LES CONSÉQUENCES DE L'ACCORD *PASSENGER NAME RECORD* SUR LA PROTECTION DES DROITS FONDAMENTAUX EN EUROPE

Sophie CLAVET[1]
Doctorante en Droit, Centre de recherche sur les Droits de l'Homme,
Université Panthéon-Assas (Paris II)

Les négociations transatlantiques témoignent d'un contexte diplomatique complexe. D'un point de vue politique, les États-Unis affirment leur volonté d'appliquer leurs législations relatives à la sécurité intérieure aux États tiers. Ce facteur, conjugué à un état de guerre déclaré contre le terrorisme international, met en valeur la spécificité américaine. La législation américaine comporte par ailleurs des dispositions à caractère extraterritorial ; en découle un conflit de loi substantiel touchant plus particulièrement la question de la protection des données personnelles et du droit à la vie privée. L'absence de texte juridique spécifique ne fait que renforcer l'insécurité juridique qui entoure la coopération transatlantique en matière de transfert de données personnelles à fin de lutte antiterroriste. D'un point de vue économique, les États-Unis disposent d'un argument de poids qui influence notablement la coopération : la perspective d'imposition de lourdes sanctions pécuniaires ainsi que de la suppression du droit d'atterrissage sur le territoire américain des compagnies aériennes européennes représentent un risque de pertes financières considérables pour l'Union et ses États membres. C'est dans un tel cadre que la Commission européenne s'est engagé dans un processus de négociation d'un « accord P.N.R. » et ce, sur la base de l'article 38 Traité de l'Union européenne (T.U.E., Titre VI), pour obtenir des engagements sur le respect de la législation européenne[2]. A la suite de ces négociations, la Commission a adopté une décision constatant que les procédures américaines et les engagements des États-Unis offraient une protection « adéquate»[3] compte tenu des exigences posées par l'article 25 de la directive sur la protection des données personnelles[4]. Le 17 mai 2004, le Conseil a approuvé l'accord sur le traitement et le transfert des données P.N.R. par les transporteurs aériens au *Customs and Border Protection* (C.B.P.)[5] et celui-ci a été signé le 28 mai 2004.

[1] L'auteur est titulaire d'un LL.M en Droit Américain obtenu à la Boston University et présente l'Examen du Barreau de New York.

[2] de KERCHOVE, Gilles, et WEYEMBERGH, Anne, *Sécurité et justice : enjeu de la politique extérieure de l'Union européenne*, Bruxelles, Institut d'Études Européennes, Éditions de l'Université de Bruxelles, 2003, p. 195.

[3] 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 [notifiée sous le numéro C (2004) 1914], Journal officiel n° L 235 du 6 juillet 2004, pp. 11-22.

[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, Journal officiel n° L 281 du 23 novembre 1995, pp. 31-50.

[5] 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, Journal officiel n° L 183 du 20 mai 2004, p. 83.

I. - La procédure d'adoption de l'accord international initial

Dès le mois de janvier 2003, les compagnies aériennes basées dans l'Union européenne effectuant des vols commerciaux à destination ou via les États-Unis ont été dans l'obligation de se conformer à la législation américaine et d'autoriser l'accès du C.B.P. aux données du dossier passager avant le décollage. La Commission européenne a informé les autorités américaines du conflit de loi potentiel que représente cette obligation qui entraînerait la violation de la législation communautaire et la législation des États membres relative à la protection des données personnelles. L'entrée en vigueur de la législation américaine envers les transporteurs européens a donc été repoussée au 5 mars 2003, afin de négocier un accord compatible avec la législation communautaire concernant le transfert des données P.N.R. En parallèle, le Parlement européen a adopté une série de résolutions[6] recommandant le respect de la directive 95/46/CE; le Groupe de travail 29 a pour sa part largement critiqué les demandes américaines[7], estimant notamment que le principe de proportionnalité n'était pas respecté. Les négociations ont abouti à un accord le 16 décembre 2003, suivi d'une communication de la Commission attestant de la volonté d'une démarche globale de l'Union européenne[8]. L'accord P.N.R. conclu le 28 mai 2004 est traité comme relevant du premier pilier et a permis de placer la Commission, et non les États membres, au cœur des négociations transatlantiques.

A. Les droits fondamentaux passés sous silence dans la réponse de la Cour de Luxembourg

Le 21 avril 2004, le Parlement décide de porter l'affaire devant la Cour de Justice des Communautés Européennes (C.J.C.E.) par le biais d'un recours en annulation de la décision de la Commission ainsi que de celle du Conseil. Présentant le cadre juridique de l'affaire, la Cour mentionne en premier lieu l'article 8 [9] de la Convention européenne des droits de l'homme (C.E.D.H.)[10]. Pour la première fois, la Cour de Justice débute un jugement en faisant référence non pas à la législation communautaire mais à une

[6] Résolution du 13 mars 2003 du Parlement européen sur la transmission des données personnelles par les compagnies aériennes lors des vols transatlantiques, P5_TA (2003)0097 ; et Résolution du Parlement européen sur la transmission des données personnelles par les compagnies aériennes dans les cas de vols transatlantiques : état des négociations avec les États-Unis, P5_TA (2003)0429.

[7] Avis 4/2003 sur le Niveau de Protection assuré aux États-Unis pour la Transmission des Données Passagers, Adopté le 13 juin 2003, 11070/03/FR, WP 78, « Remarques générales », p. 4.

[8] Communication de la Commission au Conseil et au Parlement, Transfert des données des dossiers passagers (*Passenger Name Record* - PNR): « *Une démarche globale de l'Union européenne* », COM (2003) 826 final, Bruxelles, le 16 décembre 2003, p.6 : « *L'option qui aurait consisté, du côté de l'UE, à insister sur le respect du droit communautaire aurait été politiquement justifiée, mais (...) aurait ébranlé l'influence de conseils plus modérés et coopératifs à Washington et remplacé par un rapport de force la coopération constructive que nous menons avec notre partenaire.* »

[9] Convention E.D.H., Article 8, « *Droit au respect de la vie privée et familiale : 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 sécurité 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*. »

[10] C.J.C.E., Grande chambre, 30 mai 2006, *Parlement européen c. Conseil de l'Union européenne* , Affaires jointes C-317/04 et C-318/04, point 3.

convention internationale relative aux droits de l'homme à laquelle elle n'est pourtant pas partie. Cette référence est d'autant plus surprenante que par la suite, le jugement de la Cour ne se réfère plus à l'article 8 de la C.E.D.H. en ce qu'elle n'aborde pas la question de la violation du droit à la vie privée. Effectivement, la Cour conclu que la décision d'adéquation et l'accord transatlantique ne peuvent trouver leur base légale dans la politique des transports de l'Union européenne. La Cour se réfère à la finalité poursuivie et inscrite au préambule de l'accord P.N.R.[11] afin de considérer que le transfert des données P.N.R. est une opération entrant dans le cadre de la sécurité publique et des activités de l'État en matière criminelle. Ce faisant, la Cour juge que la directive 95/46/CE n'est pas applicable en l'espèce en vertu de son article 3 (2)[12]. La Cour annule ainsi l'accord et la décision d'adéquation sur le fondement qu'ils n'entrent pas dans le cadre des activités relatives au premier pilier en matière de transport.

