
Universiteit
Leiden
The Netherlands

C.J.C.E. (gr. ch.), 30 mai 2006, Parlement européen c. Conseil et Commission [Note]

Zwenne, G.J.; Hert, P.J.A. de

Citation
Zwenne, G. J., & Hert, P. J. A. de. (2006). C.J.C.E. (gr. ch.), 30 mai 2006, Parlement européen c. Conseil et Commission [Note]. *Revue Européenne De Droit De La Consommation. European Consumer Law Journal*, *2006*(3), 199-242. Retrieved from https://hdl.handle.net/1887/46992

Version:	Not Applicable (or Unknown)
License:	Leiden University Non-exclusive license
Downloaded from:	https://hdl.handle.net/1887/46992

Note: To cite this publication please use the final published version (if applicable).

Note

C.J.C.E. (gr. ch.)
30 mai 2006
Parlement européen c. Conseil et Commission

Siég. : V. Skouris (prés.), P. Jann, C.W.A. Timmermans, A. Rosas, J. Malenovsky (prés. ch.), N. Colneric (rapp.), S. Von Bahr, J.N. Cunha Rodrigues, R. SIilva de Lapuerta, G. Arestis, A. Borg Barthet, M. Ilesic et J. Klucka (juges)

Avocat général : P. Léger

Affaires jointes C-317-04 et C-318/04

1. Rapprochement des législations – Directive 95/46 – Champ d'application (directive du Parlement européen et du Conseil 95/46, article 3, §2; décision de la Commission 2004/535)

2. Accords internationaux – Conclusion – Accord CEE-États-Unis concernant le traitement et le transfert des dossiers des passagers aériens au Bureau des douanes et de la protection des frontières des États-Unis (article 95 CE; directive du Parlement européen et du Conseil 95/46, art. 3, §2, et 25; décision du Conseil 2004/496)

1. *La décision 2004/535, 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, concerne un traitement de données à caractère personnel ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal, lequel est exclu du champ d'application de la directive 95/46, 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, en vertu de l'article 3, §2, premier tiret, de ladite directive.*

*À cet égard, le fait que les données personnelles sont collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un État tiers ne modifie pas une telle conclusion, dans la mesure où ce transfert s'insère dans un cadre institué par les pouvoirs publics et visant la sécurité publique et où il n'est pas nécessaire à la prestation de services desdits opérateurs (*cfr *points 56-59).*

2. *La décision 2004/496, 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 (Passenger Name Records) par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure, n'a pu être valablement adoptée sur la base de l'article 95 CE, lu en combinaison avec l'article 25 de la directive 95/46, 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.*

En effet, l'accord vise des traitements de données qui, dans la mesure où ils ont pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal, sont exclus du champ d'application de la directive 95/46 en vertu de l'article 3, §2, premier tiret, de cette dernière (cfr *points 67-69).*

Arrêt

1. Par sa requête dans l'affaire C-317/04, le Parlement européen demande l'annulation de la décision 2004/496/CE du Conseil, du 17 mai 2004, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (*J.O.,* L 183, p. 83 et rectificatif *J.O.,* 2005, L 255, p. 168).

2. Par sa requête dans l'affaire C-318/04, le Parlement demande l'annulation de la décision 2004/535/CE de la Commission, du 14 mai 2004, relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique (*J.O.,* L 235, p. 11, ci-après la «décision d'adéquation»).

Le cadre juridique

3. L'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la Convention), 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».

4. L'article 95, § 1er, deuxième phrase, CE est libellé comme suit :

«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».

5. 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 (*J.O.,* L 281, p. 31), telle que modifiée par le règlement (CE) nº 1882/2003 du Parlement européen et du Conseil, du 29 septembre 2003, portant adaptation à la décision 1999/468/CE du Conseil des dispositions 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 (*J.O.,* L 284, p. 1) (ci-après la «directive»), a été adoptée sur la base de l'article 100 A du Traité CE (devenu, après modification, article 95 CE).

6. Son onzième considérant énonce 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, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel».

7. Aux termes du treizième considérant de la directive :

«[L]es activités visées aux titres V et VI du Traité sur l'Union européenne concernant la sécurité publique, la défense, la sûreté de l'État ou les activités de l'État dans le domaine pénal ne relèvent pas du champ d'application du droit communautaire, sans préjudice des obligations incombant aux États membres au titre de l'article 56, § 2 et des articles 57 et 100 A du Traité [...]».

8. Le cinquante-septième considérant de la directive énonce :

«[...] 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».

9. L'article 2 de la directive prévoit :

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

a) "données à caractère personnel" : toute information concernant une personne physique identifiée ou identifiable (personne concernée); 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;

b) "traitement de données à caractère personnel" (traitement) : 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;

[…]».

10. Aux termes de l'article 3 de la directive :

«Champ d'application.

1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. 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,

[…]».

11. L'article 6, § 1er, de la directive énonce :

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

[…]

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ;

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

[…]

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 […] ».

12. L'article 7 de la directive dispose :

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

[…]

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

[…]

ou

e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées

ou

f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, § 1er ».

13. Aux termes de l'article 8, § 5, premier alinéa, de la directive :

«Le traitement de données infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique».

14. L'article 12 de la directive dispose :

«Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement :

a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs :

- la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,
- la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,
- la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15, § 1er;

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point *b*), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné».

15. L'article 13, § 1er, de la directive est libellé comme suit :

«Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6, § 1er, à l'article 10, à l'arti-

cle 11, § 1er 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 ».

16. L'article 22 de la directive prévoit :

« Recours.

Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les États membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question ».

17. Les articles 25 et 26 de la directive forment le chapitre IV concernant le transfert de données à caractère personnel vers des États tiers.

18. L'article 25 de la directive, intitulé « Principes », prévoit :

« 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, §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, §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».

19. Aux termes de l'article 26, §1er, de la directive, intitulé «Dérogations» :

«Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25, §2, peut être effectué, à condition que :

a) la personne concernée ait indubitablement donné son consentement au transfert envisagé

ou

b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée

ou

c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers

ou

d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice

ou

e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée

ou

f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier».

20. Sur la base de la directive et, notamment, de son article 25, §6, la Commission des Communautés européennes a adopté la décision d'adéquation.

21. Le onzième considérant de cette décision énonce :

«Le traitement par le CBP [*United States Bureau of Customs and Border Protection* (Bureau des douanes et de la protection des frontières des États-Unis)] des données à caractère personnel contenues dans les PNR ["*Passenger Name Records*" (dossiers passagers)] 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" (ci-après dénommée "la déclaration d'engagement") et par la législation américaine dans les conditions prévues par la déclaration d'engagement».

22. Aux termes du quinzième considérant de la même décision, 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.

23. Aux termes des articles 1er à 4 de la décision d'adéquation :

«Article premier

Aux fins de l'article 25, §2, de la directive 95/46/CE, le Bureau des douanes et de la protection des frontières des États-Unis (ci-après le "CBP") est considéré comme assurant un niveau de protection adéquat des données de dossiers passagers (ci-après dénommés les "PNR") 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.

Article 2

La présente décision concerne le niveau de protection adéquat assuré par le CBP en vue de répondre aux exigences de l'article 25, §1er, de la directive 95/46/CE et n'influe en rien sur d'autres conditions ou restrictions mettant en application d'autres dispositions de la directive qui s'appliquent au traitement de données à caractère personnel dans les États membres.

Article 3

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.

Article 4

1. Les États membres informent sans tarder la Commission des mesures adoptées conformément à l'article 3.

2. Les États membres et la Commission s'informent aussi mutuellement de tout changement dans les normes de protection ainsi que des cas dans lesquels les mesures prises par les autorités chargées de veiller au respect par le CBP des normes de protection établies en annexe ne suffisent pas à en assurer le respect.

3. Si les informations recueillies conformément à l'article 3 et aux paragraphes 1er 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, §2, de la directive 95/46/CE sera applicable en vue d'annuler ou de suspendre la présente décision».

24. La «[d]éclaration d'engagement du Bureau des douanes et de la protection des frontières du ministère de la sécurité intérieure», annexée à la décision d'adéquation, énonce :

«Afin de soutenir le projet de la Commission européenne visant à exercer les pouvoirs qui lui sont conférés par l'article 25, §6, de la directive 95/46/CE […] et à adopter une décision reconnaissant que le [CBP] du ministère de la sécurité intérieure (Department of Homeland Security) fournit un niveau de protection adéquat aux fins du transfert, par les compagnies aériennes, de données de [PNR] susceptibles de relever du champ d'application de la directive, le CBP prend les engagements suivants [...]».

25. Ces engagements comprennent 48 points, qui sont regroupés sous les titres suivants : «Base juridique du droit d'obtention des PNR»; «Utilisation des données de PNR par le CBP»; «Exigences données»; «Traitement des données "sensibles"»; «Méthode d'accès aux données de PNR»; «Stockage des données de PNR»; «Sécurité des systèmes informatiques du CBP»; «Traitement et protection des données de PNR par le CBP»; «Transmission de données de PNR à d'autres autorités gouvernementales»; «Information, accès aux données et voies de recours pour les personnes concernées par les PNR»; «Respect des dispositions»; «Réciprocité»; «Révision et durée de validité de la déclaration d'engagement», et «Absence de création de droits ou de précédent».

26. Parmi lesdits engagements figurent, notamment, les suivants :

« 1) En vertu de la loi [titre 49, section 44909 (c)(3) du Code des États-Unis] et de ses règlements (provisoires) de mise en œuvre (titre 19, section 122.49 b du Code des règlements fédéraux), toute compagnie aérienne assurant un service international de transport de passagers à destination ou au départ des États-Unis doit fournir au CBP un accès électronique aux données de PNR qui sont recueillies et stockées dans ses systèmes informatiques de réservation/contrôle des départs (ci-après dénommés les "systèmes de réservation").

[…]

3) Le 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. L'utilisation de données de PNR à ces fins permet au CBP d'axer ses ressources sur des éléments à haut risque, facilitant et préservant ainsi le trafic passagers légitime.

4) Les éléments informatifs requis par le CBP sont énumérés à l'annexe A. […]

[…]

27) Dans le cadre de toute procédure administrative ou judiciaire découlant d'une demande, introduite en vertu de la loi sur la liberté de l'information, de données de PNR obtenues auprès de compagnies aériennes, le CBP soutiendra que les registres en question ne sont pas soumis à la divulgation prévue par cette loi.

