déclaration d'engagement du CBP, qui fournissent des précisions sur le cadre juridique applicable. De plus, la décision d'adéquation fait figurer dans son préambule les références de la loi américaine pertinente et des règlements de mise en œuvre adoptés par le CBP en vertu de cette loi (98). Il nous paraîtrait dès lors excessif d'exiger que les dispositions législatives et réglementaires américaines applicables fassent l'objet d'une publication intégrale au *Journal officiel de l'Union européenne*. Outre que celui-ci, ainsi que le relève le Conseil, n'a pas vocation à publier des lois des pays tiers, nous considérons que la déclaration d'engagement du CBP, qui a été publiée au Journal officiel, contient les informations essentielles sur la procédure d'utilisation des données par le CBP et sur les garanties qui entourent ladite procédure.

219. Conformément à l'impératif de sécurité juridique, les compagnies aériennes visées par le régime PNR sont informées des obligations qui pèsent sur elles en vertu

de l'accord, et les passagers aériens sont informés de leurs droits, notamment quant à l'accès aux données et à leur rectification (99).

220. Certes, compte tenu de l'interdépendance entre les éléments composant le régime PNR, faut-il regretter que le préambule de l'accord contienne des erreurs sur la référence et la date de la décision d'adéquation. En effet, ces erreurs complexifient la démarche d'un citoyen européen qui souhaiterait s'informer sur le contenu du régime négocié avec les États-Unis. Toutefois, elles ne rendent pas, à notre avis, excessivement difficile une telle recherche dans la mesure où la décision d'adéquation a été publiée au Journal officiel et que les outils de recherche, notamment informatiques, permettent aisément sa découverte. En outre, le Conseil s'est engagé à ce qu'un rectificatif soit publié au Journal officiel, ce qu'il a en effet réalisé (100).

221. Eu égard à ces considérations, nous estimons que l'ingérence dans la vie privée des passagers aériens concernés doit être considérée comme «prévue par la loi» au sens de l'article 8, paragraphe 2, de la CEDH.

ii) L'ingérence poursuit-elle un but légitime?

222. Au regard des différentes finalités mentionnées à l'article 8, paragraphe 2, de la CEDH, nous considérons que l'ingérence dans la vie privée qui est en cause dans la présente affaire poursuit un but légitime. Tel est notamment le cas en ce qui concerne la lutte contre le terrorisme.

223. Comme le Conseil, nous pensons que la lutte contre des crimes graves autres que le terrorisme (101) entre également dans plusieurs des catégories d'intérêts légitimes mentionnés à l'article 8, paragraphe 2, de la CEDH, tels que la sécurité nationale, la sûreté publique, la défense de l'ordre ou la prévention des infractions pénales. Dès lors, nous considérons que le régime PNR poursuit un but légitime également dans la mesure où il vise ces autres crimes graves.

224. Il convient à présent de vérifier la proportionnalité de l'ingérence en se demandant si celle-ci est nécessaire dans une société démocratique en vue de prévenir et de combattre le terrorisme et d'autres crimes graves.

iii) L'ingérence est-elle nécessaire dans une société démocratique pour atteindre un tel but?

225. Avant de procéder à la vérification précise du respect de cette condition de proportionnalité, nous ferons quelques remarques préalables relatives à l'étendue du contrôle à exercer par la Cour.

226. Selon la Cour européenne des droits de l'homme, l'adjectif «nécessaire», au sens de l'article 8, paragraphe 2, de la CEDH, implique qu'«un besoin social impérieux» soit en cause et que la mesure prise soit «proportionnée au but légitime poursuivi» (102). En outre, «les autorités nationales jouissent d'une marge d'appréciation dont l'ampleur dépend non seulement de la finalité, mais encore du caractère propre de l'ingérence» (103).

227. Dans le cadre du contrôle de la marge d'appréciation des États, la Cour européenne des droits de l'homme vérifie traditionnellement si les motifs invoqués à l'appui des ingérences sont pertinents et suffisants, puis si l'ingérence est proportionnée au but légitime poursuivi et vérifie alors qu'un équilibre a été ménagé entre l'intérêt général et les intérêts de l'individu (104). Tirant enseignement de cette jurisprudence, il a ainsi pu être observé que «[l]e principe de proportionnalité, qui traduit une exigence d'adéquation entre un objectif légitime et les moyens utilisés pour l'atteindre, se situe donc au cœur du contrôle de la marge nationale d'appréciation» (105).

228. Le contrôle de proportionnalité effectué par la Cour européenne des droits de l'homme varie en fonction de paramètres tels que la nature du droit et des activités en cause, le but de l'ingérence, et la présence éventuelle d'un dénominateur commun aux systèmes juridiques des États.

229. S'agissant de la nature du droit et des activités en cause, dès lors qu'il s'agit d'un droit qui touche étroitement à la sphère d'intimité de l'individu, tel que le droit à la confidentialité des données à caractère personnel relatives à la santé (106), la Cour européenne des droits de l'homme semble considérer que la marge d'appréciation de l'État est réduite et que son contrôle juridictionnel doit être plus strict (107).

230. Toutefois, dès lors que le but de l'ingérence consiste dans la préservation de la sécurité nationale (108) ou bien dans la lutte contre le terrorisme (109), la Cour européenne des droits de l'homme tend à reconnaître aux États une marge d'appréciation d'une grande ampleur.

231. Eu égard à la nature et à l'importance de l'objectif de lutte contre le terrorisme, qui apparaît prépondérant dans le cadre du régime PNR, et en considération du contexte politiquement sensible dans lequel se sont déroulées les négociations entre la Communauté et les États-Unis, nous estimons que, dans la présente affaire, la Cour devrait considérer que le Conseil et la Commission disposaient d'une grande marge d'appréciation en vue de négocier, avec les autorités américaines, le contenu du régime PNR. Il s'ensuit que, afin de respecter cette grande marge d'appréciation, le contrôle exercé par la Cour quant à la nécessité de l'ingérence devrait, à notre sens, se limiter à la vérification d'une éventuelle erreur manifeste d'appréciation de la part de ces deux institutions (110). En exerçant un tel contrôle restreint, la Cour éviterait ainsi l'écueil consistant à substituer sa propre appréciation à celle des autorités politiques communautaires quant à la nature des moyens les plus adéquats et opportuns pour lutter contre le terrorisme et d'autres crimes graves.

232. Afin de fixer l'étendue du contrôle qu'elle entend exercer, la Cour pourrait, en plus de la jurisprudence précitée de la Cour européenne des droits de l'homme, s'appuyer sur sa propre jurisprudence, dans laquelle elle considère que lorsqu'une institution communautaire dispose dans un domaine particulier d'un large pouvoir d'appréciation, «[…] seul le caractère manifestement inapproprié d'une mesure arrêtée en ce domaine, par rapport à l'objectif que l'institution compétente entend poursuivre, peut affecter la légalité d'une telle mesure» (111). Cette limitation du contrôle de proportionnalité «s'impose particulièrement» lorsque «le Conseil est amené à opérer des arbitrages entre des intérêts divergents et à prendre ainsi des options dans le cadre des choix politiques relevant de ses responsabilités propres» (112). La limitation du contrôle peut également être justifiée par la circonstance que, dans un domaine d'action, une institution communautaire est conduite à réaliser des appréciations complexes (113).

233. Cette jurisprudence et les raisons qui la sous-tendent nous semblent devoir être appliquées dans la présente affaire dans la mesure où, dans le cadre de l'élaboration du régime PNR, le Conseil et la Commission ont été confrontés à des choix politiques entre différents intérêts difficiles à concilier et à des appréciations complexes (114). Cela serait conforme au principe de séparation des pouvoirs qui commande à la Cour de respecter les responsabilités politiques qui appartiennent aux organes législatifs et administratifs communautaires et, par suite, de ne pas se substituer à ces derniers dans les choix politiques qu'ils sont amenés à effectuer.

234. Il convient à présent de vérifier précisément si, en adoptant les différents éléments qui constituent le régime PNR, le Conseil et la Commission ont manifestement dépassé les limites qui s'imposaient à leur marge d'appréciation au regard du droit au respect de la vie privée, et plus particulièrement du droit à la protection des données à caractère personnel des passagers aériens, eu égard au but légitime poursuivi.

235. Dans le cadre de cet examen, le contenu de la déclaration d'engagement du CBP revêt une importance particulière dans la mesure où celle-ci contient le détail des

garanties qui encadrent le régime PNR. Nous indiquons, à cet égard, que, selon nous, il serait erroné de considérer que ladite déclaration est dépourvue de tout effet obligatoire et contient des engagements pouvant être librement modifiés ou rétractés par les autorités américaines.

236. En effet, la déclaration d'engagement, dont nous rappelons qu'elle est annexée à la décision d'adéquation, constitue l'une des composantes du régime PNR et, en tant que telle, son non-respect conduirait à la paralysie du régime tout entier. Nous soulignons, à cet égard, que les paragraphes 1 et 2 de l'accord subordonnent l'obligation de traitement des données PNR qui pèse sur les transporteurs aériens à l'application stricte de la décision d'adéquation, cette obligation ne valant qu'«aussi longtemps que cette dernière est applicable». De plus, aux termes du paragraphe 3 de l'accord, le CBP «déclare qu'il met en œuvre les engagements annexés à ladite décision». Enfin, les articles 3, 4 et 5 de la décision d'adéquation définissent les mesures à prendre en cas de non-respect des normes de protection contenues dans la déclaration d'engagement. Parmi ces mesures, il est prévu que les autorités compétentes des États membres pourront suspendre le transfert de données vers le CBP et que, en cas de non-respect des principes essentiels nécessaires pour assurer un niveau de protection adéquat des personnes concernées, la décision d'adéquation pourra être suspendue ou annulée, ce qui aurait pour effet de rendre inapplicables les paragraphes 1 et 2 de l'accord.