1. La décision d'adéquation adoptée *ultra vires* par la Commission

En l'espèce, la Cour s'est limitée à examiner le premier moyen selon lequel la décision prise par la Commission était adoptée ultra vires, en violation de son champ d'application. Selon les juges de Luxembourg, il ne s'agissait pas d'activités relevant du droit communautaire, mais du droit pénal. Le transfert des données visait la lutte contre le terrorisme, même si les P.N.R. étaient à l'origine collectées par les compagnies aériennes dans le cadre d'une activité qui relevait du droit communautaire.

a. Restriction du champ d'application de la Directive 95/46/CE

Cet arrêt de la Cour de Justice démontre les difficultés liées à la construction en piliers de l'Union européenne qui peut conduire à un choix de base juridique erroné[13]. Les limites du champ d'application de la directive 95/46/CE sont clairement établies dès lors que celle-ci est rattachée aux seules activités relevant du premier pilier. La solution retenue par la Cour dans l'arrêt P.N.R. diffère de sa jurisprudence

[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 [notifiée sous le numéro C(2004) 1914], Journal officiel n° L 235 du 06/07/2004 p. 0011 – 0022, paragraphe 15 : « *En ce qui concerne le principe de limitation à une finalité spécifique, les données à caractère personnel des passagers aériens contenues dans les PNR qui sont transférés au CBP doivent être traitées dans un but spécifique et n'être utilisées ou communiquées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité du transfert. En particulier, 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.* »

[12] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, Article 3 (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, - effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.* »

[13] BAZZOCCHI Valentina, « L'Accord entre l'Union européenne et les États Unis sur les données PNR », 13 octobre 2007, p. 2., disponible sur www.europeanrights.eu/index.php?funzione=S&op=5&id=45. Voir aussi l'arrêt de la C.J.C.E. du 10 décembre 2002, *British American Tobacco et Imperial Tobacco*, Affaire C-491/01, point 94, concernant la base juridique des actes communautaires poursuivant une double finalité ou ayant deux composantes.

antérieure en ce qu'elle réduit le champ d'application de la directive européenne. En effet, dans la jurisprudence Österreichischer Rundfunk[14], la Cour avait jugé que l'expression « *activités qui ne relèvent pas du champ d'application du droit communautaire*» ne devait pas être interprétée comme rendant nécessaire la vérification au cas par cas que l'activité en cause concerne directement la libre circulation entre les États membres[15]. Par la suite, la Cour a précisé dans son arrêt Lindqvist[16] que « *les activités mentionnées à titre d'exemple à l'article 3, paragraphe 2, premier tiret de la directive 95/46/CE (à savoir les activités prévues au Titre V et VI du T.U.E. ainsi que le traitement ayant pour objet la sécurité publique, la défense et les activités relatives à des domaines du droit pénal) sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers* ». Par conséquent, ces activités sont exclues du champ d'application de la directive.

Dans l'affaire P.N.R., la Commission estime que les activités des transporteurs aériens entrent dans le cadre du droit communautaire car ils traitent les données P.N.R. au sein de la Communauté et organisent leur transfert vers les États-Unis. Mais la Cour décide dans l'affaire P.N.R. que le fait que ces données aient été initialement recueillies dans le cadre d'une activité communautaire (vente d'un billet d'avion) importe peu. Selon la Cour, l'intérêt en l'espèce est de déterminer la finalité[17] pour laquelle ces données ont été recueillies. Dès lors, la détermination de cette finalité est considérée comme le seul élément à prendre en considération afin de savoir si cette activité est exclue ou non du champ d'application de la directive. Le fait qu'il s'agisse d'un acteur privé ou bien étatique qui est à l'origine de l'obtention de ces données n'est plus un critère pertinent. Aussi, l'opération de transfert de données vers une autorité publique à des fins policières ou judiciaires n'est pas couverte pas les garanties de la directive 95/46/CE. La solution retenue par la Cour de Justice signifie que la directive dans son ensemble n'est pas applicable et par conséquent, les compagnies aériennes peuvent transmettre les données P.N.R. Pour le Parlement européen, il s'agit donc d'une victoire « à la Pyrrhus »[18].

---

[14] C.J.C.E., 20 mai 2003, *Österreichischer Rundfunk*, Affaires jointes C-465/00, C-138/01 et C-139/01, point 42 : « *l'applicabilité de la directive 95/46 ne saurait dépendre de la question de savoir si les situations concrètes en cause dans les affaires au principal comportent un lien suffisant avec l'exercice des libertés fondamentales garanties par le traité et, en particulier dans lesdites affaires, avec la libre circulation des travailleurs. En effet, une interprétation contraire risquerait de rendre les limites du domaine d'application de ladite directive particulièrement incertaines et aléatoires, ce qui serait contraire à l'objectif essentiel de celle-ci, qui est de rapprocher les dispositions législatives, réglementaires et administratives des États membres afin d'éliminer les obstacles au fonctionnement du marché intérieur découlant précisément des disparités entre les législations nationales* ».

[15] DUMORTIER, Franck et POULLET, Yves, « La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union Européenne » *in Défis du droit à la protection de la vie privée*, Cahiers du Centre de Recherches Informatique et Droit, FUND-CRIDP, 2008, p. 453 [447-478]. Disponible sur http://works.bepress.com/franck_dumortier/2/ et sur http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/dumortier_poullet_/dumortier_poullet_fr.pdf.

[16] C.J.C.E., 6 novembre 2003, *Bodil Lindqvist*, Affaire C-101/01, point 43.

[17] C.J.C.E., Grande chambre, 30 mai 2006, *Parlement européen c. Conseil de l'Union européenne*, Affaires jointes C-317/04 et C-318/04, point 58.

[18] HIJMANS, Hielke, « *Le troisième pilier dans la pratique : composer avec les faiblesses. L'échange d'informations entre les États membres* », Avis préalable en vue de la réunion de l'Association néerlandaise pour le droit européen (NVER), 7 février 2007, p. 22. Disponible sur le site du Contrôleur européen des données personnelles : www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2007/07-02-07_preadvies_NVER_FR.pdf.

Il semble que la Cour de Justice ainsi que les institutions communautaires adoptent une approche sectorielle dont découle une protection inégale des données à caractère personnel dans la construction en piliers de l'Union. Le constat de ce vide juridique concernant la protection des données recueillies dans le cadre du troisième pilier, est effectué lors de la Conférence européenne sur la protection des données à Wroclaw, le 14 septembre 2004[19]. C'est dans ce contexte que la Commission a présenté une proposition de décision-cadre relative à la protection des données dans le cadre du troisième pilier[20] qui est destinée à s'appliquer aux fichiers traités dans le cadre de la coopération policière et judiciaire en matière pénale. Elle ne concerne pas le traitement des données de l'Office européen de police (Europol), ce qui semble être une lacune au regard de l'accord conclu entre Europol et les États-Unis en matière d'échange de données personnelles. L'article 15 de cette décision-cadre envisage le transfert de ces données personnelles vers des États tiers uniquement à la condition que ces derniers offrent une protection « adéquate ».

b. Le rôle de la Commission dans la conclusion de l'accord international

La décision du 14 mai 2004, portant accord sur le transfert des données P.N.R entre l'Union européenne et les États-Unis, revêt une importance particulière afin d'évaluer le niveau de considération de la protection des droits fondamentaux par la Commission européenne. Il est intéressant de noter que les préoccupations émises par le Groupe de travail de l'article 29 n'ont été que partiellement prises en considération en vue d'améliorer les garanties de protection de la vie privée des individus par le biais d'une protection accrue des données à caractère personnel. Selon le Groupe de travail de l'article 29, le système de transmission des données P.N.R. couvre des catégories très étendues des données personnelles et une telle transmission équivaut à la mise en place d'une surveillance généralisée des citoyens de l'Union européenne par un État tiers et constitue un outil visant à développer la construction de profils d'individus[21]. Bien qu'il n'existe pas de disposition conférant une compétence à la Communauté en matière de protection des données personnelles, la Commission a invoqué les articles 95 et 300 du T.C.E. pour conclure cet accord. Or, l'article 95 concerne l'établissement et le fonctionnement du marché intérieur et il n'a pas pour fonction de conférer une compétence externe à la Communauté pour négocier et signer des accords internationaux avec des pays tiers en matière de transfert de données personnelles[22]. La Commission européenne considère néanmoins que la Communauté dispose d'une compétence externe, en application de la

[19] Résolution de la Conférence européenne sur la protection des données visant à créer un forum conjoint de l'Union européenne sur la protection des données en matière de coopération policière et judiciaire.