[…]

29) Le CBP, à sa discrétion, ne transmettra de données de PNR à d'autres autorités gouvernementales de répression ou de lutte contre le terrorisme, qu'elles soient nationales ou étrangères, qu'au cas par cas, aux fins de prévenir ou de combattre les crimes visés au paragraphe 3. Les autorités avec lesquelles le CBP peut partager ces données sont ci-après dénommées "autorités désignées".

30) Le CBP exercera avec discernement son pouvoir d'appréciation concernant le transfert de données de PNR aux fins spécifiées. Il déterminera tout d'abord si la raison invoquée pour la divulgation des données de PNR à une autre autorité désignée est conforme aux finalités prévues (voy. le point 29). Dans l'affirmative, le CBP vérifiera si l'autorité désignée en question est compétente pour prévenir toute violation d'une loi ou d'un règlement lié à ces finalités ou pour mener une

enquête ou engager des poursuites à cet égard ou pour mettre en œuvre ou veiller à l'application d'une telle loi ou d'un tel règlement, pour le cas où le CBP disposerait d'un indice d'une violation effective ou potentielle de la loi. Le bien-fondé de la divulgation devra être examiné à la lumière de l'ensemble des circonstances exposées.

[…]

35) Aucune disposition de la présente déclaration d'engagement ne peut empêcher l'utilisation ou la divulgation de données de PNR dans le cadre d'une procédure pénale ou au titre d'autres exigences prévues par la loi. Le CBP informera la Commission de l'adoption, par les autorités américaines, de toute législation ayant une incidence sur le fond des présents engagements.

[…]

46) La présente déclaration d'engagement est applicable durant une période de trois ans et six mois à compter de la date d'entrée en vigueur d'un accord entre les États-Unis et la Communauté européenne autorisant le traitement de données de PNR par les compagnies aériennes pour les transmettre au CBP conformément à la directive. […]

47) La présente déclaration d'engagement ne crée ni ne confère aucun droit ni aucun avantage pour toute personne ou partie, qu'elle soit privée ou publique.

[…]»

27. L'annexe A de la déclaration d'engagement contient les «rubriques des PNR» demandées par le CBP aux compagnies aériennes. Font notamment partie desdites rubriques, le «code repère du dossier PNR», la date de réservation, le nom, l'adresse, les modes de paiement, les numéros de téléphone, l'agence de voyage, le «statut» du voyageur (*travel status of passenger*), l'adresse électronique, des observations générales, le numéro du siège occupé, l'information selon laquelle le passager est répertorié comme défaillant ainsi que les «informations APIS» éventuellement recueillies.

28. Le Conseil a adopté la décision 2004/496 notamment sur la base de l'article 95 CE, en liaison avec l'article 300, § 2, premier alinéa, première phrase, CE.

29. Aux termes des trois considérants de cette décision :

«(1) Le 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 bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure.

(2) Le Parlement européen n'a pas émis son avis dans le délai fixé, en vertu de l'article 300, §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.

(3) Il convient d'approuver l'accord».

30. L'article 1er de la décision 2004/496 prévoit :

«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, est approuvé au nom de la Communauté.

Le texte de l'accord est joint à la présente décision».

31. Ledit accord (ci-après l'«accord») est rédigé comme suit :

«La Communauté européenne et les États-Unis d'Amérique,

Reconnaissant 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,

Vu les lois et règlements américains exigeant 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] du ministère américain de la sécurité intérieure (ci-après dénommé DHS) un accès électronique aux données des [PNR] qui sont recueillies et stockées dans son système informatique de contrôle des réservations et des départs,

Vu la directive 95/46/CE, […] et notamment son article 7, point *c*),

Vu les engagements pris par le CBP le 11 mai 2004, qui seront publiés dans le registre fédéral américain (ci-après dénommés "les engagements"),

Vu la décision 2004/535/CE de la Commission adoptée le 14 mai 2004, conformément à l'article 25, §6, de la directive 95/46/CE, en vertu de laquelle le CBP est censé assurer un niveau de protection adéquat des données PNR transférées de la

Communauté européenne (ci-après dénommée "la Communauté") et concernant les vols au départ ou à destination des États-Unis, conformément aux engagements ci-annexés (ci-après dénommée "la décision"),

Notant 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,

[…]

Sont convenus de ce qui suit :

1. Le CBP peut accéder, par voie électronique, aux données PNR provenant des systèmes de contrôle des réservations et des départs des transporteurs aériens ("systèmes de réservation") situés sur le territoire des États membres de la Communauté européenne, en application stricte de la décision 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.

   [La version anglaise se lit comme suit : "CBP may electronically access the PNR data from air carriers reservation/departure control systems ('reservation systems') located within the territory of the Membre State of the European Community strictly in accordance with the Decision and for so long as the Decision is applicable and only until there is a satisfactory system in place allowing for transmission of such data by the air carriers"].

2. Les transporteurs aériens assurant un service de transport international de passagers à destination ou au départ des États-Unis traitent 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 et aussi longtemps que cette dernière est applicable.
3. Le CBP prend note de la décision et déclare qu'il met en œuvre les engagements annexés à ladite décision.
4. Le 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.

[…]

7. Le présent accord entre en vigueur dès sa signature. Chaque partie peut dénoncer le présent accord à tout moment par notification par la voie diplomatique. L'accord cesse d'être applicable quatre-vingt-dix (90) jours après la date de la notification de la dénonciation à l'autre partie. Le présent accord peut être modifié à tout moment d'un commun accord écrit.

8. Le 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».

32. Selon l'information du Conseil relative à la date de son entrée en vigueur (*J.O.,* 2004, C 158, p. 1), l'accord, signé à Washington le 28 mai 2004 par un représentant de la présidence en exercice du Conseil et par le secrétaire à la sécurité intérieure des États-Unis d'Amérique, est, conformément à son point 7, entré en vigueur le jour de sa signature.

Les antécédents des litiges

33. À la suite des attaques terroristes du 11 septembre 2001, les États-Unis ont adopté en novembre de la même année une législation disposant que les transporteurs aériens assurant des liaisons à destination ou au départ des États-Unis, ou traversant le territoire de ces derniers, étaient tenus de fournir aux autorités douanières des États-Unis un accès électronique aux données contenues dans leurs systèmes automatiques de réservation et de contrôle des départs, désignées par les termes «*Passenger Name Records*» (ci-après les «données PNR»). Tout en reconnaissant la légitimité des intérêts de sécurité en jeu, la Commission a informé les autorités des États-Unis, dès juin 2002, que ces dispositions pouvaient entrer en conflit avec la législation communautaire et celle des États membres en matière de protection des données et avec certaines dispositions du règlement (CEE) nº 2299/89 du Conseil, du 24 juillet 1989, instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation (*J.O.,* L 220, p. 1), tel que modifié par le règlement (CE) nº 323/1999 du Conseil, du 8 février 1999 (*J.O.,* L 40, p. 1). Les autorités des États-Unis ont reporté l'entrée en vigueur des nouvelles dispositions, mais ont, en définitive, refusé de renoncer à infliger des

sanctions aux compagnies aériennes ne se conformant pas à la législation concernant l'accès électronique aux données PNR après le 5 mars 2003. Depuis lors, plusieurs grandes compagnies aériennes de l'Union européenne ont fourni auxdites autorités un accès à leurs données PNR.

34. La Commission a entamé des négociations avec les autorités des États-Unis, lesquelles ont donné lieu à un document contenant des engagements («undertakings») pris par le CBP, en vue de l'adoption par la Commission d'une décision d'adéquation sur la base de l'article 25, §6, de la directive.

35. Le 13 juin 2003, le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué à l'article 29 de la directive, a rendu un avis dans lequel il a exprimé des doutes sur le niveau de protection des données garanti par lesdits engagements en ce qui concerne les traitements envisagés. Il a réitéré ces doutes dans un avis du 29 janvier 2004.

36. Le 1er mars 2004, la Commission a saisi le Parlement du projet de décision d'adéquation en vertu de l'article 25, §6, de la directive 95/46, assorti du projet d'engagements du CBP.

37. Le 17 mars 2004, la Commission a transmis au Parlement, dans la perspective de la consultation de celui-ci au titre de l'article 300, §3, premier alinéa, CE, une proposition de décision du Conseil concernant la conclusion d'un accord avec les États-Unis. Par lettre du 25 mars 2004, se référant à la procédure d'urgence, le Conseil a demandé au Parlement de rendre un avis sur cette proposition pour le 22 avril 2004 au plus tard. Dans cette lettre, le Conseil a souligné que «la lutte contre le terrorisme, qui justifie les mesures proposées, est une priorité essentielle de l'Union européenne, [que,] actuellement, les transporteurs aériens et les passagers sont dans une situation d'incertitude à laquelle il convient de remédier d'urgence [et que], en plus, il est essentiel de protéger les intérêts financiers des parties concernées».

38. Le 31 mars 2004, en application de l'article 8 de la décision 1999/468/CE du Conseil, du 28 juin 1999, fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission (*J.O.,* L 184, p. 23), le Parlement a adopté une résolution faisant état d'un certain nombre de réserves d'ordre juridique sur la proposition qui lui avait été soumise. Dans cette résolution, il a considéré, en particulier, que le projet de décision d'adéquation excédait les compétences conférées à la Commission par l'article 25 de la directive. Il a appelé à la conclusion d'un accord international approprié respectant les droits fondamentaux sur un cer-

tain nombre de points détaillés dans ladite résolution 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 aux fins de vérifier la légalité de l'accord international envisagé et, en particulier, la compatibilité de celui-ci avec la protection du droit à la vie privée.

39. 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 ce que, conformément à l'article 300, §6, CE, soit recueilli l'avis de la Cour sur la compatibilité de l'accord envisagé avec les dispositions du Traité. Cette procédure a été entamée le jour même.

40. Le Parlement a également décidé, le même jour, de renvoyer en commission le rapport sur la proposition de décision du Conseil, rejetant ainsi implicitement, à ce stade, la demande d'examen en urgence de ladite proposition présentée par le Conseil le 25 mars.

41. Le 28 avril suivant, le Conseil, se fondant sur l'article 300, §3, premier alinéa, CE, a adressé une lettre au Parlement demandant à ce dernier de rendre son avis avant le 5 mai 2004 sur la proposition de décision relative à la conclusion de l'accord. Pour justifier l'urgence de cette demande, il a repris les motifs avancés dans sa lettre du 25 mars 2004.