237. Aux fins de faire constater par la Cour que l'ingérence dans la vie privée de ces passagers ne respecte pas le principe de proportionnalité, le Parlement invoque, en premier lieu, le caractère excessif du nombre de données demandées par le CBP aux compagnies aériennes. Par ailleurs, il estime que certaines des rubriques des PNR demandées pourraient contenir des données sensibles.

238. Nous estimons que, en arrêtant la liste des 34 rubriques de données à caractère personnel telle qu'elle est annexée à la décision d'adéquation, la Commission n'a pas accepté une mesure manifestement inappropriée en vue d'atteindre l'objectif de lutte contre le terrorisme et d'autres crimes graves. D'une part, en effet, il convient de souligner l'importance de l'activité de renseignement dans la lutte antiterroriste, l'obtention d'informations adéquates pouvant permettre aux services de sécurité d'un État de prévenir un éventuel attentat terroriste. Dans cette perspective, la nécessité de tracer le profil de terroristes potentiels peut exiger l'accès à un nombre élevé de données. D'autre part, la circonstance que d'autres instruments relatifs à l'échange d'informations adoptés au sein de l'Union européenne prévoient la communication d'un nombre inférieur de données ne suffit pas à démontrer le caractère excessif du nombre de données demandées dans l'instrument spécifique de lutte antiterroriste que constitue le régime PNR (115).

239. En outre, s'il est exact de remarquer, comme le fait le Parlement, que trois des rubriques de données demandées sont susceptibles de contenir des données sensibles (116), nous observons, d'une part, que l'accès du CBP à ces trois rubriques a été strictement limité en vertu du paragraphe 5 de la déclaration d'engagement, d'autre part, que, en vertu des paragraphes 9 à 11 de ladite déclaration, il est exclu que le CBP puisse utiliser des données sensibles et, enfin, qu'un système de filtrage desdites données a été mis en place par le CBP, conformément à l'engagement pris par ce dernier (117).

240. En deuxième lieu, le Parlement considère que les données PNR des passagers aériens sont conservées trop longtemps par les autorités américaines eu égard au but poursuivi.

241. La durée de stockage de ces données est mentionnée au paragraphe 15 de la déclaration d'engagement, qui prévoit, en substance, l'accès en ligne auxdites données par les utilisateurs habilités du CBP pendant une période initiale de sept jours. Au terme de cette période, la consultation des données par un nombre restreint de fonctionnaires autorisés est possible pendant une période de trois ans et six mois. Enfin, au terme de cette deuxième période, les données qui n'ont pas été consultées manuellement durant ce laps de temps sont détruites, tandis que les données qui ont

été consultées manuellement durant la période de trois ans et six mois sont transférées par le CBP vers un fichier de dossiers supprimés où elles sont conservées pendant une période de huit ans avant leur destruction (118).

242. Il résulte de cette disposition que la durée normale de conservation des données issues de PNR est de trois ans et six mois, excepté pour celles qui ont été consultées manuellement durant cette période. Nous estimons que cette durée n'est pas manifestement excessive compte tenu notamment du fait que, comme l'indique le Conseil, les enquêtes pouvant être menées à la suite d'attentats terroristes ou d'autres crimes graves durent parfois plusieurs années. Aussi, s'il est en principe souhaitable que des données à caractère personnel soient conservées pendant une courte période, convient-il, dans la présente affaire, de mettre en perspective la durée de stockage des données issues de PNR avec l'utilité qu'elles présentent, non seulement à des fins de prévention du terrorisme, mais plus largement à des fins répressives.

243. Eu égard à ces considérations, le régime de stockage des données, tel qu'il est prévu au paragraphe 15 de la déclaration d'engagement, ne nous paraît pas constituer une méconnaissance patente du droit au respect de la vie privée.

244. En troisième lieu, le Parlement reproche au régime PNR de ne pas prévoir de contrôle juridictionnel concernant le traitement des données à caractère personnel par les autorités américaines.

245. Nous notons que tant la convention n° 108 que la directive 95/46 prévoient l'existence d'un recours juridictionnel en cas de violation des dispositions de droit national appliquant les règles contenues dans ces deux instruments juridiques (119).

246. Au regard de l'article 8, paragraphe 2, de la CEDH, nous sommes d'avis que les règles définies aux paragraphes 36 et suivants de la déclaration d'engagement, qui prévoient une série de garanties en termes d'information, d'accès aux données et de voies de recours pour les passagers aériens concernés, permettent d'éviter d'éventuels abus. L'ensemble de ces garanties nous conduisent à considérer que, eu égard à la grande marge d'appréciation qui doit, selon nous, être reconnue en l'espèce au Conseil et à la Commission, l'ingérence dans la vie privée des passagers aériens est proportionnée au but légitime poursuivi par le régime PNR.

247. Plus précisément, il y a lieu de noter que, outre les renseignements d'ordre général que le CBP s'est engagé à porter à la connaissance des passagers aériens (120), le paragraphe 37 de la déclaration d'engagement prévoit que les personnes concernées peuvent, conformément à la loi sur la liberté de l'information (121), obtenir copie des informations issues de PNR les concernant qui figurent dans les bases de données du CBP (122).

248. Certes, le paragraphe 38 de la déclaration d'engagement prévoit la faculté pour le CBP, «[d]ans certaines circonstances exceptionnelles», de refuser ou de reporter la divulgation de la totalité ou d'une partie d'un dossier PNR, par exemple lorsqu'une telle divulgation «est de nature à entraver une action répressive» ou bien si elle «aurait pour effet de révéler au grand jour des techniques ou procédures propres aux enquêtes judiciaires». Cependant, outre le fait que cette faculté dont peut user le CBP est encadrée par la loi, il importe de remarquer que, aux termes du même paragraphe de la déclaration d'engagement, le FOIA «prévoit que tout demandeur est habilité à contester, par *un recours administratif ou judiciaire*, la décision du CBP de ne pas communiquer certaines informations» (123).

249. En outre, s'agissant des demandes de rectification de données PNR contenues dans la base de données du CBP et des plaintes de particuliers concernant le traitement par ce dernier de leurs données PNR, le paragraphe 40 de la déclaration d'engagement précise qu'elles doivent être envoyées à l'«Assistant Commissioner» du CBP (124).

250. Dès lors qu'une plainte ne peut être tranchée par le CBP, elle doit être envoyée au «haut responsable de la protection de la vie privée auprès du ministère de la sécurité intérieure» («Chief Privacy Officer») (125).

251. Par ailleurs, aux termes du paragraphe 42 de la déclaration d'engagement, il est prévu que «le Bureau de la protection de la vie privée du ministère de la sécurité intérieure examinera en urgence les plaintes qui lui seront adressées par les autorités chargées de la protection des données dans les États membres de l'Union européenne pour le compte d'un résident de l'Union européenne, dans la mesure où ce résident a autorisé ces autorités à agir pour son compte et estime que sa plainte en matière de protection des données concernant les PNR n'a pas été traitée à sa satisfaction par le CBP, conformément aux paragraphes 37 à 41, ou par le Bureau de la protection de la vie privée du ministère de la sécurité intérieure».

252. Le paragraphe 42 prévoit également, d'une part, que ledit Bureau «rendra compte de ses conclusions et de toute mesure à l'autorité ou aux autorités concernées» et, d'autre part, que le Chief Privacy Officer «mentionnera, dans son rapport au Congrès des États-Unis, des renseignements quant au nombre, à la teneur et à l'issue des plaintes relatives au traitement des données à caractère personnel telles que les PNR» (126).

253. Le Parlement relève à juste titre que le Chief Privacy Officer n'est pas un organe juridictionnel. Toutefois, nous observons qu'il s'agit d'un organe administratif présentant un certain degré d'indépendance par rapport au ministère de la sécurité intérieure et dont les décisions ont un effet obligatoire (127).

254. Dès lors, la possibilité ainsi organisée pour les passagers aériens de porter plainte auprès du Chief Privacy Officer et celle de bénéficier d'un recours juridictionnel dans le cadre du FOIA constituent des garanties importantes au regard de leur droit au respect de la vie privée. En raison de ces garanties, nous estimons que le Conseil et la Commission n'ont pas dépassé les limites qui s'imposaient à leur marge d'appréciation dans le cadre de l'adoption du régime PNR.

255. Enfin, le Parlement estime que le régime PNR va au-delà de ce qui est nécessaire pour combattre le terrorisme et d'autres crimes graves, dans la mesure où il permet le transfert des données des passagers aériens à d'autres autorités publiques. Selon lui, le CBP disposerait d'un pouvoir discrétionnaire pour transmettre des données issues de PNR à d'autres autorités publiques, y compris des autorités gouvernementales étrangères, ce qui serait incompatible avec l'article 8, paragraphe 2, de la CEDH.

256. Nous ne partageons pas cet avis. En effet, là encore, les garanties qui entourent la transmission de données PNR à d'autres autorités gouvernementales permettent, selon nous, de considérer que l'ingérence dans la vie privée des passagers aériens présente un caractère proportionné en vue d'atteindre le but poursuivi par le régime PNR.