[20] Proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale {SEC(2005) 1241} /* COM/2005/0475 final -CNS 2005/0202 *

[21] Avis 4/2003 sur le Niveau de Protection assuré aux États-Unis pour la Transmission des Données Passagers, Adopté le 13 juin 2003, 11070/03/FR, WP 78 ; Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis, Adopté le 24 octobre 2002, 11647/02/FR/Final, WP 66.

[22] Proposition de décision du Conseil concernant la conclusion d'un accord entre la Communauté européenne et les Etats-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, E2543 COM (2004) 190 final du 17/03/2004, Sénat français, procédure écrite du 7 mai 2004.

jurisprudence A.E.T.R.[23], étant donné que la directive de 1995 sur la protection des données personnelles a été adoptée sur le fondement de l'article 95 T.C.E. Pourtant, l'obligation faite aux compagnies aériennes de transmettre leurs données semble relever davantage de la compétence des États membres[24]. La Communauté a néanmoins décidé qu'elle disposait d'une compétence exclusive et qu'il n'était pas question d'une compétence partagée avec les États membres de sorte que l'hypothèse de la conclusion d'un accord mixte a été écartée. En effet, l'accord mixte aurait permis d'associer les parlements nationaux à la procédure de conclusion. Par ailleurs, si l'article 24 T.U.E. (accord international, politique étrangère et de sécurité commune, Titre V)[25] avait été mis en œuvre, les députés européens auraient pu peser sur ce débat dès lors que l'article 24 permet un débat et un vote du Parlement. La conclusion n'aurait pas pour autant été retardée car l'article 24 prévoit la possibilité d'une application provisoire de l'accord, conditionnée par les conclusions du Parlement.

2. Invalidité du fondement juridique de l'accord conclu par le Conseil

L'argumentation du Conseil devant la Cour de Justice des Communautés Européennes repose sur le respect de l'article 25 de la directive 95/46/CE. Le Conseil avance que l'accord contesté concerne la libre circulation des données P.N.R. entre la Communauté et les États-Unis dans des conditions respectant le droit à la vie privée et la protection des données à caractère personnel. L'action du Conseil est présentée de sorte qu'elle vise à éliminer les distorsions de concurrence entre les compagnies aériennes et concerne, par conséquent, le domaine du premier pilier impliquant la compétence des Communautés.

a. L'accord P.N.R. considéré hors du cadre du marché intérieur

En l'espèce, les négociations transatlantiques se caractérisent par le conflit juridique impliquant d'une part la mise en œuvre de nouveaux instruments de lutte contre le terrorisme et, d'autre part, la nécessaire protection des données personnelles en tant qu'élément essentiel au sein des sociétés démocratiques. Aussi, le développement des technologies de surveillance et de la constitution de bases de données gouvernementales alimentées par des sources commerciales et policières instaure une tension durable entre deux domaines poursuivant pourtant la même finalité. En effet, la lutte contre le terrorisme et la protection des données personnelles visent tous deux le renforcement de l'État de droit. Néanmoins, la spécificité du dossier P.N.R consiste en cette approche selon laquelle ces deux notions sont confrontées et placées en concurrence, et non pas envisagées de manière complémentaire. Mais cet affrontement ne trouve pas sa

[23] C.J.C.E., 31 mars 1971, *AETR*, Affaire 22-70.

[24] Rapport sur l'initiative du Royaume d'Espagne en vue de l'adoption d'une directive du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux personnes transportées (6620/2004 – C5-0111/2004 – 2003/0809(CNS)), 7 avril 2004 adopté par la commission des libertés et des droits des citoyens, de la justice et des affaires intérieures du Parlement européen.

[25] de KERCHOVE, Gilles et WEYEMBERGH, Anne, *Sécurité et justice : enjeu de la politique extérieure de l'Union européenne*, Bruxelles, Institut d'Études Européennes, Éditions de l'Université de Bruxelles, 2003, p. 180.

seule source dans le cadre des relations transatlantiques. Bien au contraire, cette tension préexiste au sein de l'Union européenne et est illustrée par sa structure en piliers. En effet, le Groupe de l'article 29 note que : « *Les mesures proposées par le Conseil, les États membres et la Commission sont des activités qui relèvent à la fois du troisième et du premier pilier. Le Parlement européen, le Conseil et la Commission sont en désaccord sur la base juridique et, par conséquent, sur la procédure à suivre. Le Groupe de travail fait officiellement partie du premier pilier et il n'existe pas d'organisme équivalent pour conseiller le troisième pilier. Il existe un risque considérable que les implications de la protection des données ne soient pas pleinement prises en compte* »[26].

L'argumentation du Conseil devant la C.J.C.E. vise à justifier la décision 2004/496 prise sur le fondement de l'article 95 T.C.E. Le Parlement conteste la finalité de l'accord alléguée par le Conseil et qui consiste en l'établissement et au fonctionnement du marché intérieur. Selon le Parlement, la décision du Conseil a pour objectif de légaliser le traitement de données à caractère personnel imposé par la législation américaine aux compagnies aériennes européennes, sans pour autant préciser dans quelle mesure cette légalisation des transferts des données vers un pays tiers contribuerait à l'établissement ou au fonctionnement du marché intérieur. Par ailleurs, cette décision établirait le droit d'accès du C.B.P. au système des réservations des compagnies européennes. Or, la réalisation de ces buts ne tombe pas sous le coup de l'article 95 T.C.E. Cette approche du Conseil est symptomatique des dissensions existantes au sein des institutions communautaires : tandis que le Parlement envisage l'affaire P.N.R. sous l'angle de la protection des droits fondamentaux conformément à la nature de son mandat, la Conseil privilégie l'approche économique, prenant ainsi en compte les difficultés financières affrontées par les transporteurs aériens européens. Cette démarche semble à première vue cohérente compte tenu du mandat respectif du Parlement et du Conseil mais il en résulte un phénomène de « marginalisation » de la problématique liée à la protection des données personnelles. Le Conseil vise en l'espèce l'élimination des distorsions de concurrence entre les compagnies aériennes des États membres et des États tiers qui résultent du conflit juridique opposant la législation antiterroriste américaine et celle relative à la protection des données personnelles au sein de l'Union européenne. En effet, les compagnies aériennes des États membres effectuant des vols internationaux au départ ou à destination des États-Unis étaient soumises à un régime différent selon qu'elles se conformaient ou non aux exigences de l'administration américaine. Le Conseil fonde sa décision concernant l'ouverture des négociations transatlantiques sur l'article 25 de la directive 95/46/CE[27] car il considère que les conditions de concurrence « *auraient pu être faussées en raison du fait*

[26] de BIOLLEY, Serge, « *Collecte, échange et protection des données dans la coopération en matière pénale* », *Journal de droit européen*, septembre 2006, p. 195.

[27] Article 25, « Principes » : « *4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe2 du présent article, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause.5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes. Les États membres prennent les mesures nécessaires pour se*

que seulement certaines d'entre elles auraient accordé aux États-Unis un accès à leurs bases de données.»[28]

Le 30 mai 2006, la Cour a annulé la décision du Conseil. La concision du raisonnement de la C.J.C.E. révèle l'absence de positionnement quant à la question de la protection des droits fondamentaux. La Cour s'est bornée à une application à la lettre des dispositions de l'article 3, paragraphe 2 de la directive 95/46/CE[29] et, considérant que les données P.N.R. sont exclues du champ d'application de la directive, la décision du Conseil n'a pu être valablement adoptée sur le fondement de l'article 95 T.C.E. Selon la Cour, le choix du fondement juridique revêt une importance de nature constitutionnelle ; un fondement inadéquat invalide l'acte de conclusion[30] Ce faisant, la C.J.C.E. n'a pas jugé opportun d'examiner les autres moyens avancés par le Parlement tels que la violation inter alia de l'article 300, paragraphe 3, deuxième alinéa T.C.E., de l'article 8 de la C.E.D.H., du principe de proportionnalité, de l'exigence de motivation et du principe de coopération loyale. La Cour a par conséquent considéré que la conclusion de l'accord relève de la compétence de l'Union européenne et non pas des Communautés, plaçant désormais l'accord P.N.R. dans le cadre du troisième pilier. Le Conseil a dû dénoncer l'accord mais, afin d'éviter un vide juridique, la Cour a permis le maintien de cet accord jusqu'au 30 septembre 2006.