42. Ayant pris connaissance de l'absence persistante de l'ensemble des versions linguistiques de la proposition de décision du Conseil, le Parlement a rejeté, le 4 mai 2004, la demande d'examen en urgence de cette proposition que le Conseil lui avait soumise le 28 avril.

43. Le 14 mai suivant, la Commission a adopté la décision d'adéquation, qui fait l'objet de l'affaire C-318/04. Le 17 mai 2004, le Conseil a adopté la décision 2004/496, qui fait l'objet de l'affaire C-317/04.

44. Par lettre du 4 juin 2004, la présidence en exercice du Conseil a informé le Parlement que la décision 2004/496 prenait en considération la lutte contre le terrorisme – prioritaire pour l'Union – mais aussi le besoin de faire face à une situation d'insécurité juridique des compagnies aériennes, ainsi que leurs intérêts financiers.

45. Par lettre du 9 juillet 2004, le Parlement a informé la Cour du retrait de sa demande d'avis enregistrée sous le nº 1/04.

46. Dans l'affaire C-317/04, par ordonnances du président de la Cour des 18 novembre 2004 et 18 janvier 2005, la Commission et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord ont été admis à intervenir à l'appui des conclusions du Conseil.

47. Dans l'affaire C-318/04, par ordonnance du président de la Cour du 17 décembre 2004, le Royaume-Uni a été admis à intervenir à l'appui des conclusions de la Commission.

48. Par ordonnances de la Cour du 17 mars 2005, le Contrôleur européen de la protection des données a été admis à intervenir à l'appui des conclusions du Parlement dans ces deux affaires.

49. Étant donné la connexité desdites affaires, confirmée lors de la procédure orale, il convient, conformément à l'article 43 du règlement de procédure, de les joindre aux fins de l'arrêt.

Sur le recours dans l'affaire C-318/04

50. Le Parlement invoque quatre moyens d'annulation, tirés respectivement d'un excès de pouvoir, d'une violation des principes essentiels de la directive, d'une violation des droits fondamentaux et d'une violation du principe de proportionnalité.

Sur la première branche du premier moyen, tirée d'une violation de l'article 3, §2, premier tiret, de la directive

Argumentation des parties

51. Le Parlement soutient que la décision de la Commission a été adoptée *ultra vires* dès lors que n'ont pas été respectées les dispositions arrêtées dans la directive et en violation notamment de l'article 3, §2, premier tiret, de celle-ci relatif à l'exclusion des activités qui ne relèvent pas du champ d'application du droit communautaire.

52. Il ne ferait pas de doute que le traitement des données PNR après le transfert à l'autorité américaine visée par la décision d'adéquation est effectué, et le sera, pour l'exercice d'activités propres aux États au sens du point 43 de l'arrêt du 6 novembre 2003, *Lindqvist* (C-101/01, *Rec.,* p. I-12971).

53. La Commission, soutenue par le Royaume-Uni, estime que les activités des transporteurs aériens entrent clairement dans le champ d'application du droit communautaire. Elle fait valoir que ces opérateurs privés traitent les données PNR au sein de la Communauté et organisent leur transfert vers un État tiers. Il s'agirait donc d'activités relevant des particuliers et non d'activités de l'État membre dans lequel opèrent les transporteurs concernés, ou de ses pouvoirs publics, ainsi que l'a défini la Cour au point 43 de l'arrêt *Lindqvist*, précité. Le but poursuivi par les transporteurs aériens dans le traitement des données PNR serait simplement de respecter les exigences du droit communautaire, y compris l'obligation inscrite au point 2 de l'accord. L'article 3, paragraphe 2, de la directive ferait référence aux activités d'autorités publiques qui ne relèvent pas du champ d'application du droit communautaire.

Appréciation de la Cour

54. L'article 3, §2, premier tiret, de la directive exclut de son champ d'application le 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, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal.

55. La décision d'adéquation ne concerne que les données PNR transférées au CBP. Il ressort du sixième considérant de cette décision que les exigences de ce transfert 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. Selon le septième considérant de ladite décision, la législation américaine en question concerne le renforcement de la sécurité ainsi que les conditions d'entrée aux États-Unis et de sortie dudit pays. Aux termes du huitième considérant, la Communauté soutient entièrement les États-Unis dans leur lutte contre le terrorisme, dans les limites imposées par le droit de la Communauté. Le quinzième considérant de cette même décision énonce que les données 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.

56. Il en résulte que le transfert des données PNR au CBP constitue un traitement ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal.

57. S'il est 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. En effet, cette décision, ainsi qu'il a été rappelé au point 55 du présent arrêt, 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.

58. Au point 43 de l'arrêt *Lindqvist*, précité, qui a été invoqué par la Commission dans sa défense, la Cour a jugé que les activités mentionnées à titre d'exemple à l'article 3, §2, premier tiret, de la directive sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers. Toutefois, il n'en découle pas que, en raison du fait que les données PNR ont été collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un État tiers, le transfert en cause n'entre pas dans le champ d'application de cette disposition. En effet, ce transfert s'insère dans un cadre institué par les pouvoirs publics et visant la sécurité publique.

59. Il résulte des considérations qui précèdent que la décision d'adéquation concerne un traitement de données à caractère personnel au sens de l'article 3, §2, premier tiret, de la directive. Cette décision ne relève donc pas du champ d'application de celle-ci.

60. Dès lors, la première branche du premier moyen, tirée d'une violation de l'article 3, §2, premier tiret, de la directive, est fondée.

61. Par conséquent, sans qu'il soit nécessaire d'examiner les autres branches du premier moyen ainsi que les autres moyens invoqués par le Parlement, il y a lieu d'annuler la décision d'adéquation.

Sur le recours dans l'affaire C-317/04

62. Le Parlement avance six moyens d'annulation, tirés du choix erroné de l'article 95 CE comme base juridique de la décision 2004/496 et de la violation, respec-

tivement, de l'article 300, §3, deuxième alinéa, CE, de l'article 8 de la Convention, du principe de proportionnalité, de l'exigence de motivation et du principe de coopération loyale.

Sur le premier moyen, tiré du choix erroné de l'article 95 CE comme base juridique de la décision 2004/496

Argumentation des parties

63. Le Parlement fait valoir que l'article 95 CE ne constitue pas, pour la décision 2004/496, une base juridique appropriée. Cette décision n'aurait pas pour but et pour contenu l'établissement et le fonctionnement du marché intérieur en contribuant à l'élimination d'entraves à la libre prestation des services et ne contiendrait pas de dispositions visant à la réalisation d'un tel but. En effet, elle aurait pour finalité de légaliser le traitement de données à caractère personnel prescrit par la législation des États-Unis. D'ailleurs, l'article 95 CE ne serait pas susceptible de fonder la compétence de la Communauté pour conclure l'accord, puisque celui-ci vise des traitements de données exclus du champ d'application de la directive.

64. Le Conseil soutient que la directive, valablement adoptée sur la base de l'article 100 A du Traité, contient à son article 25 des dispositions prévoyant la possibilité d'un transfert de données à caractère personnel vers un État tiers assurant un niveau de protection adéquat, y compris la possibilité d'engager en cas de besoin des négociations conduisant à la conclusion par la Communauté d'un accord avec ce pays. L'accord concernerait la libre circulation des données PNR entre la Communauté et les États-Unis dans des conditions qui respectent les libertés et les droits fondamentaux des personnes, notamment la vie privée. Il viserait à supprimer toute distorsion de concurrence, entre les compagnies aériennes des États membres et entre celles-ci et les compagnies des États tiers, pouvant résulter des exigences imposées par les États-Unis, 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 en raison du fait que seulement certaines d'entre elles auraient accordé aux autorités des États-Unis un accès à leurs bases de données. L'accord tendrait à imposer à toutes les compagnies concernées des obligations harmonisées.

65. La Commission souligne l'existence d'un «conflit de lois», au sens du droit international public, entre les lois des États-Unis et la réglementation communau-

taire ainsi que la nécessité de concilier celles-ci. Elle reproche au Parlement, qui conteste que l'article 95 CE puisse constituer la base juridique de la décision 2004/496, de n'avoir pas proposé de base juridique appropriée. Selon la Commission, ledit article constitue «la base juridique naturelle» de cette décision puisque l'accord concerne la dimension externe de la protection des données à caractère personnel lors de leur transfert à l'intérieur de la Communauté. Les articles 25 et 26 de la directive fonderaient une compétence exclusive externe en faveur de la Communauté.

66. En outre, la Commission fait valoir que le traitement initial de ces données par les compagnies aériennes est effectué dans des buts commerciaux. L'utilisation que font les autorités des États-Unis de ces données ne les ferait pas échapper à l'incidence de la directive.

Appréciation de la Cour

67. L'article 95 CE, lu en combinaison avec l'article 25 de la directive, n'est pas susceptible de fonder la compétence de la Communauté pour conclure l'accord.

68. En effet, l'accord vise le même transfert de données que la décision d'adéquation et donc des traitements de données qui sont, ainsi qu'il a été exposé ci-dessus, exclus du champ d'application de la directive.

69. Par conséquent, la décision 2004/496 n'a pu être valablement adoptée sur la base de l'article 95 CE.

70. Sans qu'il soit nécessaire d'examiner les autres moyens invoqués par le Parlement, il convient donc d'annuler cette décision.

Sur la limitation des effets de l'arrêt

71. Il ressort du point 7 de l'accord que chaque partie peut dénoncer celui-ci à tout moment et qu'il cesse d'être applicable 90 jours après la date de la notification de la dénonciation à l'autre partie.

72. Cependant, conformément aux points 1 et 2 de l'accord, le droit d'accès du CBP aux données PNR et l'obligation imposée aux transporteurs aériens de les traiter comme demandé par le CBP n'existent qu'aussi longtemps que la décision d'adéquation est applicable. Au point 3 dudit accord, le CBP a déclaré qu'il met en œuvre les engagements annexés à ladite décision.

73. Eu égard, d'une part, au fait que la Communauté ne peut invoquer son propre droit comme justifiant la non-exécution de l'accord qui reste applicable pendant le délai de 90 jours à compter de sa dénonciation et, d'autre part, au lien étroit existant entre l'accord et la décision d'adéquation, il paraît justifié, pour des raisons de sécurité juridique et afin de protéger les personnes concernées, de maintenir les effets de la décision d'adéquation pendant cette même période. En outre, il convient de tenir compte du délai nécessaire à l'adoption des mesures que comporte l'exécution du présent arrêt.