257. Même si la déclaration d'engagement reconnaît au CBP un pouvoir d'appréciation important, nous remarquons que ce pouvoir est encadré. Ainsi, en vertu du paragraphe 29 de la déclaration d'engagement, la transmission de données PNR à d'autres autorités gouvernementales «de répression ou de lutte contre le terrorisme», «qu'elles soient nationales ou étrangères», ne peut être effectuée «qu'au cas par cas» et seulement, en principe, «aux fins de prévenir ou de combattre les crimes visés au paragraphe 3». Le CBP doit, en vertu du paragraphe 30 de ladite déclaration, vérifier si la raison invoquée pour la divulgation des données à une autre autorité est conforme à ces finalités.

258. Certes, les paragraphes 34 et 35 de la déclaration d'engagement procèdent à un élargissement desdites finalités dans la mesure où ils ont pour effet de permettre, respectivement, d'une part, l'utilisation ou la divulgation de données PNR aux autorités gouvernementales compétentes «lorsque cette divulgation est essentielle à la protection des intérêts vitaux de la personne concernée ou d'autres personnes,

notamment dans le cas de risques sanitaires graves» et, d'autre part, l'utilisation ou la divulgation de données PNR «dans le cadre d'une procédure pénale ou au titre d'autres exigences prévues par la loi».

259. Toutefois, outre que ces finalités sont en grande partie liées au but légitime poursuivi par le régime PNR, nous observons que la déclaration d'engagement contient un certain nombre de garanties. Ainsi, par exemple, le paragraphe 31 de celle-ci prévoit que, «[a]fin de réguler la diffusion de données de PNR pouvant être transmises à d'autres autorités désignées, le CBP est considéré comme étant 'propriétaire' des données et les autorités désignées sont soumises, en vertu des conditions expresses de diffusion» à plusieurs obligations. Parmi ces obligations pesant sur les autorités destinataires des données, figurent notamment celle de «veiller à l'élimination systématisée des données de PNR communiquées, dans le respect des procédures de conservation mises en œuvre par l'autorité désignée», et celle d'«obtenir l'autorisation expresse du CBP avant toute nouvelle diffusion».

260. En outre, le paragraphe 32 de la déclaration d'engagement précise que «[t]oute divulgation de données de PNR par le CBP est effectuée sous réserve que l'agence destinataire traite les données en question comme des informations confidentielles à caractère commercial et sensibles au regard de l'exécution des lois ou comme des informations confidentielles à caractère personnel pour les passagers […] qu'il convient de considérer comme échappant à la divulgation prévue par la loi sur la liberté de l'information […]». De plus, il est indiqué au même paragraphe que «l'agence destinataire sera informée que toute divulgation ultérieure des informations concernées est interdite sans l'autorisation préalable expresse du CBP», celui-ci n'autorisant en outre «aucun transfert ultérieur de données de PNR à des fins autres que celles prévues aux [paragraphes] 29, 34 ou 35». Enfin, le paragraphe 33 de la déclaration d'engagement dispose que «[l]es membres du personnel des autorités désignées qui divulguent des données de PNR sans autorisation appropriée s'exposent à des sanctions pénales».

261. La prise en compte de l'ensemble de ces garanties exclut, à notre avis, de considérer que le Conseil et la Commission ont dépassé les limites de la grande marge d'appréciation qui doit, selon nous, leur être reconnue aux fins de lutter contre le terrorisme et d'autres crimes graves.

262. Il en résulte que les moyens tirés de la violation du droit à la protection des données à caractère personnel et de la violation du principe de proportionnalité ne sont pas fondés et doivent, par conséquent, être rejetés.

D – *Sur le moyen tiré de ce que la décision du Conseil ne serait pas suffisamment motivée*

263. Le Parlement fait valoir que la décision du Conseil ne remplit pas l'exigence de motivation telle qu'elle résulte de l'article 253 CE. En particulier, il reproche à ladite décision de ne contenir aucune motivation expliquant si, et dans quelle mesure, cet acte a pour objet le fonctionnement du marché intérieur.

264. En revanche, le Conseil, soutenu par le Royaume-Uni et la Commission, estime que la motivation de sa décision est conforme aux exigences posées par la Cour.

265. Nous considérons que, même si elle présente un caractère succinct, la motivation de la décision du Conseil est suffisante.

266. Selon une jurisprudence constante, la motivation exigée par l'article 253 CE «doit être adaptée à la nature de l'acte en cause et doit faire apparaître de façon claire et non équivoque le raisonnement de l'institution, auteur de l'acte, de manière à permettre aux intéressés de connaître les justifications de la mesure prise et à la Cour d'exercer son contrôle». Il résulte en outre de cette jurisprudence qu'«il n'est pas exigé que la motivation spécifie tous les éléments de fait et de droit pertinents, dans la mesure où la question de savoir si la motivation d'un acte satisfait aux exigences [de

l'article 253 CE] doit être appréciée non seulement au regard de son libellé, mais aussi de son contexte ainsi que de l'ensemble des règles juridiques régissant la matière concernée» (128).

267. Concernant la nature de l'acte, il convient de rappeler qu'il s'agit d'une décision ayant pour principal objet d'approuver au nom de la Communauté l'accord entre cette dernière et les États-Unis. Ladite décision contient à cet égard les précisions nécessaires relatives à la procédure suivie, à savoir une adoption par le Conseil conformément à la procédure définie à l'article 300, paragraphe 2, premier alinéa, CE ainsi que l'indication selon laquelle le Parlement n'a pas émis son avis dans le délai qui lui avait été fixé par le Conseil en vertu de l'article 300, paragraphe 3, premier alinéa, CE. En outre, nous observons que la décision du Conseil mentionne dans ses visas l'article 95 CE.

268. De plus, compte tenu de la nature particulière de ladite décision, qu'il est difficile d'isoler complètement de l'accord international sur lequel elle porte, la vérification du caractère suffisant de la motivation doit, selon nous, intégrer également le préambule de l'accord lui-même. À cet égard, la lecture combinée de la décision du Conseil et du préambule de l'accord permettent, comme le démontre l'examen des moyens précédents, à la Cour d'exercer son contrôle, notamment quant au caractère approprié de la base juridique choisie.

269. En conséquence, nous estimons que le moyen tiré de ce que la décision du Conseil ne serait pas suffisamment motivée n'est pas fondé et doit donc être rejeté.

E – *Sur le moyen tiré de la violation du principe de coopération loyale prévu à l'article 10 CE*

270. Par ce moyen, le Parlement soutient que, même si l'article 300, paragraphe 3, premier alinéa, CE permet au Conseil de lui fixer, en fonction de l'urgence, un délai pour qu'il émette son avis, et que la procédure de demande d'avis préalable à la Cour, prévue à l'article 300, paragraphe 6, CE, n'a pas un caractère suspensif, le Conseil aurait méconnu, dans le cadre de la procédure d'adoption de l'accord, le devoir de coopération loyale que lui impose l'article 10 CE.

271. Le Conseil, soutenu par la Commission et le Royaume-Uni, estime, quant à lui, qu'il n'a pas violé le principe de coopération loyale en concluant l'accord alors que le Parlement avait saisi la Cour d'une demande d'avis en vertu de l'article 300, paragraphe 6, CE.

272. L'article 10 CE fait peser sur les États membres un devoir de coopération loyale vis-à-vis des institutions communautaires, mais ne consacre pas expressément le principe de coopération loyale entre lesdites institutions. Toutefois, la Cour a estimé que, dans le cadre du dialogue interinstitutionnel, sur lequel repose notamment la procédure de consultation, prévalent les mêmes devoirs réciproques de coopération loyale que ceux qui régissent les relations entre les États membres et les institutions communautaires» (129).

273. Il ressort du cadre factuel de la présente affaire que le 17 mars 2004, la Commission a transmis au Parlement la proposition de décision du Conseil et que, par lettre du 25 mars 2004, le Conseil a demandé au Parlement de rendre son avis sur cette proposition pour le 22 avril 2004 au plus tard. Dans sa lettre, le Conseil souligne que «[l]a lutte contre le terrorisme, qui justifie les mesures proposées, est une priorité essentielle de l'Union européenne. Actuellement, les transporteurs aériens et les passagers sont dans une situation d'incertitude à laquelle il convient de remédier d'urgence. En plus, il est essentiel de protéger les intérêts financiers des parties concernées».

274. Le 21 avril 2004, le Parlement a décidé, conformément à l'article 300, paragraphe 6, CE, de recueillir l'avis de la Cour sur la compatibilité de l'accord envisagé avec les dispositions du traité.

275. Le 28 avril 2004, le Conseil, en se fondant sur l'article 300, paragraphe 3, premier alinéa, CE, a adressé une lettre au Parlement lui demandant de rendre son avis sur la conclusion de l'accord avant le 5 mai 2004. Pour justifier l'urgence, le Conseil a repris les motifs indiqués dans sa lettre du 25 mars 2004.

276. Cette demande d'urgence a été rejetée par le Parlement, dont le président a par ailleurs appelé le Conseil et la Commission à ne pas poursuivre dans leurs intentions tant que le Cour n'aurait pas rendu l'avis sollicité le 21 avril 2004. Le Conseil a malgré tout adopté la décision contestée le 17 mai 2004.

277. Nous ne pensons pas que le Conseil ait violé son obligation de coopération loyale vis-à-vis du Parlement en adoptant cette décision d'approuver l'accord au nom de la Communauté avant l'aboutissement de la procédure de demande d'avis à la Cour introduite par le Parlement en vertu de l'article 300, paragraphe 6, CE.