b. L'article 8 de la C.E.D.H. écarté de l'appréciation de la Cour

α - Les conclusions de l'Avocat général : l'absence de violation du droit au respect de la vie privée

Dans le contexte de lutte contre le terrorisme, le contrôle juridictionnel ne peut s'exercer dans sa plénitude pour apprécier la légalité des actes et doit se limiter à la vérification d'une éventuelle erreur manifeste d'appréciation de la part du Conseil et de la Commission. Ceci pour éviter que la Cour ne substitue sa propre appréciation à celle des autorités politiques communautaires en matière de lutte contre le terrorisme. Concernant la violation de l'article 8 de la C.E.D.H., l'Avocat général considère que l'existence d'une ingérence dans la vie privée des passagers est indéniable[31]. En vertu de l'article 8 de la C.E.DH., cette ingérence est tolérée si elle respecte les trois conditions suivantes : l'ingérence est prévue par la loi, elle poursuit un but légitime et, enfin, elle est nécessaire dans une société démocratique. Il s'agit

conformer à la décision de la Commission ».

[28] C.J.C.E., Grande chambre, 30 mai 2006, *Parlement européen c. Conseil de l'Union européenne*, Affaires jointes C-317/04 et C-318/04, point 64.

[29] « *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, […]*»

[30] Avis 2/00, du 6 décembre 2001, rendu en vertu de l'article 300, paragraphe 6, CE, Rec. p. I-9713, point 5 et C.J.C.E., 9 novembre 1995, *Allemagne c. Conseil*, Affaire C-426/93, point 33.

[31] Conclusions de l'Avocat général M. Philippe LÉGER présentées le 22 novembre 2005, p. 34.

d'envisager en premier lieu si cette ingérence est prévue par la loi. Comme le rappelle l'Avocat général, cette condition implique non seulement une base légale mais aussi la qualité de la loi[32] qui signifie que la loi doit être accessible, prévisible et précise[33]. En conséquence, l'Avocat général considère que la déclaration d'engagement américaine est suffisamment précise et que la décision d'adéquation de la Commission renvoi dans son préambule aux législations américaines pertinentes. En deuxième lieu, l'Avocat général considère que la lutte contre les crimes graves autres que le terrorisme[34] constitue un objectif légitime en vertu de l'article 8 de la C.E.D.H. En troisième lieu, l'Avocat général envisage si cette ingérence est nécessaire dans une société démocratique. Il rappelle la jurisprudence de la Cour de Strasbourg qui considère que le terme « nécessaire » implique « qu'un besoin impérieux » soit en cause et que la mesure prise soit « proportionnée au but légitime poursuivi »[35]. En l'espèce, l'Avocat général s'attache à examiner si le Conseil et la Commission ont respecté leur marge d'appréciation en décidant des éléments constitutifs du régime P.N.R. et si cela respecte le droit à la vie privée et la protection des données personnelles. Dès lors, il constate que la déclaration d'engagement américaine est pourvue d'un effet obligatoire et que son non-respect entraînerait l'annulation ou la suspension de la décision d'adéquation. Du point de vue du respect du principe de proportionnalité, l'existence d'une liste de trente-quatre rubriques de données constitue une mesure appropriée eu égard à l'objectif de lutte contre le terrorisme qui suppose l'obtention de nombreuses informations afin de constituer des profils d'individus. Concernant l'accès aux données sensibles[36], l'Avocat général souligne que le C.B.P. ne bénéficie que d'un accès limité à ces données[37] et qu'il n'est pas habilité à les utiliser[38]. Quant à la durée normale de stockage des données P.N.R., celle-ci est de trois ans et six mois, durée qui n'est donc pas considérée comme excessive par l'Avocat général au vue de la durée des enquêtes en matière de terrorisme et considérant l'utilité de ce stockage à des fins de prévention et de répression du terrorisme. Quant à l'absence de contrôle juridictionnel, et en dépit de l'exception mentionnée à l'engagement 38 de la déclaration américaine, le F.O.I.A. prévoit que tout demandeur peut contester, par un recours administratif ou judiciaire, la décision du C.B.P. de ne pas communiquer ces informations[39].

---

[32] C.E.D.H., 24 avril 1990, *Kruslin c. France*, § 27.

[33] C.E.D.H., Plénière, 24 mars 1988, *Olsson c. Suède (n° 1)*, 24 mars 1988, §§ 61 et 62.

[34] Le préambule de l'accord P.N.R. évoque la prévention et le combat contre le terrorisme « *et les délits qui y sont liés, ainsi que d'autres délits graves de nature transnationale, notamment la criminalité organisée* ». Le paragraphe 3 de la déclaration d'engagement dispose que « *[l]e CBP utilise les données de PNR dans le but unique de prévenir et de combattre: 1) le terrorisme et les crimes liés au terrorisme; 2) d'autres crimes graves, y compris la criminalité organisée, qui, par nature, revêtent un caractère transnational, et 3) la fuite en cas de mandat d'arrêt ou de mise en détention pour l'un des crimes susmentionnés.* »

[35] C.E.D.H., 24 novembre 1986, *Gillow c. Royaume-Un*i, § 55 cité dans les Conclusions de l'Avocat général M. Philippe Léger présentées le 22 novembre 2005, p. 56.

[36] Rubriques n°19 « Observations générales »; 26 « Données OSI [‘*Other Service Information’*] », et 27 « Données SSI/SSR [‘*Special Service Request’*]», Décision 2004/535/CE de la Commission du 14 mai 2004, Annexe «A», « Rubriques des PNR demandées par le CBP aux compagnies aériennes », Journal officiel n° L 235 du 6 juillet 2004, pp. 11-22.

[37] Engagement 5.

[38] Engagements 9 à 11.

[39] L'engagement 38 renvoie au titre 5, section 552(a)(4)(B) du code des États-Unis et au titre 19, section 103.7-103.9 du Code des règlements fédéraux.

En dernier lieu, et concernant le transfert des données P.N.R. par le C.B.P. à d'autres autorités publiques nationales ou étrangères, l'Avocat général précise que ce pouvoir accordé au C.B.P. est encadré[40] et qu'il ne s'effectue qu'au cas par cas, avec l'accord préalable du C.B.P. En ces termes, le C.B.P. est considéré comme propriétaire des données du dossier passager[41] au sens des principes du *Safe Harbor* et par conséquent, diverses obligations lui incombent afin de s'assurer de l'adéquation des mécanismes de protection des données offerte par ces autorités. Ce faisant, l'Avocat général conclu que les moyens tirés de la violation du droit à la protection des données personnelles et de la violation du principe de proportionnalité ne sont pas fondés.

β - L'intervention du C.E.P.D. devant la Cour de Luxembourg

Considérant la nature de l'affaire portée devant la C.J.C.E., le Contrôleur européen de la protection des données (C.E.P.D.) est intervenu[42] pour la première fois devant la Cour et ce, à titre d'*amicus curiae*. La compétence d'intervention du C.E.P.D. devant la Cour est en effet fondée lorsque l'affaire relève du domaine de la protection des données. Dans ses ordonnances du 17 mars 2005 relatives aux affaires concernant les données des dossiers passagers (P.N.R.)[43], la Cour de Justice a considéré que ce droit s'étendait à toutes les questions communautaires concernant le traitement des données à caractère personnel. Le C.E.P.D., Peter Hustinx, a immédiatement réagit à ce jugement rendu dans l'affaire P.N.R.[44] en soulignant que la Cour n'a pas statué sur le contenu des décisions du Conseil et de la Commission mais seulement sur la procédure utilisée. Bien plus, le Contrôleur note que l'arrêt de la Cour, en excluant du champ d'application de la directive 95/46/CE les cas où les données sont utilisées par la justice, marque une régression de la protection des droits : « *Le jugement semble avoir affaibli la protection des données des citoyens européens dans le cas où leurs données sont utilisées pour des finalités liées aux services répressifs. Ce qui rend d'autant plus important qu'un instrument juridique exhaustif et cohérent sur la protection des données personnelles en dehors du premier pilier soit adopté sans délai* »[45]. Dans cette interprétation, la collecte de données personnelles pour des raisons commerciales doit respecter les règles énoncées par la directive 95/46/CE. Mais si elles sont utilisées par exemple, dans le cadre de la lutte contre le terrorisme, les gardes fous de la directive européenne ne s'appliquent plus. La plaidoirie[46] présentée par le représentant du C.E.P.D. met en lumière les problématiques principales caractérisant l'accord P.N.R. Il

[40] Engagements 29 et 30.