74. Il y a donc lieu de maintenir les effets de la décision d'adéquation jusqu'au 30 septembre 2006, sans toutefois que ces effets soient maintenus au-delà de la date d'extinction de l'accord.

Sur les dépens

75. Aux termes de l'article 69, §2, du règlement de procédure, toute partie qui succombe est condamnée aux dépens, s'il est conclu en ce sens. Le Parlement ayant conclu à la condamnation du Conseil et de la Commission et ceux-ci ayant succombé en leurs moyens, il y a lieu de les condamner aux dépens. En application du paragraphe 4, premier alinéa, du même article, les intervenants aux présents litiges supportent leurs propres dépens.

Par ces motifs,

la Cour,

Déclare et arrête :

1) 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, et 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, sont annulées.

2) Les effets de la décision 2004/535 sont maintenus jusqu'au 30 septembre 2006, sans toutefois que ces effets soient maintenus au-delà de la date d'extinction dudit accord.

3) Le Conseil de l'Union européenne est condamné aux dépens dans l'affaire C-317/04.

4) La Commission des Communautés européennes est condamnée aux dépens dans l'affaire C-318/04.

5) La Commission des Communautés européennes supporte ses propres dépens dans l'affaire C-317/04.

6) Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord ainsi que le contrôleur européen de la protection des données supportent leurs propres dépens.

Note
Sur les données des dossiers passagers, la directive «vie privée» 95/46/CE et la non-adéquation de la législation européenne

1. Fin mai de l'année dernière, la Cour européenne de justice a rendu un arrêt, attendu de longue date, sur les données des dossiers passagers transmises aux autorités de recherche et aux services de renseignements des États-Unis. On pouvait s'attendre à ce que la Cour se prononce sur la protection juridique devant garantir le respect de la vie privée ou sur la proportionnalité des transferts de données à grande échelle. Dans l'arrêt, la Cour s'est toutefois bornée à répondre à des questions sur les compétences institutionnelles propres au premier pilier ainsi que sur les bases juridiques des réglementations mises en cause. Elle a annulé les décisions à l'origine des transferts de données, mais a prévu une période transitoire permettant à la Commission et au Conseil de réparer les erreurs et de poursuivre le transfert de données des dossiers passagers. Dans cette contribution, nous présenterons un aperçu des événements qui ont conduit à l'arrêt, ainsi qu'une réflexion sur la non-adéquation du législateur européen et sur le *profiling* en tant que moyen de lutter contre le terrorisme. Dans ce qui suit, nous évoquerons l'anamnèse et les événements qui ont débouché sur l'arrêt et ce qui s'est passé ensuite. Puis, nous joindrons quelques observations.

2. Les événements qui ont conduit à l'arrêt, peuvent être résumés autour de cinq épisodes que nous avons identifiés comme suit : (i) la naissance du conflit en matière de protection de la vie privée, (ii) les négociations en vue d'aboutir à un règlement de ce conflit, (iii) l'accord entre la Commission et les États-Unis,

(iv) l'opposition du Parlement européen, (v) l'arrêt de la Cour européenne de justice et les événements subséquents.

Dans la foulée du 11 septembre 2001, les États-Unis ont pris des mesures radicales pour renforcer la sécurité aérienne. L'une des mesures [1] potentiellement les plus judicieuses était le *screening* préventif des passagers des compagnies aériennes. Depuis plusieurs années déjà, l'*American Bureau of Customs and Border Protection* examine tout le trafic aérien et applique l'évaluation des risques sur la base d'un système de *profiling* (appelé *Automated Targeting System*) [2]. Les passagers et les bagages se voient attribuer une «note de risque» et il est également fait recours à des données provenant de diverses banques de données. L'évaluation des risques est conservée pendant 40 ans et peut être échangée avec toute une série d'institutions publiques, semi-publiques et même privées.

Dans le prolongement de cette initiative, les États-Unis ont instauré une législation obligeant les compagnies aériennes volant en direction des États-Unis ou les survolant, à transmettre des données sur leurs passagers aux autorités douanières américaines, avant l'arrivée de l'avion aux États-Unis [3]. Très rapidement après l'instauration de cette nouvelle législation, il est apparu que celle-ci ne faisait pas bon ménage avec les principes de la directive «vie privée» 95/46/CE [4], laquelle vise à harmoniser les règles relatives à la protection des données à caractère personnel dans l'Union européenne. L'objectif est d'appliquer, partout dans l'Union européenne, plus ou moins les mêmes droits et les mêmes obligations, pour éviter que des entreprises, des autorités et autres prestataires de services ne soient enclins à contourner les règles plus sévères en application dans un État membre en traitant leurs données à caractère personnel dans un autre État membre, moins sévère celui-là. En même temps, la directive attend des États membres qu'ils ne dressent pas d'obstacles à la transmission de données vers un autre État membre. Pour éviter le contournement des règles européennes en matière de protection de

1 Voy. pour le sens et le non-sens du contrôle des coupe-ongles, etc. : B. SCHNEIER, *Beyond Fear – Thinking Sensibly about Security in an Uncertain World*, Copernicus Books, 2003 <www.schneier.com>.

2 *Cfr*. *The New York Times*, «US assigns terror scores to international travellers», 1er décembre 2006.

3 «Aviation and Transportation Security Act (ATSA) du 19 novembre 2001», *Public Law* 107–71. Plus tard aussi : «Enhanced Border Security and Visa Reform Act du 14 mai 2002», *Public Law* 107-173.

4 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, *J.O.,* L 281/31, 1995.

la vie privée, il est stipulé dans la directive que des données à caractère personnel ne peuvent pas être transférées vers un État n'appartenant pas à l'Union européenne si cet État n'offre pas un niveau de protection adéquat. Pour diverses raisons [5], il est constaté que les États-Unis n'offrent pas un tel niveau de protection adéquat. En principe, et pour cette raison, des données à caractère personnel ne peuvent pas être transférées d'un État membre aux États-Unis, même pas pour la lutte contre le terrorisme ou à d'autres fins qui se justifieraient en soi.

Tout cela a plongé les compagnies aériennes dans une situation fort embarrassante. En vertu des règles européennes, elles ne pouvaient pas transmettre des données à caractère personnel aux États-Unis. En même temps, elles étaient directement interpellées par les États-Unis, qui les obligeaient à fournir quand même les données sous peine d'une amende de 5 000 USD par passager ou de la perte des droits d'atterrissage. Les compagnies aériennes ont dès lors fait leurs comptes et ont décidé de transmettre les données ainsi exigées. Les États membres européens, et notamment les autorités de contrôle pour la protection de la vie privée, n'ont pas pu fermer les yeux. C'est ainsi qu'est né le conflit en matière de protection de la vie privée.

3. La question a été mise rapidement à l'agenda politique en Europe. En 2003, le groupe de travail européen des autorités de contrôle nationales, le groupe de travail «Art. 29», relève l'existence de problèmes liés à ces transferts de données aux autorités américaines sur le plan de la protection des données à caractère personnel. En octobre de cette même année, le groupe de travail formule un premier avis et demande des ajustements et une adaptation [6]. Des discussions ont lieu entre-temps entre la Commission européenne et les États-Unis. Elles débouchent sur une déclaration commune dans laquelle ils proclament leur volonté d'autoriser les compagnies aériennes, sous conditions, à fournir des données des dossiers passagers [7].

Il s'ensuit une résolution du Parlement européen [8] et une lettre du groupe de travail «Art. 29» précité, qui ne manquent pas de critiquer l'accord intervenu entre la

---

5 Voy. à ce sujet : P. Blok, «Botsende rechtsculturen bij transatlantisch gegevensverkeer», *N.J.B.*, vol. 3, 2001, 1607-1612.

6 Art. 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, WP66, 24 octobre 2002.

7 Joint Statement, Brussels, 17/18 février 2003 <www.cbpweb.nl>.

8 Parlement européen, résolution du Parlement européen sur le transfert de données à caractère personnel par des compagnies aériennes lors de vols transatlantiques, document nº B5-0187/2003 (P5-TA-PROV(2003)0097), procès-verbal du 13 mars 2003.

Commission européenne et les États-Unis [9]. Le groupe de travail estime en outre que les États-Unis ne peuvent utiliser les données des dossiers passagers que lorsque c'est nécessaire pour lutter contre le terrorisme, et non à d'autres fins, telles que les contrôles de routine aux frontières ou, de manière plus générale, la sécurité nationale. Le groupe de travail juge également important de ne fournir qu'un nombre réduit de données et de limiter le délai de conservation desdites données. Le groupe de travail ajoute que les autorités américaines n'offrent pas de garanties suffisantes qu'elles respecteront ces dispositions. Le groupe de travail conseille dès lors vivement à la Commission d'aboutir dans les négociations avec les États-Unis à un système de transfert de données des dossiers passagers qui s'inscrive dans le cadre de la législation européenne sur la vie privée.

Le 2 septembre 2003, un porte-parole de la Commission fait savoir que le système américain, dans les conditions actuelles, est incompatible avec le droit européen en matière de protection de la vie privée et que les Américains ne sont pas en mesure d'offrir des garanties pour la protection des données [10]. En outre, il n'y a pas eu de réponse satisfaisante susceptible de rencontrer le souci des Américains relatif au fait de pouvoir avoir accès à des données sensibles, telles que des données sur la religion, l'origine ethnique ou la santé. Ce faisant, le feu vert est donné à l'intervention des autorités nationales de contrôle contre les compagnies aériennes qui continuent à transmettre ces données.

4. Fin 2003, une nouvelle concertation a lieu entre le commissaire européen chargé des affaires douanières, Frits Bolkenstein, et un senior U.S. Homeland Security official non identifié. Dans le communiqué de presse sur cette concertation, des doutes ont été émis sur les possibilités pratiques d'infliger des amendes aux compagnies aériennes, dès lors que celles-ci devraient choisir dans ce cas entre une sanction européenne et la menace américaine de retrait de leur permis de vol aux États-Unis. L'idée de menacer également les États-Unis d'un retrait de permis de vol américains n'a de toute évidence jamais été prise au sérieux. En mai 2004, un accord politique intervient entre la Commission et les États-Unis. Sa mise en œuvre concrète a néanmoins nécessité l'intervention notamment réglementaire de plusieurs instances européennes.