278. En effet, comme le reconnaît d'ailleurs le Parlement lui-même, l'introduction d'une telle procédure de demande d'avis à la Cour n'a pas un caractère suspensif. Elle n'empêche donc pas le Conseil de prendre la décision d'approuver l'accord alors que ladite procédure est encore en cours, et ce quand bien même le délai qui sépare l'introduction de la demande d'avis à la Cour et la décision approuvant l'accord est, comme en l'espèce, relativement bref.

279. Il convient à cet égard d'indiquer que l'absence de caractère suspensif d'une demande d'avis à la Cour, introduite en vertu de l'article 300, paragraphe 6, CE, peut être déduite tant du libellé de cet article, qui ne prévoit pas expressément un tel caractère suspensif, que de la jurisprudence de la Cour. En effet, celle-ci a jugé dans son avis 3/94 (130) qu'une telle demande d'avis devient sans objet, et qu'il n'y a pas lieu pour la Cour d'y répondre, lorsque l'accord sur lequel elle porte, qui était un accord envisagé lors de la saisine de la Cour, a entre temps été conclu. Elle a également précisé, d'une part, que la procédure de l'article 300, paragraphe 6, CE «vise, en premier lieu, […] à prévenir les difficultés résultant de l'incompatibilité avec le traité d'accords internationaux engageant la Communauté et *non pas à protéger les intérêts et les droits de l'État membre ou de l'institution communautaire à l'origine de la demande d'avis*» (131) et, d'autre part, que, «[e]n toute hypothèse, l'État ou l'institution communautaire à l'origine de la demande d'avis dispose de la voie du recours en annulation contre la décision du Conseil de conclure l'accord […]» (132).

280. Par ailleurs, il ressort tant des pièces du dossier que du deuxième considérant de la décision du Conseil que ce dernier a suffisamment motivé l'urgence dont il s'est prévalu pour obtenir dans un court délai l'avis du Parlement, conformément à l'article 300, paragraphe 3, premier alinéa, CE. Nous notons enfin que ce dernier article prévoit expressément que, «[e]n l'absence d'avis dans ce délai, le Conseil peut statuer».

281. Compte tenu de l'ensemble de ces éléments, nous estimons que le moyen tiré de la violation par le Conseil de son devoir de coopération loyale n'est pas fondé et doit donc être rejeté.

VII – Sur les dépens

282. Dans l'affaire C-318/04, le bien-fondé du recours engagé par le Parlement implique que la Commission soit condamnée aux dépens, conformément aux dispositions de l'article 69, paragraphe 2, du règlement de procédure de la Cour. De plus, en application de l'article 69, paragraphe 4, du même règlement, les parties intervenantes, à savoir le Royaume-Uni et le CEPD, supportent leurs propres dépens.

283. Dans l'affaire C-317/04, le bien-fondé du recours engagé par le Parlement implique que le Conseil soit condamné aux dépens, conformément aux dispositions de l'article 69, paragraphe 2, du règlement de procédure de la Cour. De plus, en application de l'article 69, paragraphe 4, du même règlement, les parties

intervenantes, à savoir le Royaume-Uni, la Commission et le CEPD, supportent leurs propres dépens.

VIII – Conclusion

284. Eu égard à l'ensemble des considérations qui précèdent, nous proposons à la Cour:

– dans le cadre de l'affaire C-318/04, d'annuler 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;

– dans le cadre de l'affaire C-317/04, d'annuler 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.

---

1 – Langue originale: le français.

---

2 – Décision 2004/496/CE (JO L 183, p. 83, ci-après la «décision du Conseil»).

---

3 – Décision 2004/535/CE (JO L 235, p. 11, ci-après la «décision d'adéquation»).

---

4 – Cette problématique concerne également les relations de la Communauté avec d'autres pays tiers. Ainsi, nous signalons qu'un accord du même type que celui en cause dans l'affaire C-317/04 a été signé entre la Communauté européenne et le Canada le 3 octobre 2005.

---

5 – Voir Aviation and Transportation Security Act (ATSA) du 19 novembre 2001 (Public Law 107-71, 107th Congress, titre 49, section 44909(c)(3) du code des États-Unis). Cette loi a été suivie par des règlements de mise en œuvre adoptés par le Bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (United States Bureau of Customs and Border Protection, ci-après le «CBP»), tels que le Passenger and Crew Manifests Required for Passengers Flights in Foreign Air Transportation to the United States, publié au *Federal Register* (registre fédéral américain) le 31 décembre 2001, et le Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, publié au *Federal Register* le 25 juin 2002 (titre 19, section 122.49b du code des règlements fédéraux).

---

6 – Règlement (CEE) n° 2299/89 du Conseil, du 24 juillet 1989, instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation (JO L 220, p. 1), tel que modifié par le règlement (CE) n° 323/1999 du Conseil, du 8 février 1999 (JO L 40, p. 1).

7 – JO L 281, p. 31, directive telle que modifiée par le règlement (CE) n° 1882/2003 du Parlement européen et du Conseil, du 29 septembre 2003, portant adaptation à la décision 1999/468/CE du Conseil des dispositions relatives aux comités assistant la Commission dans l'exercice de ses compétences d'exécution prévues dans des actes soumis à la procédure visée à l'article 251 du traité CE (JO L 284, p. 1).

8 – Ce groupe de travail a été institué en vertu de l'article 29 de la directive 95/46. Il s'agit d'un organe consultatif indépendant qui intervient dans le domaine de la protection des personnes à l'égard du traitement des données à caractère personnel. Ses missions sont définies à l'article 30 de ladite directive ainsi qu'à l'article 15, paragraphe 3, 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 L 201, p. 37).

9 – Avis 4/2003 sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers. Voir site Internet:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_fr.htm.

10 – Avis 2/2004 sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (US CBP). Voir site Internet:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2004_fr.htm.

11 – Décision 1999/468/CE (JO L 184, p. 23).

12 – Voir point 8 des présentes conclusions.

13 – Dans ses requêtes, le Parlement justifie ce rejet par le constat d'une absence persistante de l'ensemble des versions linguistiques de la proposition de décision du Conseil.

14 – Cette demande d'avis a été radiée du registre de la Cour par ordonnance du président de la Cour du 16 décembre 2004.

15 – Série des traités européens, n° 108 (ci-après la «convention n° 108»). Cette convention est entrée en vigueur le 1er octobre 1985. Des amendements à cette convention ont été adoptés par le comité des ministres du Conseil de l'Europe le 15 juin 1999, afin de permettre l'adhésion des Communautés européennes (ces amendements n'ont pas,

à ce jour, été acceptés par tous les États parties à la convention n° 108). Voir également protocole additionnel à la convention n° 108, concernant les autorités de contrôle et les flux transfrontières de données, ouvert à la signature le 8 novembre 2001 et entré en vigueur le 1er juillet 2004 (série des traités européens, n° 181).

16 – JO 2000, C 364, p. 1. Cette charte, qui a été signée et proclamée par les présidents du Parlement, du Conseil et de la Commission lors du Conseil européen de Nice, le 7 décembre 2000, figure dans la partie II du traité établissant une Constitution pour l'Europe, non encore entré en vigueur à ce jour (JO 2004, C 310, p. 41). Ainsi que le Tribunal de première instance des Communautés européennes a pu le souligner, «bien que n'étant pas dotée de force juridique contraignante, [la charte des droits fondamentaux de l'Union européenne] démontre l'importance, dans l'ordre juridique communautaire, des droits qu'elle énonce». Voir arrêt du 15 janvier 2003, Philip Morris International e.a./Commission (T-377/00, T-379/00, T-380/00, T-260/01 et T-272/01, Rec. p. II-1, point 122).

17 – Quant au paragraphe 2 de l'article 286 CE, il est rédigé comme suit:

«Avant la date visée au paragraphe 1, le Conseil, statuant conformément à la procédure visée à l'article 251, institue un organe indépendant de contrôle chargé de surveiller l'application desdits actes communautaires aux institutions et organes communautaires, et adopte, le cas échéant, toute autre disposition utile».

Sur la base de l'article 286 CE, a été adopté le règlement (CE) n° 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO 2001, L 8, p. 1).

18 – Pour une présentation détaillée du contexte général dans lequel a été élaborée cette directive et des dispositions de celle-ci, voir de Boulanger, M.-H., de Terwangne, C., Léonard, T., Louveaux, S., Moreau, D., et Poullet, Y., «La protection des données à caractère personnel en droit communautaire», JTDE, 1997, nos40, 41 et 42. Voir également Simitis, S., *Data Protection in the European Union − the Quest for Common Rules*, Collected Courses of the Academy of European Law, Volume VIII, Book I, 2001, p. 95. Nous soulignons également qu'une directive spécifique, à savoir la directive 2002/58, est destinée à régir le secteur des communications électroniques.

19 – Septième considérant.

20 – Huitième considérant.

21 – Neuvième considérant.

22 – À titre d'exemple, on peut citer les flux de données liés à la mobilité des personnes, au commerce électronique et à des transmissions à l'intérieur d'un groupe d'entreprises.

23 – Cinquante-septième considérant de la directive 95/46.

24 – Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les Gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990 (JO 2000, L 239, p. 19).

25 – Voir articles 102 à 118 de ladite convention. S'agissant du système d'information Schengen de deuxième génération (SIS II), la Commission a présenté des propositions en vue de l'adoption d'une décision du Conseil [COM(2005) 230 final], et de deux règlements [COM(2005) 236 final et COM(2005) 237 final].

26 – JO 1995, C 316, p. 2, ci-après la «convention Europol».