[41] Engagement 31.

[42] Ce droit d'intervention est fondé sur l'article 47 du règlement 45/2001.

[43] C.J.C.E, Grande Chambre, Ordonnance, 17 mars 2005, « Intervention », Affaire C-317/04 et C.J.C.E., Grande Chambre, Ordonnance de la Cour, 17 mars 2005, « Intervention », Affaire C-318/04.

[44] « *PNR: première réaction du CEPD au jugement de la Cour de justice* », communiqué de presse EDPS/06/8, 30 mai 2006. Disponible sur http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/06/8&format=HTML&aged=1&language=FR&guiLanguage=en.

[45] *Ibid*.

[46] Audience de la Cour dans les affaires C-317/04 et C-318/04 (18 octobre 2005), Plaidoirie du C.E.P.D, document présenté par Hielke Hijmans, Agent du Contrôleur européen de la protection des données.

est à noter que certaines réflexions du C.E.P.D. semblent en contradiction avec celles du Groupe de travail 29[47]. A titre d'exemple, postérieurement au jugement rendu par la Cour, tandis que le C.E.P.D. semble conclure à la nécessité d'adopter un instrument spécifique dans le cadre du troisième pilier, le Groupe de l'article 29 estime que « *l'arrêt de la Cour montre une fois de plus les difficultés dues à la division artificielle entre les piliers et la nécessité d'un cadre transpiliers cohérent en matière de protection des données* »[48].

En premier lieu, la plaidoirie met en exergue l'effet dérogatoire que comporte l'accord P.N.R. bien que l'article 8 de l'accord souligne que ce dernier n'a pas pour objet de déroger à la législation des parties. A ce propos, le C.E.P.D. mentionne l'article 32 de la Convention de Vienne sur le droit des traités de 1969 selon lequel on ne peut interpréter les dispositions d'un traité de manière littérale. Qui plus est, l'accord précise en son article 2 l'obligation de respecter la législation américaine pertinente mais n'établi pas une obligation similaire quant au respect des dispositions de la directive 95/46/CE. Le C.E.P.D. affirme le caractère non contraignant des engagements du C.B.P.[49] dans la mesure où la déclaration d'engagement n'est pas annexée à l'accord avec les États-Unis mais à la décision de la Commission. Ce caractère non contraignant est clairement affirmé par l'engagement 47 qui dispose : « *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* »[50]. Le C.E.P.D. avance l'argument selon lequel le U.S. Customs n'est vraisemblablement pas le seul responsable du traitement des données P.N.R. si l'on prend en considération l'utilisation du système « *pull* ». Les compagnies aériennes sont co-responsables du traitement des données obtenues par le C.B.P. et cette pratique contrevient aux dispositions de l'article 4 (2) de la directive 95/46/CE[51]. Enfin, concernant la protection des droits fondamentaux, le C.E.P.D. considère qu'il y a ingérence dans la vie privée des individus et que le transfert des données sensibles n'est pas une mesure acceptable dès lors que le filtrage de ces données n'est pas garanti en permanence et que les mécanismes de contrôle sont inexistants. Aussi, des agences telles que le F.B.I. ont alors accès à ces données alors qu'elles n'ont pas signé la déclaration d'engagement. Enfin, l'absence de recours judiciaire garanti par les engagements américains[52] représente une lacune subsidiaire de l'accord P.N.R.

---

[47] DUMORTIER, Franck et POULLET, Yves, « La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union Européenne », *loc. cit.*, p. 448.

[48] Avis 5/2006 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, Adopté le 14 juin 2006, WP 129, p. 3.

[49] Déclaration d'engagement du Bureau des douanes et de la protection des frontières du Ministère de la sécurité intérieure

[50] *Ibid.*

[51] Article 4, « *Droit national applicable: 1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque: (...) (c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté. 2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.* »

[52] Engagement 42.

B. La position du Parlement européen quant à l'accord P.N.R.

En l'espèce, l'accord originel a été rattaché au premier pilier; contrairement aux États-Unis qui considèrent leur législation comme une mesure antiterroriste, l'Union a considéré la requête américaine comme relative au marché intérieur. Compte tenu du jugement rendu par la C.J.C.E., l'accord P.N.R. relève du troisième pilier ce qui signifie que les décisions concernant cet accord ne sont pas communautaires. Le rôle du législateur est alors strictement attribué au Conseil, et le Parlement, s'il se voit attribuer un rôle simplement consultatif, s'assure néanmoins que l'Union européenne respecte les droits fondamentaux par l'entremise de ses actes, qu'ils relèvent du domaine communautaire ou non. Dans sa résolution de 2004[53], le Parlement souligne que l'accès demandé par le C.B.P. aux données P.N.R. en vertu du *Aviation Transportation Security Act* requiert un cadre juridique précis aux termes du droit national et du droit européen sur la vie privée. Le constat effectué est qu'il n'existe aucune base juridique dans l'Union européenne pour utiliser des données commerciales à des fins de sécurité publiques et, par conséquent, cette base juridique est indispensable pour modifier le but dans lequel les données ont été collectées.

1. La question procédurale : la codécision et la procédure de l'avis conforme écartées

L'affaire P.N.R. met en exergue le rôle prédominant que s'est octroyé la Commission européenne afin de négocier un accord international avec les États-Unis. Cet activisme de la Commission en matière de sûreté du transport aérien est notable dans la mesure où, si l'Union européenne a pu acquérir un rôle de premier plan dans le domaine de l'aviation civile, elle a été longuement absente en matière de sûreté. L'accord P.N.R. de 2004 témoigne de ce nouveau leadership dont fait preuve la Commission afin de conclure un accord juridique avec un État tiers.

a. Le Parlement relégué à un rôle consultatif

Le choix du premier pilier comme base juridique de l'accord P.N.R. originel revêt une importance particulière d'un point de vue juridique. Ce choix du premier pilier est la traduction légale de la reconnaissance du caractère adéquat des normes américaines concernant le protection des données et donc, de la légalité du transfert des données P.N.R. entre les États-Unis et l'Union européenne. La légalité du transfert de ces données a été analysée sur le fondement de la directive 95/46/CE dont les dispositions s'appliquent aux matières relevant du premier pilier. Par conséquent, en vertu de l'article 25 de la directive, l'évaluation de la légalité de ce transfert n'est pas effectuée sous la procédure de codécision, qui

[53] Résolution du Parlement européen su le projet de décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel contenues dans le dossier des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (2004/2011(INI), P5_TA_PROV-(2004)0245.

est la procédure ordinaire de l'Union européenne. L'absence de procédure de codécision emporte des conséquences quant à la légitimité démocratique de l'accord. En effet, la codécision visée à l'article 251 du T.C.E. donne le pouvoir au Parlement européen d'arrêter des actes conjointement avec le Conseil de l'Union européenne. Cette procédure a pour effet de multiplier les contacts inter-institutionnels et renforce le pouvoir législatif du Parlement européen. Pourtant, l'évaluation de la légalité du transfert des données P.N.R. a été effectuée par comitologie selon l'article 202 du T.C.E. Si la décision du Conseil « comitologie » garanti un droit de regard au Parlement, la procédure de comitologie demeure moins transparente que celle de la codécision et réduit substantiellement le rôle du Parlement européen et des parlements nationaux.