---

9 Art. 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers. Data, WP78 13 juin 2003.

10 Reijo KEMPPINEN cité dans «EU : U.S. Anti-Terror Flight Rules Breach Privacy», 2 septembre 2002, <www.reuters.com/news>.

Il y a d'abord la décision de la Commission en date du 14 mai 2004 [11]. Dans cette décision, la Commission, faisant usage de ses compétences sur la base de la directive «vie privée» [12], constate que le *Bureau of Customs and Border Protection* américain est réputé offrir un niveau de protection adéquat pour la transmission de données des dossiers passagers en manière telle que plusieurs catégories de ces données peuvent être transférées dorénavant à cette organe. Ce transfert doit toutefois s'opérer conformément aux engagements du 11 mai 2004 repris dans l'annexe à la décision.

Ensuite, l'Union européenne et les États-Unis concluent le 17 mai 2004 un accord, [13] stipulant que le *Bureau of Customs and Border Protection* peut accéder, par voie électronique, aux données des dossiers passagers provenant des systèmes de réservation des transporteurs aériens européens, en application stricte de la décision de la Commission du 14 mai 2004 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 compagnies aériennes. De son côté, le *Bureau of Customs and Border Protection* déclare qu'il mettra en œuvre les engagements du 11 mai 2004, annexés à la décision de la Commission. Il est important de noter en outre, ainsi que nous le verrons plus tard, que l'accord peut être dénoncé moyennant un délai de préavis de 90 jours.

Enfin, dans la décision du 17 mai 2004, le Conseil approuve cet accord [14] et ce conformément à l'article 300, deuxième alinéa, du Traité instituant la Communauté européenne.

Dans les engagements que les États-Unis doivent tenir selon l'accord, figurent une série d'obligations concrètes concernant l'utilisation des données, le traitement des données sensibles, le mode d'accès aux données, le stockage et la protection de celles-ci, la transmission à d'autres autorités et les droits des individus concer-

[11] 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, *J.O.,* L 235/11, 1994.

[12] Article 25, sixième alinéa, de la directive.

[13] 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, *J.O.,* L 183/84, 2004.

[14] 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, *J.O.,* L 183/83, 2004.

nés. En réalité, les États-Unis obtiennent l'accès *on line* aux systèmes de réservation électroniques des compagnies aériennes européennes [15] pour y extraire des données sur des passagers de vols en provenance et à destination des États-Unis, en ce compris les personnes en transit. 34 données (les *passenger name records* ou «PNR») peuvent être demandées pour ces passagers, notamment : nom, adresse, destination, numéro du siège, agence de voyages et des données sur, par exemple, l'utilisation d'une chaise roulante ou de médicaments dans l'avion, ou des enfants qui voyagent sans être accompagnés [16]. Si les systèmes de réservation renferment aussi (d'autres) données sensibles, telles que des données sur les convictions religieuses, l'origine ethnique ou la santé, ces données seront filtrées et supprimées. Les données demandées peuvent ensuite être utilisées dans le but unique de prévenir et de combattre le terrorisme et les crimes liés au terrorisme, d'autres crimes graves, et la fuite en cas de mandat d'arrêt ou de mise en détention pour l'un des crimes susmentionnés. À cette fin, ces données peuvent être conservées trois ans et demi, ainsi qu'il appert des engagements.

Il est important de noter à ce propos que, aussi longtemps que les compagnies aériennes ne sont pas en mesure, pour des raisons techniques, d'envoyer elles-mêmes les données (*uploading*) aux systèmes informatiques des autorités américaines, ces dernières peuvent avoir accès *on-line* aux systèmes de réservation des compagnies aériennes. À cet égard, on parle de systèmes *pull* et *push* : aussi longtemps que les compagnies aériennes ne peuvent pas «pousser» elles-mêmes les données vers les systèmes des Américains (*push*), ces derniers peuvent «tirer»

[15] Plus spécifiquement, les Américains peuvent vérifier au plus tôt 72 h avant le commencement du vol et jusqu'à trois fois, le système de réservation pour y examiner 34 données.

[16] Il s'agit, selon l'Annexe A à l'accord, des données 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. Toutes les informations sur les modes de paiement; 8. Adresse de facturation; 9. Numéros de téléphone de personnes de contact; 10. Itinéraire complet pour le PNR spécifique; 11. Informations «grands voyageurs» (uniquement les miles parcourus et adresse(s)); 12. Agence de voyages; 13. Agent de voyages; 14. Informations du PNR sur le partage de codes; 15. Statut du passager; 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 (autres informations sur la fourniture de services); 27. Données SSI/SSR (informations sur la fourniture de services particuliers et les exigences posées à cette occasion); 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 éventuellement recueillies (Advanced Passenger Information System); 34. Données ATFQ (Automatic Ticketing Fare Quote).

eux-mêmes les données des systèmes de réservation (*pull*). L'une et l'autre de ces notions signifient que les Américains ont accès aux systèmes de réservation des compagnies aériennes de l'U.E., et peuvent ainsi savoir quel passager vole avec quelle compagnie aérienne vers quelle destination. Les données obtenues à propos des passagers sont comparées par les États-Unis aux données figurant dans leurs propres bases de données sur des personnes soupçonnées de terrorisme ou d'autres crimes graves, y compris la criminalité organisée, qui revêtent un caractère transnational. Si un passager figure sur cette *no fly list* américaine, il y a intervention. L'objectif de toute cette procédure est de savoir clairement, avant le départ de l'avion, si l'on peut y trouver des passagers suspectés des crimes précités.

5. Le Parlement européen ainsi que le groupe de travail «Art. 29» [17], ont critiqué la procédure. Fin mars 2003, le Parlement adopte une résolution dans laquelle il formule en des termes dénués de toute ambiguïté des réserves juridiques sur le projet de décision de la Commission. Dans cette résolution, il se réserve également le droit de saisir la Cour européenne de justice pour vérifier la légalité de l'accord visé, et en particulier sa compatibilité avec la protection de la vie privée.

Une fois la décision prise par la Commission, et après que le Conseil ait approuvé l'accord avec les États-Unis, le Parlement franchit en effet ce pas après quelques escarmouches procédurales. Fin juillet 2004, il adresse à la Cour la demande d'annulation de la décision de la Commission du 14 mai 2004 et de celle du Conseil en date du 17 mai 2004 [18]. Le Parlement invoque l'argument selon lequel les bases juridiques de ces décisions ne sont pas correctes. Selon lui, la transmission de données des dossiers passagers a lieu pour les besoins de la sécurité et ne relève pas de la directive «vie privée», qui concerne le marché intérieur et dépend par conséquent du premier pilier. En l'espèce, la transmission des données des dossiers passagers relève, selon le Parlement, du champ d'application de ce qui est appelé «le troisième pilier», à savoir : les compétences relatives au droit pénal et à la sécurité publique, matières réglées sur une base intergouvernementale. Les

[17] Groupe de travail «Article 29» sur la protection des données, Avis 4/2003 relatif au niveau de protection garanti aux États-Unis pour la transmission de données passagers, WP78 13 juin 2003; groupe de travail «Art. 29», Avis 2/2004 relatif 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 (US CBP), WP87, 29 janvier 2004.

[18] Recours formé le 27 juillet 2004 par le Parlement européen contre la Commission des Communautés européennes, *J.O.,* C 228/32, 2004.

traitements de données à caractère personnel à des fins tombant dans le champ du troisième pilier (à savoir : la sécurité publique, la défense et les activités des États membres dans le domaine pénal) sont exclus du fonctionnement de la directive [19]. Le Parlement allégue également le fait que l'accord avec les États-Unis viole les droits fondamentaux, notamment, des aspects essentiels du droit à la protection des données à caractère personnel, chose incompatible avec l'article 8 de la Convention européenne de sauvegarde des droits de l'homme. Le Parlement évoque en outre une violation du principe de proportionnalité au motif qu'un nombre excessif de données peuvent être transmises et conservées beaucoup trop longtemps par les États-Unis.

6. L'espoir et l'attente étaient, comme nous l'avons dit, que la Cour se prononce avec audace et ambition sur la garantie de la protection de la vie privée et sur la proportionnalité des transmissions de données. Mais elle ne l'a pas fait. Dans un arrêt relativement court, la Cour se penche presque exclusivement sur les questions de compétence, notamment, la question de savoir si la Commission et le Conseil ont respecté le cadre institutionnel existant et si la transmission de données relève du premier pilier (marché intérieur) ou du troisième pilier (à savoir : le droit pénal et la sécurité). À l'instar du Parlement, la Cour estime que la Commission et le Conseil ont considéré à tort que la transmission des données des dossiers passagers relève dans ce contexte du premier pilier. Par conséquent, la base juridique est erronée.

À cet égard, la Cour accorde notamment de la valeur au considérant de la décision de la Commission du 14 mai 2005, selon lequel la transmission des données à caractère personnel a pour but de prévenir et de lutter contre le terrorisme et d'autres crimes graves. Cela désigne, selon la Cour, le troisième pilier, de sorte que la directive «vie privée» 95/46, et plus particulièrement son article 3, deuxième alinéa, ne s'applique pas. La Cour annule la décision du Conseil pour la même raison. Elle reposait sur l'article 95 du Traité instituant la Communauté européenne (lu en combinaison avec l'article 300 du Traité instituant la Communauté européenne), conférant le pouvoir d'établir des règles pour la réalisation du marché intérieur. La circonstance que les données des dossiers passagers sont collectées par des particuliers à des fins commerciales et sont transférées ensuite par eux aux États-Unis, ne veut pas encore dire que la transmission en question ne relève pas du champ d'application de cette disposition. L'élément déterminant est que la

[19] Article 3, deuxième alinéa, de la directive.

transmission s'insère dans un cadre institué par les pouvoirs publics visant à garantir la sécurité publique.

À la suite de l'annulation, la Cour ne doit pas examiner le contenu des autres arguments du Parlement. Elle fixe toutefois un délai dans lequel la Commission peut encore réparer la lacune de la base juridique des décisions. La Cour considère que la Communauté ne pourrait pas invoquer qu'elle ne respecte pas l'accord avec les États-Unis au motif que son propre droit semble l'en empêcher. Pour des raisons de sécurité juridique et en vue de protéger les personnes concernées, la Cour juge dès lors approprié de maintenir les effets de la décision jusqu'au 30 septembre 2006, qui non par hasard correspond précisément au délai de préavis prévu par l'accord.