27 – Décision 2002/187/JAI, du 28 février 2002, instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité (JO L 63, p. 1, ci-après la «décision Eurojust»). Voir articles 14 et suiv. de ladite décision.

28 – JO 2005, C 68, p. 1.

29 – JO 1995, C 316, p. 34. Voir, en particulier, articles 13 à 15, 17 et 18 de ladite convention.

30 – Acte du Conseil, du 29 mai 2000, établissant, conformément à l'article 34 du traité sur l'Union européenne, cette convention (JO 2000, C 197, p. 1). Voir, notamment, article 23 de celle-ci.

31 – COM(2005) 475 final. Cette proposition de décision-cadre est fondée sur les articles 30 UE, 31 UE et 34, paragraphe 2, sous b), UE. Elle constitue l'une des mesures prévues par le plan d'action du Conseil et de la Commission mettant en œuvre le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne (JO 2005, C 198, p. 1, paragraphe 3.1).

32 – S'agissant d'une mesure d'exécution de la directive 95/46, la décision d'adéquation a été arrêtée conformément à la procédure prévue à l'article 31, paragraphe 2, de cette directive qui, lui-même, impose l'application des articles 4, 7 et 8 de la décision 1999/468. Ainsi, lorsqu'elle adopte une mesure d'exécution de ladite directive, la Commission est assistée par un comité composé des représentants des États membres et présidé par le représentant de la Commission. Il s'agit en l'espèce du comité dit «article 31».

33 – Voir paragraphe 47 de la déclaration d'engagement.

34 – Il s'agit des rubriques suivantes: «1) Code repère du dossier PNR; 2) Date de réservation; 3) Date(s) prévue(s) du voyage; 4) Nom; 5) Autres noms figurant dans le PNR; 6) Adresse; 7) Modes de paiement; 8) Adresse de facturation; 9) Numéros de téléphone; 10) Itinéraire complet pour le PNR spécifique; 11) Informations 'grands voyageurs' [uniquement miles parcourus et adresse(s)]; 12) Agence de voyage; 13) Agent de voyage; 14) Informations du PNR sur le partage de codes; 15) «Statut» du voyageur (*Travel status of passenger*); 16) PNR scindé/divisé; 17) Adresse électronique; 18) Informations sur l'établissement des billets; 19) Observations générales; 20) Numéro du billet; 21) Numéro du siège occupé; 22) Date d'émission du billet; 23) Passager répertorié comme défaillant; 24) Numéros d'étiquetage des bagages; 25) Passager de dernière minute sans réservation; 26) Données OSI ['Other Service Information']; 27) Données SSI/SSR ['Special Service Request']; 28) Informations sur la source; 29) Historique des changements apportés au PNR; 30) Nombre de voyageurs dans le PNR; 31) Informations relatives au siège occupé; 32) Allers simples; 33) Informations APIS ['Advanced Passenger Information System'] éventuellement recueillies; 34) Données ATFQ ['Automatic Ticket Fare Quote']».

35 – Ci-après l'«accord».

36 – Voir information relative à la date d'entrée en vigueur de l'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, C 158, p. 1).

37 – Il convient à cet égard de relever que le préambule de l'accord mentionne une référence erronée de la décision d'adéquation. Il s'agit en vérité de la décision 2004/535/CE du 14 mai 2004, notifiée sous le numéro C(2004) 1914, et non de la décision C(2004) 1799 du 17 mai 2004. Cette erreur a fait l'objet d'un rectificatif publié au *Journal officiel de l'Union européenne.* Voir procès-verbal de rectification de l'accord (JO 2005, L 255, p. 168).

38 – La transmission des données par les transporteurs aériens correspond à ce qu'il est convenu d'appeler le système «push», tandis que l'accès direct du CBP à ces données correspond au système «pull».

39 – Il s'agit de la décision d'adéquation, seule «décision» visée dans le préambule de l'accord.

40 – Même remarque qu'à la note précédente.

41 – Paragraphe 5 de l'accord.

42 – Paragraphe 6 de l'accord.

43 – Respectivement, ordonnances du président de la Cour des 18 janvier 2005 et 18 novembre 2004.

44 – Ordonnance de la Cour du 17 mars 2005.

45 – Ordonnance du président de la Cour du 17 décembre 2004.

46 – Ordonnance de la Cour du 17 mars 2005.

47 – Arrêt du 6 novembre 2003, Lindqvist (C-101/01, Rec. p. I-12971, point 63).

48 – Nous rappelons que, parmi ces facteurs, figurent notamment la nature des données ainsi que la finalité et la durée du ou des traitements envisagés.

49 – Arrêt Lindqvist, précité, point 56. Dans cette affaire, la Cour a jugé que l'inscription sur une page Internet de données à caractère personnel, du seul fait qu'elle les rend accessibles aux personnes se trouvant dans un pays tiers, ne constitue pas un «transfert vers un pays tiers» au sens de l'article 25 de la directive 95/46. Pour arriver à cette conclusion, la Cour a tenu compte, d'une part, de la nature technique des opérations en cause et, d'autre part, de l'objectif ainsi que de l'économie du chapitre IV de ladite directive, au sein duquel figure l'article 25.

50 – Et ce quand bien même les données sont reçues par une composante spécifique de la structure administrative interne dudit pays tiers.

51 – Il est intéressant d'observer que les notions de traitement et de transfert de données à caractère personnel se recoupent dans une certaine mesure. Ainsi, la communication par transmission, la diffusion ou la mise à disposition de telles données nous paraissent être susceptibles de constituer à la fois un traitement et un transfert de celles-ci au sens de ladite directive. Dans la présente affaire, les notions de transfert et de traitement se recoupent dans la mesure où le régime institué a notamment pour objet la mise à la disposition du CBP des données PNR. Ce constat s'explique, à notre avis, par la définition très large du traitement qui couvre un panel étendu d'opérations. Au final, dans une telle hypothèse, le transfert de données vers un pays tiers s'analyse comme une forme spécifique de traitement. En ce sens, voir proposition de décision-cadre de la Commission: son article 15, relatif au «[t]ransfert aux autorités compétentes de pays tiers ou à des instances internationales», fait partie du chapitre III intitulé «Formes spécifiques de traitement».

52 – Nous observons, à titre d'exemple, que la décision 2000/519/CE de la Commission, du 26 juillet 2000, relative à la constatation, conformément à la directive 95/46, du caractère adéquat de la protection des données à caractère personnel en Hongrie (JO L 215, p. 4), dispose, à son article 1er, que, «[a]ux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, la Hongrie est considérée comme offrant un niveau de protection adéquat des données à caractère personnel transférées à partir de la Communauté *pour toutes les activités entrant dans le champ d'application de ladite directive*» (souligné par nous).

---

53 – Souligné par nous. Dans son arrêt Lindqvist, précité, la Cour a observé que «[l]es activités mentionnées à titre d'exemples à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 […] sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers» (point 43).

---

54 – Sixième considérant.

---

55 – Septième considérant.

---

56 – Huitième considérant.

---

57 – Voir, en ce sens, article de Poullet, Y., et Peres Asinan, M. V., «Données des voyageurs aériens: le débat Europe – États-Unis», JTDE, 2004, n° 113, p. 274. Selon ces auteurs, «la solution qui légitimera ces flux transfrontières d'un type bien particulier doit garantir la validité d'un transfert des données à des administrations publiques étrangères accompli dans le but de combattre le terrorisme […], ce qui excède notoirement le champ d'application d'une directive du premier pilier». Ils ajoutent que «[c]eci correspond, au niveau européen, à une matière de troisième pilier, ce qui remet en cause la compétence de la Commission à agir en la matière […]». Voir également De Schutter, O., «La Convention européenne des droits de l'homme à l'épreuve de la lutte contre le terrorisme», dans *Lutte contre le terrorisme et droits fondamentaux*; Bribosia, E., et Weyembergh, A. (dir.), Collection droit et justice, Bruylant, Bruxelles, 2002, p. 112, note n° 43: après avoir cité l'article 3, paragraphe 2, premier tiret, de la directive 95/46, l'auteur remarque que «[c]ette restriction au champ d'applicabilité de la [d]irective s'explique par le caractère limité des compétences de la Communauté européenne, laquelle ne dispose pas d'une compétence générale à légiférer dans le domaine des droits de l'homme, mais peut agir dans ce domaine notamment là où, et dans la mesure où, comme c'est le cas avec [ladite directive], il s'agit de faciliter l'établissement d'un marché intérieur impliquant notamment l'élimination des entraves à la libre circulation des marchandises et à la libre prestation des services».

---

58 – Les données PNR font l'objet d'un traitement à l'intérieur de la Communauté, qui consiste dans leur mise à la disposition du CBP. Elles sont également destinées à faire l'objet d'un traitement après leur transfert, en raison de leur utilisation par le CBP.

---

59 – Cela ne signifie pas qu'une décision d'adéquation adoptée dans un contexte semblable à celui de la présente affaire devrait, dans l'ordre juridique de l'Union européenne, être considérée comme exonérée du respect des garanties essentielles en matière de protection des données à caractère personnel, telles qu'elles sont notamment énumérées dans la convention n° 108. Seulement, dans cette perspective, nous estimons que la directive 95/46 ne constitue pas la norme de référence appropriée dès lors que, comme nous l'avons vu, le but de la décision d'adéquation déborde le champ d'application de la norme de base que constitue ladite directive. Dès lors, en l'absence de norme de droit dérivé applicable dans le cas d'un traitement de données à caractère personnel à des fins répressives et de sécurité publique, il n'est pas possible de procéder à un contrôle juridictionnel abstrait desdites garanties. Dans un tel cas de figure, la protection juridictionnelle n'est toutefois pas absente. En effet, la vérification des garanties essentielles en matière de protection des données à caractère personnel est, comme nous le verrons, étroitement liée à l'examen des conditions posées par l'article 8, paragraphe 2, de la CEDH.