Le 21 avril 2004, le Parlement européen a saisit la C.J.C.E. afin qu'elle se prononce sur la légalité de la décision d'adéquation et de l'accord international. Par acte séparé déposé au greffe de la Cour le même jour, le Parlement a, en vertu de l'article 62 bis du règlement de procédure de la Cour, demandé à cette dernière de soumettre le recours à une procédure accélérée. Effectivement, le Parlement avance l'argument selon lequel la décision du Conseil et de la Commission constituent « *une violation des droits fondamentaux, notamment du droit à la vie privée et à la protection des données à caractère personnel, d'un nombre très important de personnes physiques, étant donné la densité du trafic aérien de passagers entre l'Union européenne et les États-Unis d'Amérique* »[54]. Par ordonnances en date du 21 septembre 2004, la Cour a rejeté la demande de procédure accélérée concernant les deux affaires jointes en vertu de trois motifs. En premier lieu, la Cour considère que le nombre de personnes qui seraient potentiellement affectées par la mise en œuvre de l'accord ne constitue pas une circonstance exceptionnelle[55]. De même, la clarification du cadre juridique applicable et la détermination de la portée de la déclaration américaine d'engagement ne constituent pas une circonstance exceptionnelle. En deuxième lieu, l'argument de l'expiration imminente du délai fixé à l'article 6 de la décision d'adéquation rendue par la Commission le 14 mai 2004 est inopérant. En effet, l'application de la procédure accélérée n'aurait aucun effet dès lors que le jugement de la Cour serait dans tous les cas prononcé après expiration de ce même délai. Précision importante apportée par la C.J.C.E. : le Parlement européen aurait dû demander un sursis à exécution de la décision du Conseil et de la décision 2004/535 de la Commission afin de limiter les effets juridiques de l'accord sur les individus. Enfin, l'argument selon lequel le transfert des données P.N.R. emporterait des conséquences graves échappant à la Communauté est rejeté car la procédure accélérée n'empêcherait pas que les individus soient affectés par les conséquences découlant de l'exécution de l'accord.

b. Procédure de consultation non suspensive selon la Commission

[54] Ordonnance du Président de la Cour, 21 septembre 2004, « Procédure accélérée », Affaire C-317/04 et Ordonnance du Président de la Cour, 21 septembre 2004, « Procédure accélérée », Affaire C-318/04.

[55] Concernant cet argument, la Cour se fonde sur l'ordonnance du Président du 10 février 2004 rendue dans l'affaire *Parlement c. Conseil*, point 10.

Concernant l'accord P.N.R. originel et le rôle du Parlement quant à son adoption, la procédure de l'avis simple (procédure de consultation) a été mise ne œuvre plutôt que la procédure de l'avis conforme. Le choix de cette procédure déroge à la procédure de droit commun qui demeure la procédure de l'avis conforme pour la conclusion d'un accord fondamental avec un pays tiers. En vertu de l'article 192 T.C.E., la procédure de l'avis conforme implique que le Conseil doit obtenir l'assentiment du Parlement européen pour prendre les décisions considérées d'importance majeure pour l'Union européenne[56]. Cette procédure revêt un caractère contraignant car le défaut d'avis conforme interdit l'adoption de l'acte. A l'inverse, la procédure de l'avis simple utilisée en l'espèce permet seulement au Parlement d'émettre un avis concernant une proposition de la Commission. Néanmoins, le Conseil n'est pas lié par ces recommandations mais seulement par l'obligation de le consulter ; le seul principe applicable en l'espèce est le principe de coopération loyale entre les institutions[57]. Ce faisant, peu après la saisine de la C.J.C.E., le Parlement a fait savoir qu'il attendrait le jugement de la Cour avant de transmettre son avis sur l'accord au Conseil, suivant la procédure de consultation de l'article 300, paragraphe 6 T.C.E. Le 28 avril 2004, le Conseil a enjoint le Parlement à appliquer la procédure d'urgence, imposant ainsi le délai du 5 mai 2004 afin de transmettre l'avis parlementaire[58] mais le Parlement a rejeté l'application de cette procédure par 343 voix contre 301[59]. Le Conseil a néanmoins décidé de procéder à la conclusion de l'accord international sans l'avis du Parlement, arguant la nécessité urgente de remédier à la situation d'incertitude subie par les passagers et les compagnies aériennes. En ces termes, la Commission européenne a considéré que la consultation du Parlement ainsi que de la Cour n'était pas suspensive[60]. Cette perception de l'état d'urgence semble caractériser les mesures adoptées par l'Union européenne post 11 septembre, et est utilisée comme justification afin d'accélérer l'adoption de législations qui revêtent pourtant une importance considérable pour le justiciable.

Dans cette affaire, le Parlement allègue la violation de l'article 300, paragraphe 3, deuxième alinéa T.C.E. en ce que l'accord transatlantique constituerait une modification de la directive 95/46/CE A ce propos, l'Avocat général M. Philippe Léger rappelle qu'en matière de conclusion d'accords internationaux par la Communauté, la consultation du Parlement est la procédure de droit commun. Par dérogation, l'article 300, paragraphe 3, deuxième alinéa T.C.E. impose l'avis conforme du Parlement dans quatre cas, notamment lorsqu'un accord implique « *une modification d'un acte adopté selon la procédure visée à*

[56] Europa Glossaire, « Procédure de l'avis conforme ».

[57] Principe résultant notamment de l'article 218 instituant la Communauté européenne

[58] Lettre de Lord Filkin à Lord Grenfell du 27 avril 2004, citée dans MITSILEGAS, Valsamis, « Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme », *Cultures & Conflits*, n° 60, hiver 2005, § 16 [pp. 185-197] ; disponible à http://www.conflits.org/index1829.html.

[59] CNIL, *PNR : la chronologie du dossier et les textes de référence.* Disponible à www.cnil.fr/index.php?id=1018 et désormais sur le site de l'Agence andorrane de protection des données (APDA) à l'adresse suivante https://www.apda.ad/system/files/5-CNIL+-+PNR-+CRONOLOGIA.pdf.

[60] Projet d'accord entre la Communauté européenne et les États-Unis sur le traitement et le transfert des données des dossiers passagers, Sénat français, Justice et affaires intérieures, E2543 -COM (2004) 190 final du 17/03/2004, Procédure écrite du 7 mai 2004. Disponible à http://www.senat.fr/ue/pac/E2543.html.

l'article 251 ». L'intérêt est donc de déterminer si l'accord transatlantique a pour effet de modifier la directive susmentionnée. L'Avocat général souligne que, pour qu'il y ait modification, « *l'une des conditions est que le champ d'application de l'accord recoupe celui couvert par l'acte interne* »[61]. Dès lors, l'Avocat général considère que l'accord n'a pu modifier le contenu de la directive et n'impliquait donc pas la mise en œuvre de la procédure de l'avis conforme. Tout d'abord, l'Avocat général précise que l'accord et la directive poursuivent des finalités distinctes : si l'accord vise la lutte contre le terrorisme et autres crimes graves reliés, la directive tend à assurer la libre circulation des données personnelles entre les États membres. De cet état de fait, l'Avocat général en déduit que ces deux instruments ont des champs d'application différents. L'accord s'applique au traitement de données personnelles tendant au renforcement de la sécurité intérieure des États-Unis tandis que la directive exclue de son champ d'application les mesures ayant pour objet la sécurité publique, la défense nationale ou encore la sûreté de l'État. *De facto*, l'accord n'emporte aucune modification de la directive 95/46/CE et n'implique donc pas la mise en œuvre de la procédure de l'avis conforme.