7. La Commission est, bien entendu, déçue par l'arrêt, mais elle s'empresse de signaler que l'annulation de sa décision et de celle du Conseil ne porte pas sur le contenu de l'accord, mais uniquement sur la base juridique. Et, par conséquent, l'accord peut rester inchangé sur le plan du contenu. Seule la base doit être adaptée. La nouvelle base est l'article 38 du Traité instituant la Communauté européenne, qui relève tout simplement du champ d'application du troisième pilier (la coopération en matière judiciaire et de police), mais qui renvoie également à l'article 24 du Traité instituant la Communauté européenne qui relève du champ d'application du deuxième pilier (politique étrangère et de sécurité commune).

Néanmoins, de nouvelles négociations sont nécessaires. Pressés par le temps, la Commission et les États-Unis parviennent, une semaine après l'expiration du délai fixé par la Cour, le vendredi 7 octobre, à un nouvel accord [20]. Contrairement à ce qu'a déclaré la Commission à ce moment-là, ce nouvel accord ne correspond pas tout à fait, sur le plan du contenu, à l'accord précédent. Aux termes du nouvel accord, les États-Unis semblent pouvoir faire beaucoup plus avec les données transférées : outre le *Bureau américain of Customs and Border Protection*, la CIA et le BEFI ont également accès maintenant aux données passagers. Il doit s'agir toutefois de passagers pouvant présenter un «certain risque» dans le cadre de la lutte contre le terrorisme. Bien que, par conséquent, il ne soit pas question, en théorie, d'un accès automatique aux données passagers, l'interprétation de la notion «un certain risque» est laissée à l'appréciation des divers services américains de renseignements et de sécurité. Peu importe, en fait, qui procède à la collecte des données, les services de renseignements américains reçoivent quand

[20] COM2006.

même les informations qu'ils veulent avoir. Dans ces circonstances, le Parlement n'accueille pas le nouvel accord avec une joie unanime [21].

8. L'arrêt et l'argumentation de la Cour rendent la législation et la réglementation de l'Union européenne précaires et instables. Si nous comprenons bien, la Cour considère que le transfert et la transmission de données des dossiers passagers doivent être considérés comme une question relevant davantage du troisième pilier (à savoir : la justice et la sécurité) plutôt que du premier pilier (marché intérieur) – et ce, parce que la dimension liée à la sécurité pèse en fin de compte beaucoup plus lourd que les considérations liées à la concurrence au sein de la Communauté.

Cette argumentation peut se comprendre, et n'est pas vraiment neuve non plus. Nous pouvons y voir une continuation d'une approche fonctionnelle des questions relatives aux compétences dans l'Union européenne, approche également suivie dans l'arrêt dit «*Environnement*» du 13 septembre 2005. Aux termes de celle-ci, un sujet touchant au marché intérieur, qui relève du premier pilier, peut devenir à un certain moment une affaire de justice et relever par conséquent du troisième pilier, lorsque les éléments droit pénal et sécurité sont prépondérants. Le point 48 de l'arrêt semble dire que l'aspect «prépondérant» n'est même pas nécessaire. Ce qui semble être important c'est l'effectivité. La dimension pénale d'une norme communautaire peut être marginale par rapport à l'ensemble sans pour autant lui faire perdre son effectivité. Un article suffit…

L'inverse peut aussi se produire : un sujet du troisième pilier se transforme en sujet du premier pilier lorsque les éléments droit pénal et sécurité ne sont plus prépondérants. Dans l'arrêt «*Environnement*», la Cour a annulé une décision cadre du Conseil sur la protection de l'environnement par le recours à des sanctions pénales [22]. La Cour a soulevé l'argument que les sanctions pénales prescrites dans la décision cadre peuvent seulement résulter du premier pilier, alors que la décision cadre concernait un instrument du troisième pilier.

À la lumière dudit arrêt environnement, le prononcé de l'arrêt *PNR* n'est peut-être pas aussi incompréhensible qu'il y paraît. Mais, nonobstant cela, ce n'est pas encore heureux. Savoir si un élément appartient au premier ou au troisième pilier s'avère sou-

[21] Selon la rapporteuse libérale Sofie in 't Veld, à l'assemblée plenière du Parlement européen le 11 octobre 2006 (via http ://www.europarl.europa.eu/eplive/expert/shotlist_page/20061010SHL11541/default_nl.htm).

[22] C.J.C.E., 13 septembre 2005, *Commission c. Conseil*, aff. C-176/03 ; à ce sujet P. De Hert, P. Paepe et H. Griffioen, «Europees milieustrafrecht – Minder ruimte voor nationale strafbevoegdheden», *Nieuw Juridisch Weekblad*, 2006, nº 144, 482-495.

vent délicat et peut donner lieu à des discussions dans presque tous les cas. Un exemple de situation où ce risque existe concerne la directive 2006/24 sur la conservation de données traitées dans le cadre de l'offre de services de communications électroniques (pour des raisons de facilité, nous appelons cette directive la directive «conservation des données» [23]). Sur la base de cette directive, les entreprises du secteur des communications électroniques sont tenues de conserver les données de trafic – c'est-à-dire : les données sur la manière dont il est fait usage de services de télécommunications – et de les tenir à disposition dans le cadre (notamment) de la lutte contre le terrorisme. La directive «conservation des données» a été élaborée dans le cadre du premier pilier au motif que les communications électroniques ont été considérées de tout temps comme une question de marché intérieur [24] et sans doute aussi parce que les autres directives [25] prises dans ce domaine relèvent du premier pilier.

Après l'arrêt *PNR*, il y a tout lieu de se demander si c'est encore tout à fait exact. La directive «conservation des données» porte encore et toujours sur le secteur des communications électroniques, mais aussi et peut-être surtout sur la sécurité. Ce faisant, un sentiment de doute et d'insécurité juridique réapparaît et projette son ombre sur une autre législation et réglementation européenne, dans laquelle s'abritent peut-être des éléments mixtes de sécurité et de marché intérieur [26]. En

---

[23] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.,* L 105, 2006.

[24] David Cronin, «EU lawyers judge data retention scheme illegal», *European Voice*, vol. 11, nº 14, 14 avril 2005.

[25] À savoir : directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre») *J.O.,* L 108/33, 2002; directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive «Autorisation»), *J.O.,* L 108/21, 2002; directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive «Accès») *J.O.,* L 108/7, 2002; directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive Service universel) *J.O.,* L 108/51, 2002; 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) *J.O.,* L 201/37, 2002; directive 2002/77/CE de la Commission du 16 septembre2002 relative à la concurrence dans les marchés de réseaux et des services de communications électroniques, *J.O.,* L 249/21, 2002.

[26] La même insécurité peut d'ailleurs se produire lorsqu'il s'agit d'une législation qui comporte des éléments du premier et du deuxième pilier.

l'absence d'une Constitution européenne qui abroge le système de piliers, nous devons nous attendre, comme d'autres l'ont également fait remarquer [27], à davantage de jurisprudence de la Cour. Tous ces éléments font de l'Union européenne un législateur peu fiable.

À notre avis, partagé également par d'autres, les choses auraient pu se passer autrement. À l'instar de Hijmans, nous pensons que la base des décisions du Conseil et de la Commission aurait pu être trouvée dans le premier pilier, même si l'objectif majeur de ces décisions n'en dépend sans doute pas [28]. Hijmans renvoie à cet égard à l'arrêt *British American Tobacco* [29], où l'objectif principal de la directive concernée était la protection de la santé publique par la lutte contre le tabac (problématique ne relevant pas des compétences de l'U.E.); néanmoins, cette directive pouvait reposer, selon la Cour, sur l'article 95 du Traité instituant la Communauté européenne (autrement dit : le premier pilier) parce que la directive fixait des règles concernant le négoce de cigarettes sur le marché intérieur. Dans l'arrêt *PNR*, la Cour aurait pu partir du même raisonnement et dire que l'objectif principal des décisions se situait certes dans le champ pénal, mais que l'élément fondamental concernait la manière de traiter des données collectées au départ dans des relations commerciales.

Et à l'instar de Kranenborg, nous sommes d'avis que la Cour aurait mieux fait de faire confiance aux motifs de la Commission et du Conseil en prenant en considération la directive «vie privée» comme un instrument du premier pilier dans le cadre de la question des données des dossiers passagers [30]. En effet, cet auteur considère que l'élément sécurité réside avant tout dans la législation américaine, et moins dans les considérations de la Commission et du Conseil relatives au fait de trouver une solution à un problème auquel se heurtaient des compagnies aériennes en Europe, en l'espèce, le fait que la concurrence était faussée parce que certaines compagnies étaient en mesure, et d'autres non, de satisfaire aux conditions fixées par les États-Unis. L'arrêt mentionne que le Conseil a soulevé cet argument dans la procédure devant la Cour [31]. Mais peut-être parce que cela ne

[27] «Don't blame ECJ for filling treaty void», éditorial dans *European Voice*, vol. 12, 4 mai 2006, 8.
[28] H. Hijmans, «De derde pijler in de praktijk : leven met gebreken – Over de uitwisseling van informatie tussen lidstaten», *SEW,* 2006, 91, pp. 382-383.
[29] C.J.C.E., 10 décembre 2002, aff. C-491/01, *British American Tobacco* et *Imperial Tobacco, Jur.*, p. I-11453, considérant 94.
[30] H. Kranenborg, sous C.J.C.E., 30 mai 2006, aff. C-317/04 et C-318/04, *C.E.D.H.*, 2006, nº 81, 765.
[31] Selon le considérant 64 de l'arrêt.

transparaît pas directement du texte des décisions de la Commission et du Conseil, cela n'a pas convaincu la Cour.

9. De surcroît, l'arrêt met au jour des vices du système au niveau institutionnel. Selon la Cour, les décisions relatives au transfert et à la transmission de données sur les passagers doivent être prises dans le cadre du troisième pilier. Et, ce que le Parlement européen n'a sans doute pas suffisamment réalisé lorsqu'il a saisi la Cour, cela veut dire ni plus ni moins que son importance et son contrôle sur cette prise de décision sont largement rabotés [32]. Car, contrairement aux questions du premier pilier qui concernent le marché intérieur, le Parlement ne joue pas de rôle législatif pour des décisions dans le cadre du troisième pilier, qui portent sur la sécurité et le droit pénal. S'il s'agit de questions du troisième pilier, le Parlement est seulement consulté et peut uniquement, sur la base de l'article 39 du Traité instituant la Communauté européenne, rendre un avis non contraignant. Le Parlement ne peut pas non plus s'adresser à la Cour, ce qu'il pouvait encore faire, comme nous l'avons vu, dans l'hypothèse d'une décision relevant du premier pilier.