---

60 – Ci-après le «régime PNR».

---

61 – Arrêt du 31 mars 1971, Commission/Conseil, dit «AETR» (22/70, Rec. p. 263).

---

62 – Voir, notamment, arrêts du 11 juin 1991, Commission/Conseil, dit «Dioxyde de titane» (C-300/89, Rec. p. I-2867, point 10); du 12 novembre 1996, Royaume-Uni/Conseil (C-84/94, Rec. p. I-5755, point 25); du 25 février 1999, Parlement/Conseil (C-164/97 et C-165/97, Rec. p. I-1139, point 12); du 4 avril 2000, Commission/Conseil (C-269/97, Rec. p. I-2257, point 43); du 19 septembre 2002, Huber (C-336/00, Rec. p. I-7699, point 30); du 29 avril 2004, Commission/Conseil (C-338/01, Rec. p. I-4829, point 54), et du 13 septembre 2005, Commission/Conseil (C-176/03, non encore publié au recueil, point 45).

---

63 – Arrêt du 26 mars 1987, Commission/Conseil (45/86, Rec. p. 1493, point 11).

---

64 – Avis 2/00, du 6 décembre 2001, rendu en vertu de l'article 300, paragraphe 6, CE (Rec. p. I-9713, point 5).

---

65 – Dans les développements qui suivent, nous utiliserons l'expression de «lutte contre le terrorisme et d'autres crimes graves» pour désigner cet objectif.

---

66 – De plus, le terrorisme constitue un phénomène international qui se joue du cloisonnement des espaces.

---

67 – Voir point 10 des conclusions de l'avocat général Tesauro dans l'affaire Dioxyde de Titane, précitée.

---

68 – Arrêts du 5 octobre 2000, Allemagne/Parlement et Conseil (C-376/98, Rec. p. I-8419, points 83, 84 et 95), et du 10 décembre 2002, British American Tobacco (Investments) et Imperial Tobacco (C-491/01, Rec. p. I-11453, point 60).

---

69 – Voir, en ce sens, arrêt du 13 juillet 1995, Espagne/Conseil (C-350/92, Rec. p. I-1985, point 35), ainsi que arrêt Allemagne/Parlement et Conseil, précité (point 86); du 9 octobre 2001, Pays-Bas/Parlement et Conseil (C-377/98, Rec. p. I-7079, point 15); British American Tobacco (Investments) et Imperial Tobacco, précité (point 61), et du 14 décembre 2004, Arnold André (C-434/02, Rec. p. I-11825, point 31).

---

70 – Voir, notamment, arrêt du 9 novembre 1995, Allemagne/Conseil (C-426/93, Rec. p. I-3723, point 33).

---

71 – Voir, notamment, arrêts du 17 mars 1993, Commission/Conseil (C-155/91, Rec. p. I-939, points 19 et 21); du 23 février 1999, Parlement/Conseil (C-42/97, Rec. p. I-869, points 39 et 40); du 30 janvier 2001, Espagne/Conseil (C-36/98, Rec. p. I-779, point 59), et du 12 décembre 2002, Commission/Conseil (C-281/01, Rec. p. I-12049, point 34).

---

72 – Voir, notamment, arrêts précités Dioxyde de titane (points 13 et 17); du 23 février 1999, Parlement/Conseil (points 38 et 43); Huber (point 31), et du 12 décembre 2002, Commission/Conseil (point 35).

---

73 – Arrêt du 12 décembre 2002, Commission/Conseil, précité, point 46.

---

74 – Arrêt du 20 mai 2003, Österreichischer Rundfunk e. a. (C-465/00, C-138/01 et C-139/01, Rec. p. I-4989, point 39). Compte tenu de la différence d'objet et de finalité entre l'accord et la directive 95/46, nous estimons également qu'il est improbable que, comme le soutient la Commission, ladite directive aurait été affectée, au sens de la jurisprudence AETR, si les États membres avaient séparément ou conjointement conclu un accord de ce type en dehors du cadre communautaire.

---

75 – Nous notons que la dimension «troisième pilier» du transfert de données à caractère personnel des compagnies aériennes aux États-Unis est parfois évoquée. Ainsi, le «groupe article 29» sur la protection des données a pu, dans un avis du 24 octobre 2002 (Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis), exprimer l'opinion selon laquelle, «[f]ondamentalement, les transferts de données à destination d'autorités publiques d'un État tiers pour des raisons liées à l'ordre public de cet État devraient être appréhendés dans le contexte des mécanismes de coopération instaurés dans le troisième pilier (coopération judiciaire et policière) […]. Il apparaît important d'éviter un contournement via le premier pilier de ces mécanismes normaux de coopération instaurés dans le troisième pilier». Voir site Internet:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2002_fr.htm.

76 – S'agissant de l'échange direct d'informations entre autorités publiques, nous mentionnons la décision du Conseil, du 27 mars 2000, autorisant le directeur d'Europol à engager des négociations concernant des accords avec des États tiers et des instances non liées à l'Union européenne (JO C 106, p. 1). Sur cette base, un accord entre Europol et les États-Unis d'Amérique sur l'échange de données personnelles a été signé le 20 décembre 2002.

77 – Cette problématique se trouve être au cœur du débat interinstitutionnel actuel relatif à la rétention des données par les fournisseurs de services de téléphonie et de communications électroniques. Les prises de position antagonistes exprimées lors de ce débat, entre ceux qui défendent la prise en compte de cette problématique dans le cadre du premier pilier et ceux qui estiment, au contraire, que la matière relève du troisième pilier, témoignent à la fois de la nouveauté et de la complexité de la problématique relative à l'utilisation de données commerciales à des fins répressives. Voir, à ce sujet, projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection, la poursuite de délits et d'infractions pénales, y compris du terrorisme (projet présenté le 28 avril 2004 à l'initiative de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni), et proposition concurrente de la Commission d'une directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58, présentée le 21 septembre 2005 [document COM(2005) 438 final].

78 – Voir, s'agissant de l'imposition de sanctions économiques et financières telles que le gel des fonds à l'encontre d'individus et d'entités soupçonnés de contribuer au financement du terrorisme, arrêts du Tribunal du 21 septembre 2005, Yusuf et Al Barakaat International Foundation/Conseil et Commission (T-306/01, non encore publié au Recueil, point 152), ainsi que Kadi/Conseil et Commission (T-315/01, non encore publié au Recueil, point 116). Dans le cadre particulier de ces affaires, le Tribunal a toutefois tenu compte de «la 'passerelle' spécifiquement établie, lors de la révision résultant du traité de Maastricht, entre les actions de la Communauté portant sanctions économiques au titre des articles 60 CE et 301 CE et les objectifs du traité UE en matière de relations extérieures» (point 159 de l'arrêt T-306/01, et point 123 de l'arrêt T-315/01). De façon plus générale, il a également constaté que «la lutte contre le terrorisme international et son financement relève incontestablement des objectifs de l'Union au titre de la PESC, tels qu'ils sont définis à l'article 11 UE [...]» (point 167 de l'arrêt T-306/01, et point 131 de l'arrêt T-315/01). Nous ajoutons que, aux termes de l'article 2 UE, «[l']Union se donne pour objectifs [...] de maintenir et de développer l'Union en tant qu'espace de liberté, de sécurité et de justice au sein duquel est assurée la libre circulation des personnes, en liaison avec *des mesures appropriées en matière* de

contrôle des frontières extérieures, d'asile, d'immigration ainsi que *de prévention de la criminalité et de lutte contre ce phénomène* […]» (souligné par nous). De plus, selon l'article 29, deuxième alinéa, UE, l'objectif de l'Union consistant à offrir aux citoyens un niveau élevé de protection dans un espace de liberté, de sécurité et de justice «est atteint par *la prévention de la criminalité, organisée ou autre, et la lutte contre ce phénomène, notamment le terrorisme* […]» (souligné par nous). Sur la dimension externe de l'espace pénal européen, voir de Kerchove, G., et Weyembergh, A., *Sécurité et justice: enjeu de la politique extérieure de l'Union européenne*, éditions de l'Université de Bruxelles, 2003.

---

79 – La Cour s'est en revanche déjà prononcée sur un autre cas dans lequel l'avis conforme du Parlement est exigé, à savoir celui relatif aux «accords ayant des implications budgétaires notables pour la Communauté»: arrêt du 8 juillet 1999, Parlement/Conseil (C-189/97, Rec. p. I-4741).

---

80 – Voir Schmitter, C., «Article 228», dans Constantinesco, V., Kovar, R., et Simon, D., *Traité sur l'Union européenne, commentaire article par article*, Économica, 1995, p. 725, spécialement point 43.

---

81 – Voir, en ce sens, Schmitter, C., op. cit.

---

82 – Nous indiquons à cet égard que l'approche retenue dans le traité établissant une Constitution pour l'Europe est plus large et favorable à l'approbation du Parlement: l'article III-325 de ce traité, qui est relatif à la procédure de conclusion des accords internationaux, prévoit en effet, à son paragraphe 6, sous a), v), que le Conseil adopte la décision visant à conclure l'accord après l'approbation du Parlement, notamment dans le cas des «accords couvrant *des domaines* auxquels s'applique la procédure législative ordinaire ou la procédure législative spéciale lorsque l'approbation du Parlement européen est requise» (souligné par nous).