2. La question de fond : la violation des droits fondamentaux

A propos de la conclusion de l'accord P.N.R., le Parlement européen soulignait que « *dans le cas des États-Unis, même après de longues négociations avec la Commission et en dépit de la bonne volonté manifestée dans les "déclarations d'engagement", il n'existe toujours pas de protection juridique des données dans le domaine du transport aérien; par conséquent, il est possible d'avoir accès à toutes les données P.N.R., à la seule exception des données "sensibles", et les données peuvent être conservées pendant plusieurs années après que le contrôle de sécurité a été effectué; en outre, il n'existe pas de protection judiciaire pour les non ressortissants des États-Unis* »[62]. C'est en ces termes que le Parlement allègue la violation des droits fondamentaux.

a. Droit à la vie privée, protection des données et droit de recours

L'un des principaux arguments du Parlement afin de contester l'action unilatérale de la Commission européenne est la violation des droits fondamentaux, considérant les dispositions de l'article 6 du Traité instituant l'Union européenne, l'article 8 de la Convention européenne des droits de l'homme (C.E.D.H.) et la directive 95/46/CE sur la protection des données personnelles. Afin d'appuyer ses allégations, le Parlement constate tout d'abord l'absence de base juridique dans l'Union européenne pour utiliser des données commerciales à des fins de sécurité publique. Une telle base est donc nécessaire et doit définir les données exactes à collecter, les règles concernant leur traitement et les responsabilités de chaque partie prenante. Dès lors, le Parlement rappelle que le protection de la vie privée aux États-Unis ne constitue pas

[61] Conclusions de l'Avocat général M. Philippe LÉGER présentées le 22 novembre 2005, paragraphe 183, p. 29.

[62] Cf. recommandation à l'intention du Conseil en date du 7 septembre 2006.

un droit fondamental mais est réglementée par des dispositions spécifiques qui ne bénéficient pas aux citoyens non américains : les citoyens de l'Union européenne sont ainsi dépourvus de leur droit au juge en cas d'abus dans les mesures restreignant leur liberté de voyager. Le Parlement européen conteste plus particulièrement plusieurs dispositions de l'accord P.N.R originel et de l'accord de 2007. Entre autre, le Parlement met en exergue le fait que la décision d'adéquation de la Commission s'appuie sur les engagements américains dont le caractère contraignant demeure incertain. En premier lieu, cette incertitude se fonde sur la source même de ces engagements qui est de nature administrative et donc sujette aux réorganisations internes du Ministère de la sécurité intérieure. En second lieu, il est question de l'absence de bases juridiques américaines afin de garantir la mise en œuvre de ces engagements. A titre d'exemple, aucune législation ne garantie le droit de recours d'un citoyen européen afin de contester devant une Cour américaine une utilisation abusive de ses donnés personnelles[63].

Par ailleurs, le Parlement conteste que les autorités américaines puissent accéder directement aux données provenant des systèmes de contrôle des réservations et des départs des transporteurs aériens situés sur le territoire de l'Union européenne via le programme d'extraction « *pull* »[64]. Ce programme autorise un accès direct des autorités américaines de façon temporaire, le temps que les compagnies aériennes se dotent des moyens techniques leur permettant de transmettre les informations elles-mêmes par le biais du programme « *push* ». Selon le Parlement, le système « *pull* », très invasif, est utilisé sans base légale par l'administration américaine et ne contient pas de filtrage concernant l'obtention des données sensibles. L'accord doit s'attacher à définir les données qui pourraient être transférées d'une manière automatisée (A.P.I.) et celles qui pourraient être transférées au cas par cas afin de respecter le principe de proportionnalité. Le Parlement considère *de facto* qu'il y a ingérence dans la vie privée des individus et que les conditions qui pourraient la justifier légalement, ne sont pas remplies[65]. Les personnes concernées par cet accord, autrement dit tout passager aérien voyageant à destination des États-Unis, ne pourront connaître avec exactitude les obligations qui en résultent puisque l'accord renvoie à la loi américaine à laquelle il est plus difficile d'avoir accès. Aussi, le Parlement considère que la lutte contre le terrorisme constitue un but légitime mais la condition de nécessité dans une société démocratique n'est pas respectée. Notamment, l'accord originel prévoit le transfert d'un nombre excessif de données (34 données), affirmation qui demeure applicable à l'accord en date de 2007 considérant que la réduction des données

[63] 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 du dossier passager (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007) - Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données du dossier passager (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), Journal Officiel N° L 204 du 04 août 2007, pp. 16-25, p. 9 ; Lettre du Ministère américain de la Sécurité intérieure (DHS) des États-Unis d'Amérique à l'attention de la présidence du Conseil et de la Commission, relative à l'interprétation d'un certain nombre de dispositions de la déclaration d'engagement, diffusée par le DHS le 11 mai 2004, sur le transfert des donnés contenues dans les dossiers des passagers (données PNR) par des transporteurs aériens, Journal officiel de l'Union européenne n° C 259/1 du 27 octobre 2006.

[64] Résolution du Parlement européen sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions, P6_TA (2007)0039, 14 février 2007.

[65] Cf. Article 8 de la Convention E.D.H.

transférables au nombre de dix-neuf ne constitue qu'une réduction en trompe l'œil. Enfin, la durée de conservation des données est excessive et le contrôle juridictionnel concernant le traitement des données par les autorités américaines n'est pas garanti tandis que le transfert des données à d'autres autorités publiques est rendu possible. Ce faisant, la Commission des libertés civiles, de la justice et des affaires intérieures (Commission L.I.B.E. du Parlement) a présenté le 1 juin 2006 un plan en trois points pour la conclusion d'un nouvel accord avec les États-Unis. Ce document recommande d'une part, d'ouvrir un débat avec le Conseil et la Commission sur les différentes bases juridiques qui pourraient fonder le nouvel accord, et, d'autre part, d'associer les parlements nationaux au débat sur les normes de protection des données et d'énoncer des règles européennes claires de protection des données dans le domaine de la sécurité publique, qui n'est pas couvert par la directive 95/46/CE.

b. La « désolidarisation » des États membres

Le 26 février 2008, la République Tchèque a signé un protocole d'entente avec les États-Unis sur l'échange de données concernant les passagers des vols transatlantiques. Faut-il considérer cette « désolidarisation » de la République Tchèque comme une conséquence de la négociation à huis clos des institutions de l'Union européenne de l'accord P.N.R. ? En effet, les États membres de l'Union européenne n'ont que peu participé aux négociations de l'accord P.N.R., si ce n'est au travers de l'acceptation de la décision d'adéquation de la Commission le 27 février 2004[66]. Mais concernant l'accord P.N.R. 2007, les États membres n'ont été consultés qu'*a posteriori*[67]. En effet, le Parlement européen affirme dès 2004 que l'accord transatlantique dépossède les États membres, qui étaient auparavant responsables d'assurer la protection des personnes à l'égard des données P.N.R., de toute possibilité de bloquer les transferts pour garantir les droits de leurs citoyens[68]. La « désolidarisation » des États membres était déjà illustrée en 2006 lorsque le président hongrois Laszlo Solyom a décidé de ne pas signer la loi nationale promulguant l'accord transatlantique et l'avait renvoyé à l'appréciation du Parlement national. L'objectif était alors d'intégrer une disposition nécessitant l'approbation expresse de l'individu concerné par la divulgation des données P.N.R. A ce propos, le Directeur du Programme de la protection des données de la section hongroise de l'Association américaine de protection des libertés publiques (A.C.L.U.) a déclaré : « *Even if the Hungarian law on promulgating the PNR agreement includes provisions on asking for the passengers' consent for handling their personal data, it won't be very useful. How can anybody regard the consent as freely given when the passengers are not allowed to board or disembark the airplane without providing them. Although the President's veto is not futile: the current agreement shall expire no later than 31 July*

[66] Acceptation dans le cadre de la procédure prévue à l'article 31 de la directive 95/46.

[67] *Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) – Declarations made in accordance with Article 24(5) TEU - State of Play, Council of the European Union*, Brussels, 16 July 2008, 11163/1/08 REV 1.