Le Parlement a dès lors dû apprendre des médias qu'un nouveau projet d'accord était soumis aux États-Unis. À la suite de cette annonce, il a adressé à la Commission une demande en vue d'être au moins informé [33]. La Commission a ensuite promis d'impliquer davantage le Parlement dans les négociations avec les États-Unis. Mais l'avenir nous dira si cette promesse dépassera le stade de la seule déclaration d'intention. En tous cas, les cadres institutionnels offrent peu de possibilité de l'y contraindre.

Dans le même registre, l'importance de la Cour est affaiblie pour des décisions prises sur la base d'un fondement du troisième pilier. Ainsi, la Cour ne peut pas se prononcer, dans le cadre du troisième pilier, sur un accord conclu aux termes des articles 24 et 38 du Traité instituant la Communauté européenne, mais seulement sur la validité et l'interprétation de la décision du Conseil de conclure l'accord, et ce, uniquement à la suite d'une procédure préjudicielle ou à l'initiative de la Commission ou de l'un des États membres [34]. Le Conseil doit décider à l'unanimité et

[32] H. KRANENBORG, sous C.J.C.E., 30 mai 2006, aff. C-317/04 et C-318/04, *C.E.D.H.*, 2006, nº 81, 751-766; E. GUILD et E. BROUWER, «The Political Life of Data – The ECJ Decision on the PNR Agreement between the EU and the US», *CEPS Policy brief*, juillet 2006, 3-5 <www.ceps.be>.

[33] Lettre du président du Parlement Jean-Marie Cavada et de la parlementaire européenne Sofie in 't Veld en date du 23 août 2006 au Conseil <www.statewatch.org>. Voy. aussi M. KRANENBURG, «Europarlement waakt over passagiersgegevens», *NRC*, 7 septembre 2006.

[34] H. KRANENBORG, *loc. cit.*, 763. Nous constatons que seulement 14 États membres ont fait la déclaration (nécessaire) pour permettre à des juges nationaux de poser une question préjudicielle

la Commission perd donc l'initiative sur ce point. S'il s'agit d'un accord reposant sur les articles 24 et 38 du Traité instituant la Communauté européenne, les négociations y afférentes peuvent se dérouler en principe sous la présidence de l'Union (article 24 du Traité instituant la Communauté européenne). Cependant, comme il est souvent hors de question, pour des raisons pratiques, qu'un État membre dirige les négociations avec les États-Unis, il est évident que la Commission continue malgré tout de garder l'initiative dans ce domaine.

Enfin, il y a l'autorité européenne chargée de la protection des données, le *European Data Protection Supervisor*. Dans un jugement interlocutoire, la Cour a tranché que cette autorité de contrôle européenne pouvait intervenir dans la procédure et faire connaître son opinion [35]. Cela n'allait pas tout à fait de soi : cet organe encore assez récent contrôle, d'après la décision l'instituant, le traitement de données à caractère personnel par des institutions européennes [36]. Que la Cour autorise cet organe à intervenir dans une procédure lorsqu'il s'agit du traitement de données à caractère personnel par des particuliers, peut être considéré comme une interprétation compréhensive de la réglementation. Compréhensive, mais pas à tort.

La prise de décision en Europe n'a pas gagné en clarté avec l'arrêt. Et ce dernier n'a pas amélioré la crédibilité de l'Union en tant que partie fiable dans les négociations avec les États-Unis [37]. Et, constat qui n'est peut-être pas beaucoup plus insignifiant, il appelle, en terme de légitimation démocratique, plus que de simples interrogations. Il s'agit d'une question qui touche à la protection de la vie privée de nombreux, et même de très nombreux, citoyens européens. S'il y a une conclusion que nous pouvons tirer de l'arrêt, c'est précisément la nécessité pour le Parlement européen d'effectuer un contrôle étroit dans ce domaine.

à la Cour. Voy. Commission, communication visant l'adaptation des dispositions du titre IV du traité instituant la Communauté européenne relatives aux compétences de la Cour de justice, en vue d'assurer une protection juridictionnelle plus effective, Bruxelles, 28 juin 2006 com(2006) 346 final (http ://ec.europa.eu).

35 Voy. aussi les «orders» de la Cour du 17 mars 2005, autorisant l'EDPS à présenter sa vision : EDPS, «EDPS at oral hearing in the Court of Justice», *EDPS Newsletter*, nº 1, 27 octobre 2005, 3-4 (www.edps.europa.eu.).

36 Décision du Parlement européen et du Conseil du 22 décembre 2003 portant nomination de l'autorité de contrôle indépendante prévue à l'article 286 du traité CE (2004/55/CE), *J.O.,* L 012, 2004, ainsi que le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.,* L 008, 2001.

37 E. Guild et E. Brouwer, *loc. cit.*, 3.

10. Pour celui qui pensait que, avec la directive «vie privée», la protection de sa vie privée était garantie, l'arrêt *PNR* est sans doute décevant. Il convient cependant de relativiser quelque peu ce sentiment. Et ce, parce que la chronologie des événements qui ont conduit à l'arrêt, montre que le système de législation et d'institutions qui a été mis en place dans la Communauté dans le cadre de la protection des données à caractère personnel, a bien fonctionné malgré tout. Le groupe de travail «Art. 29» a pu inscrire rapidement la question à l'agenda politique. En outre, plusieurs autorités nationales de contrôle, dont la néerlandaise, ont pu apporter une contribution à la recherche de solution au problème. En même temps, nous devons toutefois bien constater qu'il n'a pas été possible de trouver une solution ni au sein des cadres offerts par ces législations nationales relatives à la protection de la vie privée ni au sein de la directive «vie privée» [38]. À noter également que peu d'autorités nationales de contrôle ont pris des mesures de sauvegarde lorsque cela était possible et peut-être même nécessaire. Aucun des contrôleurs nationaux n'a éprouvé le moindre doute relativement au fait que la transmission des données passagers n'était pas autorisée sur la base de la législation nationale de protection de la vie privée. Et pourtant, la plupart des autorités de contrôle [39], dont la commission néerlandaise de protection des données à caractère personnel, n'ont pas voulu entreprendre beaucoup plus qu'un envoi de requêtes pressantes.

11. Contrairement à ce qu'on avait pensé et espéré, la Cour ne s'est pas prononcée sur les garanties de la protection de la vie privée, sur la proportionnalité du transfert de données sur une grande échelle et sur les pouvoirs des autorités de contrôle. Blok a souligné que, le cas échéant, il n'y a pas ou peu de restrictions au transfert de données sur les passagers et d'autres données à caractère personnel à des autorités de recherche et à des services de renseignements étrangers [40]. Le superviseur européen à la protection des données, P. Hustinx, considère que

[38] Voy. pour une analyse fouillée du rôle de la protection des donnée dans des débats tels que ceux sur les données passagers et sur les caméras : P. De Hert et S. Gutwirth, «Veiligheid en grondrechten – Het belang van een evenwichtige privacypolitiek», *in* E.R. Muller (réd.), *Veiligheid – Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn, 2004, pp. 585-630.

[39] L'autorité de contrôle italienne a interdit à la compagnie aérienne Alitalia de continuer à transmettre des données à caractère personnel. La CBP tardant à prendre une initiative comparable, des questions ont été posées à la Chambre (deuxième chambre) au ministre de la Justice Donner. *Cfr.* «SP stelt vragen over privacy op vluchten VS», *Staatscourant*, 29 juillet 2003, (nº 143), 5.

[40] P. Blok, «Rechtzaak van het Europarlement is geen zegen voor *privacy* van de luchtvaartreiziger», *NJB*, 2006, p. 25.

l'arrêt est un «*loophole in the protection of the European citizen*» [41]. Et le membre du Conseil d'État Hirsch Ballin fait remarquer que le Parlement européen s'est tiré lui-même une balle dans le pied [42]. D'autres auteurs ont utilisé des termes moins forts, mais ils expriment quasiment tous leur souci à propos des conséquences de l'arrêt [43].

La thèse selon laquelle l'arrêt élimine toute forme de limitation des transferts des données sur les passagers et d'autres données à caractère personnel à des autorités de recherche et à des services de renseignements étrangers [44], doit toutefois être modulée quelque peu. L'article 8 de la Convention [45] et la Convention de Strasbourg pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [46] s'appliquent en effet intégralement et peuvent également apporter une protection dans ce domaine. Mais tout cela n'enlève rien à l'incohérence liée au fait que la collecte de données passagers par des compagnies aériennes relève manifestement de la directive «vie privée», mais pas le transfert de ces données aux États-Unis et peut-être à d'autres pays offrant un niveau de protection encore (beaucoup) plus bas, lorsque cette transmission s'opère pour des raisons touchant à la sécurité nationale [47]. Ce n'est pas aisément explicable, et ce, pour deux raisons. *Primo*, pourquoi sommes-nous protégés par la directive lorsque des données sont collectées, et nous le savons, à des fins incontestablement commerciales, à savoir : les services fournis par des compagnies aériennes, et que nous avons demandés, alors que nous ne sommes pas protégés lorsque ces mêmes

[41] EDPS first reaction to the Court of Justice Judgment, 31 mai 2006 <www.libertysecurity.org/article985.html>.

[42] À l'occasion de l'assemblée annuelle de la NJV en date du 9 juin 2006 à Maastricht.

[43] H. Hijmans, «De derde pijler in de praktijk : leven met gebreken – Over de uitwisseling van informatie tussen lidstaten», *SEW,* 2006, 91, pp. 382-384.

[44] P. Blok, «Rechtzaak van het Europarlement is geen zegen voor privacy van de luchtvaartreiziger», *NJB,* 2006, 26.

[45] E. Guild et E. Brouwer, *loc. cit.,* 3, ont déjà souligné que la Cour, dans l'énumération habituelle des dispositions pertinentes, cite en premier lieu l'article 8 de la Convention européenne des droits de l'homme, l'article consacrant le droit à la protection d'une vie privée. C'est étonnant en soi, car il n'est pas démontré précédemment, du moins pas à notre connaissance, que la Cour ne commence pas par une disposition du droit communautaire. Celui qui lit l'arrêt pour la première fois, pourrait en conclure à ce moment-là que la Cour a choisi ce droit fondamental comme point de départ et se forgerait, peut-être à la lumière des critères du deuxième alinéa, un avis sur la proportionnalité de la transmission. Mais ce n'est pas le cas. La Cour s'en tient dans l'arrêt à cet unique renvoi et ne revient pas dessus.