---

83 – Souligné par nous.

---

84 – Point 107 des présentes conclusions.

---

85 – Voir points 109 et suiv. des présentes conclusions.

---

86 – Le Parlement cite à ce propos l'arrêt du 20 mai 2003, Consorzio del Prosciutto di Parma et Salumificio S. Rita (C-108/01, Rec. p. I-5121, point 89).

---

87 – Le Parlement cite notamment à ce propos la convention Europol qui prévoit, à son article 8, paragraphe 2, le traitement de cinq données, ainsi que la directive 2004/82/CE du Conseil, du 29 avril 2004, concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO L 261, p. 24). Cette directive, qui a

pour base juridique les articles 62, paragraphe 2, sous a), CE et 63, paragraphe 3, sous b), CE, prévoit, à son article 3, l'obligation pour les transporteurs aériens de transmettre, à la demande des autorités chargées du contrôle des personnes aux frontières extérieures, un total de neuf données à caractère personnel.

88 – Il s'agit, selon lui, des rubriques n°s 11 «Informations 'grands voyageurs' [uniquement miles parcourus et adresse(s)]»; 19 «Observations générales»; 26 «Données OSI ['Other Service Information']»; 27 «Données SSI/SSR ['Special Service Request']»; 30 «Nombre de voyageurs dans le PNR», et 33 «Informations APIS ['Advanced Passenger Information System'] éventuellement recueillies».

89 – Il s'agit des rubriques n°s 19, 26 et 27 (voir note précédente).

90 – Le paragraphe 5 de la déclaration d'engagement dispose:

«En ce qui concerne les rubriques 'OSI' et 'SSI/SSR' (communément qualifiées de remarques générales et de champs ouverts), le système informatique du CBP recherchera dans ces champs la présence d'autres éléments d'information énumérés [dans la liste des rubriques des données PNR demandées]. Le personnel du CBP ne sera pas autorisé à parcourir manuellement la totalité des champs OSI et SSI/SSR, sauf si la personne faisant l'objet d'un PNR est considérée par le CBP comme présentant un risque élevé au regard de l'un des objectifs spécifiés au paragraphe 3».

91 – Le paragraphe 9 de la déclaration d'engagement prévoit:

«Le CBP n'utilisera pas de données 'sensibles' figurant dans les PNR, à savoir des données personnelles révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques et l'appartenance à un syndicat ainsi que des données relatives à l'état de santé ou la vie sexuelle de la personne».

Le paragraphe 10 de ladite déclaration dispose:

«Le CBP mettra en œuvre, dans les délais les plus brefs, un système informatisé filtrant et supprimant des PNR certains codes et termes 'sensibles' identifiés par le CBP après consultation de la Commission[…]».

Le paragraphe 11 de la même déclaration est rédigé comme suit:

«Dans l'attente de la mise en œuvre de ces filtres informatiques, le CBP affirme qu'il n'utilise et n'utilisera pas d'informations 'sensibles' des PNR et s'engage à supprimer de telles données de toute divulgation discrétionnaire de PNR en vertu des paragraphes 28 à 34».

Ces derniers paragraphes sont relatifs à la transmission de données PNR à d'autres autorités gouvernementales.

---

92 – Voir, notamment, arrêts du 12 novembre 1969, Stauder (29/69, Rec. p. 419, point 7); du 17 décembre 1970, Internationale Handelsgesellschaft (11/70, Rec. p. 1125, point 4), et du 14 mai 1974, Nold/Commission (4/73, Rec. p. 491, point 13).

---

93 – Voir, notamment, arrêts du 18 juin 1991, ERT (C-260/89, Rec. p. I-2925, point 41); du 29 mai 1997, Kremzow (C-299/95, Rec. p. I-2629, point 14), et du 6 mars 2001, Connolly/Commission (C-274/99 P, Rec. p. I-1611, point 37).

---

94 – Arrêt du 13 juillet 1989, Wachauf (5/88, Rec. p. 2609, point 19).

---

95 – Arrêt du 26 juin 1980, National Panasonic/Commission (136/79, Rec. p. 2033, points 18 et 19). Ce droit comporte notamment le droit à la protection du secret médical [voir arrêts du 8 avril 1992, Commission/Allemagne (C-62/90, Rec. p. I-2575), et du 5 octobre 1994, X/Commission (C-404/92 P, Rec. p. I-4737)]. S'agissant du droit à la protection des données à caractère personnel, nous mentionnons à nouveau les arrêts Österreichischer Rundfunk e.a. et Lindqvist, précités.

---

96 – Voir Cour eur. D. H., arrêt Kruslin c. France du 24 avril 1990, série A n° 176, § 27.

---

97 – Voir Cour eur. D. H., arrêt Olsson c. Suède du 24 mars 1988, série A n° 130, § 61 et 62. Les restrictions doivent être prévues par des dispositions normatives libellées de façon suffisamment précise pour permettre aux intéressés de régler leur conduite en s'entourant au besoin de conseils éclairés (Cour eur. D. H., arrêt Sunday Times c. Royaume-Uni du 26 avril 1979, série A n° 30, § 49).

---

98 – Voir sixième considérant de la décision d'adéquation ainsi que ses notes 2 et 3.

---

99 – Voir paragraphes 36 à 42 de la déclaration d'engagement.

---

100 – Voir procès-verbal de rectification de l'accord qui, rappelons-le, a été publié au JO L 255 du 30 septembre 2005.

---

101 – Nous rappelons que le préambule de l'accord évoque la prévention et le combat contre le terrorisme «et les délits qui y sont liés, ainsi que d'autres délits graves de nature transnationale, notamment la criminalité organisée». De plus, le paragraphe 3 de la déclaration d'engagement dispose que «[l]e CBP utilise les données de PNR dans le but unique de prévenir et de combattre: 1) le terrorisme et les crimes liés au terrorisme; 2) d'autres crimes graves, y compris la criminalité organisée, qui, par nature, revêtent un caractère transnational, et 3) la fuite en cas

de mandat d'arrêt ou de mise en détention pour l'un des crimes susmentionnés». Dans les mêmes termes, voir également quinzième considérant de la décision d'adéquation.

---

102 – Voir, notamment, Cour eur. D. H., arrêt Gillow c. Royaume-Uni du 24 novembre 1986, série A n° 109, § 55.

---

103 – Voir Cour eur. D. H., arrêt Leander c. Suède du 26 mars 1987, série A n° 116, § 59.

---

104 – Voir, par exemple, Cour eur. D. H., arrêt Klass du 6 septembre 1978, série A n° 28, § 59, à propos de la surveillance secrète de la correspondance et des télécommunications des citoyens aux fins de lutte contre le terrorisme. Dans cet arrêt, ladite Cour a jugé «inhérente au système de la Convention une certaine forme de conciliation entre les impératifs de la défense de la société démocratique et ceux de la sauvegarde des droits individuels».

---

105 – Sudre, F., *Droit européen et international des droits de l'homme*, 7e édition refondue, PUF, 2005, p. 219. L'auteur constate également que, «[s]elon qu'elle énonce plus ou moins strictement la condition de proportionnalité – proportion rigoureuse, juste, raisonnable –, la Cour européenne module l'intensité de son contrôle et, en conséquence, fait varier l'étendue de la marge d'appréciation de l'État […]».

---

106 – Voir Cour eur. D. H., arrêt Z. c. Finlande du 25 février 1997, *Recueil des arrêts et décisions* 1997-I.

---

107 – En ce sens, Sudre, F., op. cit., p. 219. Voir également Wachsmann, P., «Le droit au secret de la vie privée», dans *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Sudre, S. (dir.), Bruylant, 2005, p. 141: à propos de l'arrêt Z. c. Finlande, précité, l'auteur note que «[l]e contrôle de la nécessité de l'ingérence est en l'espèce exercé avec rigueur, ce qu'explique le caractère extrêmement sensible de la question de la révélation à des tiers de la séropositivité d'une personne».

---

108 – Arrêt Leander c. Suède, précité. M. Leander était devenu gardien d'un musée naval en Suède et avait perdu son emploi à la suite d'un contrôle du personnel réunissant sur son compte des informations secrètes, aboutissant à la conclusion qu'il ne pouvait pas travailler dans un musée dont plusieurs entrepôts se trouvaient dans une zone militaire interdite. Cette affaire a permis à la Cour européenne des droits de l'homme d'affirmer clairement le principe selon lequel la mémorisation comme la communication de données à caractère personnel, assortie du refus d'accorder la faculté de les réfuter constituent une atteinte au respect de la vie privée. Lors de l'examen de la justification d'une telle atteinte, le juge européen a considéré que «[p]our préserver la sécurité nationale, les États contractants ont indéniablement besoin de lois qui habilitent les autorités internes compétentes à recueillir et à mémoriser dans des fichiers secrets des renseignements sur des personnes, puis à les utiliser quand il s'agit d'évaluer l'aptitude de candidats à des postes importants

du point de vue de ladite sécurité» (§ 59). Eu égard aux garanties dont s'entourait le système suédois de contrôle du personnel et à la grande marge d'appréciation reconnue à l'État, la Cour a jugé que «le gouvernement défendeur était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant». L'ingérence subie par M. Leander n'était donc pas disproportionnée au regard du but légitime poursuivi (§ 67).