[46] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, January 28, 1981, *European Treaty Series*, n° 108.

[47] European Data Protection Supervisor, «PNR Judgement», in *Newsletter,* n° 4, 1er juin 2006, sub 4 via www.edps.europa.eu.

données sont ensuite utilisées pour servir la sécurité nationale d'un pays dans lequel nous ne pouvons pas ou guère prétendre à une protection de la vie privée digne de ce nom... ? *Secundo*, l'arrêt *PNR* ne semble guère pouvoir s'inscrire dans la jurisprudence, non exempte de critiques, de la Cour relative à la directive «vie privée». Ainsi, dans l'arrêt *Österreichiser Rundfunk* [48], on se demandait si la réglementation autrichienne qui charge certaines instances de transmettre des informations sur le salaire et la pension des travailleurs à l'autorité de contrôle Rechnungshof, qui publie ensuite ces données dans un rapport public, tombe dans le champ d'application de la directive. Le gouvernement autrichien dit que la directive ne s'applique pas et que la réglementation ne relève absolument pas du droit communautaire, parce que le contrôle par la Rechnungshof poursuit des objectifs d'intérêt général dans le domaine des finances publiques. La Cour ne partage pas ce point de vue et dit que, pour l'application de la directive, un lien direct avec l'une des libertés fondamentales du Traité instituant la Communauté européenne, notamment, par exemple, la libre circulation des travailleurs, n'est pas nécessaire. En outre, les limites de la directive deviendraient vagues et incertaines s'il y a lieu de vérifier chaque fois s'il existe un lien avec les libertés fondamentales du Traité instituant la Communauté européenne, précise la Cour. Dans l'arrêt données passagers, la Cour s'éloigne de cette application libérale, large, de la directive [49].

Dans l'affaire *Lindqvist*, la question était de savoir si la directive s'applique à une bénévole suédoise qui place des données à caractère personnel sur un site web. Une autre question était : s'agissait-il d'une transmission de données, étant donné que ce site web était accessible depuis des pays non européens ? Pour «sauver» la directive, la Cour s'est vue contrainte d'interpréter la notion de transfert dans la directive pour que l'interdiction de transfert ne s'applique pas à des données placées sur un site web et qui peuvent être consultées d'en dehors de l'Union européenne (c'est-à-dire : un cas de «*pull*») [50]. À la suite de cet arrêt *Lindqvist*, divers auteurs [51] ont souligné dès lors que la directive, lorsqu'il s'agit

48 C.J.C.E., 20 mai 2003, *Österreichiser Rundfunk*, aff. C-465/00.

49 E. Guild et E. Brouwer, *loc. cit.*, 4.

50 G.-J. Zwenne, *Bodil Lindqvist,* note sous C.J.C.E., 6 novembre 2003, *JAVI,* 2004/2, 66-70 ; P. De Hert et W. Schreurs, «De bescherming van persoonsgegevens op het Internet : nuttige verduidelijking door de rechtspaak», note sur C.J.C.E., 6 novembre 2003 (*Bodil Lindqvist c. Suède*), *A&M,* 2004/2, 127-138.

51 P.J. Hustinx, «Data Protection in the European Union», *P&I*, 2005-2, 62-65 ; P.H. Blok, «De waarde van de omnibuswet», *P&I*, 2005-6, 247 ; G.-J. Zwenne, *Bodil Lindqvist*, note sous C.J.C.E., 6 novembre 2003, *JAVI,* 2004-2, 66-69.

de traitements transfrontaliers et de développements technologiques, connaît davantage ce genre de carence, et entretient plus précisément des relations difficiles avec le monde d'internet [52]. Ce ne sont pas des incidents ou des accidents d'entreprise isolés.

D'une part, la directive «vie privée» s'applique par conséquent, selon l'arrêt *Lindqvist* – et ce de manière tendue – à internet et à d'autres activités quotidiennes souvent innocentes, mais transnationales. Mais, d'un autre côté, la même directive ne s'applique pas, selon l'arrêt *PNR*, à des transferts de données structurels, sur une grande échelle et difficilement contrôlables, tels que ceux effectués dans le cadre de la lutte contre le terrorisme. Nous ne sommes pas contre ces traitements, mais nous attendons, sous l'angle de la protection de la vie privée et des droits fondamentaux, une meilleure prise en compte des risques de ceux-ci et des garanties contre lesdits risques [53].

En ce moment, l'Europe planche sur une loi-cadre protection des données pour des traitements du troisième pilier. Cependant, les négociations n'avancent guère, semble-t-il, et il ne reste pas grand-chose de la première proposition de la Commission. Il y a une forte tendance au sein des négociateurs qui ne veulent pas d'une réglementation européenne pour des «traitements de sécurité nationale» (destinés à une utilisation *law enforcement* dans un pays), mais uniquement pour des traitements destiné à des fins intraeuropéennes (utilisation transfrontalière du *law enforcement*). Il y a également une tendance tout aussi forte qui veut profiter de la nouvelle initiative pour rendre la protection des données inoffensive, dans la mesure du possible, et veut décharger le plus possible l'industrie du *law enforcement* [54]. Attendons ce qui va en sortir.

---

[52] Un exemple concerne les *cookies*, les fichiers textes qui sont enregistrés par des sites web sur l'ordinateur de l'utilisateur internet, par exemple, pour stocker le mot de passe et le nom d'utilisateur de celui-ci. Selon le groupe de travail «Art. 29», l'utilisation de *cookies* peut entraîner l'application de la directive, même si le serveur de ce site web ou le fournisseur de celui-ci ne se trouve pas dans l'Union européenne et ne s'adresse pas à des résidents de l'Union européenne. Selon le groupe de travail «Art. 29», document de travail concernant l'application internationale de la législation sur la protection des données de l'Union européenne au traitement de données à caractère personnel sur internet par des sites web situés en dehors de l'Union européenne, WP56, 30 mai 2002.

[53] A.H.J. Schmidt et G.-J. Zwenne, «Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens», *Mediaforum,* 2005/9, pp. 292-302.

[54] E. Guild et E. Brouwer, *loc. cit.,* 5-6.; E. Brouwer, P. De Hert et R.. Saelens, «Ontwerp-Kaderbesluit derde pijler holt bescherming persoonsgegevens uit», *Privacy & Informatie*, 2007, vol. 10, nº 1, 9-13.

Post scriptum

L'accord du 19 octobre 2006, ayant expiré le 31 juillet dernier, a été remplacé par un nouvel accord conclu le 26 juillet dernier à Washington[55]. Par cet accord, l'Union européenne s'engage à ce que les transporteurs aériens assurant un service de transport international de passagers à destination ou au départ des États-Unis rendent disponibles les données PNR stockées dans leurs systèmes de réservation comme l'exige le DHS.

Le nouvel accord consacre les dispositions suivantes :

- le nombre d'autorités américaines qui pourront accéder aux données PNR sur le territoire américain a été étendu ;
- les finalités d'utilisation des données PNR pourront varier en cas de modification unilatérale de leur législation par les États-Unis ;
- la décision éventuelle de transférer des données PNR européennes vers d'autres pays tiers sera prise de manière unilatérale par les États-Unis, sans consultation préalable des autorités européennes ;
- il est désormais possible aux autorités américaines, «en cas de nécessité», d'avoir accès à des données dites «sensibles», c'est-à-dire pouvant révéler l'origine raciale, ethnique, les opinions politiques, l'état de santé des personnes, malgré un filtrage initialement prévu ;
- les données seront conservées non plus 3 ans et demi mais 15 ans, sous forme d'une conservation «active» pendant 7 ans et «passive» pendant 8 ans, sans garantie que les fichiers non consultés soient définitivement détruits ;
- le passage du mode *pull* actuellement en vigueur (c'est-à-dire l'accès direct par les autorités américaines aux données détenues par les compagnies aériennes) au mode *push* (c'est-à-dire l'envoi des données par les compagnies aériennes, ne permettant plus d'accès direct aux autorités américaines) ne sera réalisé au 1er janvier 2008 que si les conditions techniques de ce passage paraissent acceptables aux États-Unis ;

[55] Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), *J.O.U.E.* L. 204, du 4 août 2007, pp. 16-17.

– l'évaluation de l'application de l'accord (*review*) perd son caractère annuel obligatoire. Seul le commissaire européen de la direction générale Justice, liberté, sécurité sera chargé de cette inspection, sans que les autorités nationales de protection des données y soient clairement associées ;

– les autorités américaines auront la faculté de décider de manière unilatérale s'il sera répondu favorablement aux demandes des passagers européens d'accès et de rectification aux données les concernant détenues par les autorités américaines.

Le nouvel accord met certes un terme à la période d'incertitude ouverte par la décision de la Cour de justice des Communautés européennes du 30 mai 2006 annulant le précédent accord conclu le 28 mai 2004. Cependant, d'après les autorités européennes de protection des données, le Parlement européen et le contrôleur européen, cet accord est loin d'offrir un niveau de protection adéquat aux données PNR transmises [56]. On ne peut en effet que regretter l'insuffisance de dispositions claires et proportionnées relatives au partage d'informations, de conservation, d'envois supplémentaires de données, de contrôle par les autorités de protection des données, et s'inquiéter de ce que la mise en œuvre de nombreuses dispositions soit soumise à la discrétion des États-Unis.

Gerrit-Jan Zwenne et Paul De Hert [57]

[56] Voir Groupe de travail «Article 29» sur la protection des données, avis 7/2006 sur l'arrêt de la Cour de justice du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04 relatives au transfert de données PNR aux États-Unis et à la nécessité urgente d'un nouvel accord, adopté le 27 septembre 2006, 01612/06/FR, WP 124, 3 p. site internet : http ://europa.eu.int/comm/justice_home/fsj/privacy/index_fr.htm.

[57] Gerrit-Jan Zwenne est avocat à La Haye et professeur (UHD) à l'Université de Leiden. Paul De Hert est professeur (UHD) à l'Université de Tilburg et professeur à la Vrije Universiteit Brussel. Pour ce dernier, cet article constitue une contribution à une étude VIDI, *Law, technology, and shifting balances of power*.