---

109 – Voir Cour eur. D. H., arrêt Murray c. Royaume-Uni du 28 octobre 1994, série A, n° 300, § 47 et 90. Dans cette affaire, l'objectif de lutte contre le terrorisme permet de justifier la consignation par les forces armées de détails personnels sur la première requérante. Cette Cour observe notamment qu'il ne lui appartient pas «de substituer sa propre appréciation à celle des autorités nationales pour ce qui est de la meilleure politique dans le domaine de la poursuite des infractions terroristes» (§ 90). Voir également arrêt Klass, précité, § 49.

---

110 – Selon Ritleng, D., comme pour la notion synonyme de «méconnaissance patente», il y a erreur manifeste d'appréciation «en cas de violation grave des dispositions légales au point d'être évidente. Toute discrétionnaire qu'elle soit, l'appréciation des faits ne saurait conduire les institutions communautaires à décider n'importe quoi; par le contrôle de l'erreur manifeste d'appréciation, le juge interdit un usage gravement erroné de la liberté d'appréciation». Voir «Le contrôle de la légalité des actes communautaires par la Cour de justice et le Tribunal de première instance des Communautés européennes», thèse soutenue le 24 janvier 1998 à l'Université Robert Schuman de Strasbourg, p. 538, point 628.

---

111 – Voir, en matière de politique agricole commune, arrêt de la Cour du 13 novembre 1990, Fedesa e.a. (C-331/88, Rec. p. I-4023, point 14). Voir également, en matière de droits antidumping, arrêt du Tribunal du 5 juin 1996, NMB France e.a./Commission (T-162/94, Rec. p. II-427, point 70).

---

112 – Voir, en matière de politique agricole commune, arrêt de la Cour du 5 octobre 1994, Allemagne/Conseil (C-280/93, Rec. p. I-4973, point 91). Cette jurisprudence s'étend à d'autres domaines, par exemple en matière de politique sociale, où la Cour a pu reconnaître au Conseil «un large pouvoir d'appréciation s'agissant d'un domaine qui […] implique, de la part du législateur, des choix de politique sociale et où il est appelé à effectuer des appréciations complexes» (arrêt Royaume-Uni/Conseil, précité, point 58). Nous indiquons également que, en matière d'accès du public aux documents des institutions communautaires, et s'agissant de l'étendue du contrôle juridictionnel sur la légalité d'une décision de refus, le Tribunal a reconnu au Conseil une large marge d'appréciation dans le cadre d'une décision de refus fondée sur la protection de l'intérêt public en matière de relations internationales, ou sur la protection de l'intérêt public relatif à la sécurité publique: voir, notamment, en matière de lutte contre le terrorisme, arrêt du Tribunal du 26 avril 2005, Sison/Conseil (T-110/03, T-150/03 et T-405/03, non encore publié au Recueil, points 46, et 71 à 82).

---

113 – Outre l'arrêt Royaume-Uni/Conseil, précité, il existe de nombreux exemples dans lesquels le juge communautaire a reconnu le caractère complexe des appréciations auxquelles sont contraintes les institutions communautaires: voir, notamment, en matière de liberté d'établissement: arrêt du 13 mai 1997, Allemagne/Parlement et Conseil (C-233/94, Rec. p. I-2405, point 55). Pour un exemple de reconnaissance par le Tribunal d'«appréciations complexes d'ordre économique et social», voir arrêt du 13 septembre 1995, TWD/Commission (T-244/93 et T-486/93, Rec. p. II-2265, point 82).

---

114 – Ainsi, par exemple, la Commission disposait, selon nous, d'une large marge d'appréciation afin de déterminer si, dans le cadre particulier du transfert de données PNR, les États-Unis étaient en mesure d'assurer un niveau de protection adéquat desdites données personnelles.

---

115 – Selon la Commission, «le régime PNR établit une solution spécifique à un problème spécifique […]. En effet, la Communauté et les États-Unis ont négocié un système fermé de protection des données propre au CBP, distinct du système américain, et encadré par des garanties administratives supplémentaires du contrôle américain et des contrôles administratifs et légaux européens» (point 13 de ses observations sur le mémoire en intervention du CEPD dans l'affaire C-318/04).

---

116 – Nous rappelons qu'il s'agit des rubriques n°s 19 «Observations générales»; 26 «Données OSI ['Other Service Information']», et 27 «Données SSI/SSR ['Special Service Request']».

---

117 – Voir points 20 et 21 des observations de la Commission sur le mémoire en intervention du CEPD dans l'affaire C-318/04.

---

118 – Il est également précisé, à la note 7 de la déclaration d'engagement, que lorsque le dossier PNR est transféré vers un fichier de dossiers supprimés, il est stocké sous la forme de données brutes qui ne sont pas immédiatement interrogeables et ne peuvent donc pas être exploitées pour des enquêtes «traditionnelles».

---

119 – Voir points 8, sous d), et 10 de la convention n° 108, ainsi que article 22 de la directive 95/46.

---

120 – Voir paragraphe 36 de la déclaration d'engagement qui énonce:

«Le CBP portera à la connaissance des passagers les exigences relatives aux PNR et tous les éléments liés à leur utilisation, par exemple par la publication sur le site internet du CBP ou dans des dépliants à l'intention des voyageurs, de renseignements à caractère général concernant l'autorité responsable de la collecte des données, la finalité de la collecte, la protection des informations, le partage des données, l'identité du fonctionnaire responsable, les procédures de recours et les points de contact où soumettre les questions ou problèmes éventuels».

---

121 – Il s'agit du *Freedom of Information Act* (titre 5, section 552, du code des États-Unis, ci-après le «FOIA»). En ce qui concerne les documents détenus par le CBP, il convient de lire ces dispositions du FOIA en liaison avec le titre 19, sections 103.0 et suiv. du code des règlements fédéraux.

---

122 – Le FOIA établit la présomption selon laquelle chaque document gouvernemental fédéral doit être mis à la disposition de toute personne. Toutefois, l'organisme gouvernemental concerné peut s'affranchir de cette présomption de divulgation s'il prouve que les informations recherchées font partie d'une catégorie d'informations exemptée de l'obligation de divulgation. À cet égard, il convient de remarquer que, aux termes du paragraphe 37 de la déclaration d'engagement, «[d]ans le cas de demandes émanant des personnes concernées elles-mêmes, le fait que le CBP considère normalement les données de PNR comme des informations confidentielles à caractère personnel dans le cas des passagers ou relevant du secret commercial dans le cas des compagnies aériennes ne sera pas invoqué par le CBP en vertu de la loi sur la liberté de l'information pour ne pas communiquer les données de PNR aux personnes concernées».

---

123 – Souligné par nous. Le paragraphe 38 de la déclaration d'engagement renvoie à cet égard au titre 5, section 552(a)(4)(B) du code des États-Unis ainsi qu'au titre 19, section 103.7-103.9 du code des règlements fédéraux. Il ressort de ces textes que le recours juridictionnel («judicial review») contre le rejet par le CBP d'une demande de divulgation doit être précédé d'un recours administratif devant le FOIA Appeals Officer (titre 19, section 103.7 du code des règlements fédéraux). Si le refus de divulgation persiste à l'issue de ce recours administratif, le demandeur peut alors introduire un recours juridictionnel devant une *District Court* fédérale, qui est compétente pour ordonner la divulgation de toute information erronément refusée par un organisme gouvernemental.

---

124 – L'adresse de l'«Assistant Commissioner» est mentionnée dans le même paragraphe.

---

125 – Son adresse figure au paragraphe 41 de la déclaration d'engagement.

---

126 – Voir, en ce sens, paragraphe 5 de la section 222 de la loi américaine de 2002 sur la sécurité intérieure (Homeland Security Act – Public Law, 107-296, du 25 novembre 2002) qui prévoit que le Chief Privacy Officer doit, chaque année, soumettre au Congrès un rapport portant sur les activités du ministère de la sécurité intérieure ayant une incidence sur la protection de la vie privée, et faisant état des plaintes éventuelles pour atteinte à la vie privée.

---

127 – Voir note 11 de la déclaration d'engagement dont il résulte que le Chief Privacy Officer «n'est rattaché à aucune direction du ministère de la sécurité intérieure. Sa mission consiste à veiller à ce que les informations à caractère personnel soient utilisées dans le respect des lois applicables en la matière […]. Les décisions rendues par [ce haut responsable] […] sont contraignantes pour le ministère, qui ne peut les

annuler pour des motifs politiques». Par ailleurs, nous précisons que l'exigence relative à la possibilité de soumettre un recours à un organe indépendant doté d'un pouvoir de décision ressort notamment de l'arrêt de la Cour européenne des droits de l'homme du 7 juillet 1989, Gaskin c. Royaume-Uni (série A n° 160, § 49). Nous notons également que l'article 8 de la charte des droits fondamentaux de l'Union européenne prévoit, à son paragraphe 3, que le respect des règles qu'il énonce «est soumis au contrôle d'une autorité indépendante».

---

128 – Voir, par exemple, arrêt du 29 février 1996, Belgique/Commission (C-56/93, Rec. p. I-723, point 86).

---

129 – Arrêts du 27 septembre 1988, Grèce/Conseil (204/86, Rec. p. 5323, point 16), et du 30 mars 1995, Parlement/Conseil (C-65/93, Rec. p. I-643, point 23).

---

130 – Avis du 13 décembre 1995 (Rec. p. I-4577), rendu sur demande de la République fédérale d'Allemagne au sujet de la compatibilité avec le traité de l'accord-cadre sur les bananes entre la Communauté européenne et la Colombie, le Costa Rica, le Nicaragua ainsi que le Venezuela.

---

131 – Point 21 de l'avis (souligné par nous).

---

132 – Point 22 de l'avis.