[68] Résolution du Parlement européen su le projet de décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel contenues dans le dossier des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (2004/2011(INI), P5_TA_PROV-(2004)0245.

2007. His veto should be a benchmark for the Hungarian Government in the renegotiations. »[69] Il semble intéressant de constater que l'administration américaine a pu apaiser cette opposition en proposant que la Hongrie bénéficie du *Visa Waiver Program*, ce qui permettrait aux citoyens hongrois de pénétrer le territoire américain sans avoir a effectuer de démarches en vue de l'obtention d'un visa. La signature du Memorandum par la République Tchèque vient renforcer cette idée de « désolidarisation » et de rupture de l'unité au sein de l'U.E. mais aussi, ce type d'accord bilatéral affecte la protection des données à caractère personnel. Cela pourrait signifier que les nouveaux pays membres de l'Union seraient ainsi libres de négocier des accords bilatéraux pour obtenir des exemptions de visa avec les États-Unis. En contrepartie Prague a accepté un transfert d'informations qui va au-delà de ce que l'Union européenne a accepté par le biais de l'accord P.N.R. 2007. Le contenu de ce Memorandum[70] implique notamment la transmission d'informations sur les passagers qui ne font que survoler le territoire américain et sur les personnes qui accompagnent des mineurs ou des malades sans pour autant embarquer. La problématique réside en ce que la République Tchèque, contre la perspective d'une dérogation pour les visas, accepte les nouvelles demandes américaines sans obtenir aucune garantie supplémentaire. A ce propos, le texte du protocole d'entente précise que « *les participants s'accordent pour collecter, analyser, utiliser et partager l'A.P.I. conformément à leur législation respective* »[71] ; or le niveau de protection offert par la législation américaine semble inférieur à celle prévue par la directive européenne en la matière. Dès lors, la Commission européenne a tenté de dissuader les Tchèques de signer cet accord en attendant que les Vingt-sept déterminent une position commune à adopter vis-à-vis des États-Unis. Le refus des tchèques risque d'affaiblir la position de négociation de l'U.E. et d'influencer des pays tels que l'Estonie, également désireux d'intégrer le *Visa Waiver Program* américain.

II. - Le nouvel accord P.N.R. du 23 juillet 2007

Le 30 septembre 2007 expirait le délai fixé par l'arrêt prononcé par la C.J.C.E concernant la date de conclusion d'un nouvel accord entre l'Union européenne et les États-Unis. Lors des négociations, les États-Unis ont exigé d'une part, que les agences américaines chargées de lutter contre le terrorisme puissent avoir accès aux données P.N.R. (qui étaient au départ seulement accessibles au C.B.P.) et, d'autre part, que la liste des données accessibles soit augmentée. L'objectif conjoint des négociations est de mettre fin au conflit juridique caractérisé par l'absence de standard de protection « adéquat » des données personnelles. Ces termes sont dès lors problématiques en ce que « adéquat » ne signifie pas que la protection accordée par les États-Unis doit être équivalente à celle offerte par l'Union européenne. On

[69] Challenge, *Liberty & Security*, "*Hungary's President says no to the PNR agreement*", 13 décembre 2006. Disponible à l'adresse suivante : http://www.libertysecurity.org/article1212.html.

[70] *Memorandum of understanding between the Ministry of the Interior of the Czech Republic and the Department of Homeland Security of the United States of America regarding the United States Visa Waiver Program and related enhanced security measures.*

[71] *Ibid.*

assiste donc à une appréciation d'un « standard minimum » afin de respecter les législations pertinentes des deux parties. La finalité n'est donc pas de considérer le standard qui sera le plus protecteur des individus mais de parvenir à un accord sur la nature des règles applicables. Les considérations politiques sont ainsi prégnantes car, en toile de fond, il est question de part et d'autre d'importer un modèle juridique de lutte contre le terrorisme. La problématique se pose alors en ces termes : les négociations de l'accord P.N.R. mettent en exergue des approches différentes caractérisées par la primauté de la sécurité de la patrie pour les États-Unis, et l'importance de la protection de la vie privée pour l'Union européenne. C'est dans un tel contexte que, le 15 février 2007, le Conseil a donc donné mandat à la Commission européenne pour négocier un nouvel accord avec les États-Unis.

A. Le contenu de l'accord, un progrès en matière de protection des droits fondamentaux ?

Le nouvel accord P.N.R. a été signé le 23 juillet 2007 : il est applicable pour une durée de sept ans et autorise les compagnies aériennes à communiquer au Ministère américain de la sécurité intérieure des informations personnelles sur les passagers transportés à destination ou via les États-Unis. En l'espèce, le Contrôleur européen de la protection des données et le Groupe de l'article 29 dénoncent inter alia la durée excessive de conservation des données, la possibilité d'accès, même limitée, aux données sensibles et enfin, l'évaluation de l'application de l'accord confiée au seul Commissaire européen en charge de la Justice-Liberté-Sécurité, sans que les autorités nationales de protection des données n'y soient clairement associées.

1. Limitation des données transférables et augmentation des délais de conservation

Abordant la question du transfert des données P.N.R., il s'agit de s'en remettre à la définition déterminée par l'O.A.C.I.[72] L'accord P.N.R. de 2007 tient compte des recommandations émises par le Groupe de travail de l'article 29 qui préconisait déjà en 2004 le transfert de dix-neuf données P.N.R.[73] afin de respecter le principe de proportionnalité inscrit à l'article 6 (1) (c) de la directive 95/46/CE[74]. En effet, les demandes américaines originelles présentées lors des négociations en 2003 concernaient la totalité des

[72] Lignes Directrices sur les données des dossiers passagers (P.N.R.), Cir 309 AT/131, OACI, avril 2006, Annexe 3, Glossaire, p. 13 : « *transfert, à partir du ou des systèmes d'un exploitant d'aéronefs, de données P.N.R. à un État qui a demandé les données en question ou accès par l'État aux données contenues dans le ou les systèmes de l'exploitant*. »

[73] Avis 4/2003 sur le Niveau de Protection assuré aux États-Unis pour la Transmission des Données Passagers, Adopté le 13 juin 2003, 11070/03/FR, WP 78, « Données personnelles transférables » : « *Les données devraient inclure les informations suivantes: "PNR record locator code", date de réservation, date(s) prévue(s) du voyage, nom du passager, autres noms présents dans le PNR, l'itinéraire de voyage, identifiants de billets gratuits, billets aller simple, "ticketing field information", données "ATFQ (Automatic Ticket Fare Quote)", numéro de billet, date à laquelle le billet a été délivré, "no show history", nombre de bagages, numéros des étiquettes de bagages, " go show information", nombre de bagages sur chaque segment, changements de classe volontaires ou involontaires, détail des changements effectués sur les données PNR et concernant les éléments mentionnés précédemment* », p. 8.

[74] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, Article 6 : « *1. Les États membres prévoient que les données à caractère personnel doivent être: […] c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*. »

données inclues dans le dossier passager. La Commission a néanmoins obtenu que cette demande soit réduite à trente-quatre données en 2004 et enfin à dix-neuf en 2007. Il faut cependant noter que cette réduction du nombre de rubriques de données transférables est effectuée en trompe l'œil dans la mesure où différents types de données sont regroupés au sein de chaque rubrique dans l'accord de 2007 alors qu'elles étaient envisagées de manière isolée dans l'accord de 2004. A titre d'exemple, la rubrique 17 de l'accord de 2007 comprend les « Remarques générales, y compris les données *Other Service Information* (O.S.I.), *Sensitive Security Information* (S.S.I.) et *Special Service Request* (S.S.R.) », rubriques qui étaient distinguées dans l'accord de 2004 sous les rubriques 26 et 27 et qui sont fusionnées dans l'accord de 2007. Ces données sont ainsi recueillies par le D.H.S. à des fins de traitement[75] en vue du profilage des terroristes potentiels. La question du transfert des données P.N.R. renvoi aussi à la problématique sous-jacente des modalités de gestion des systèmes informatisés de réservation (S.I.R.)[76] et des systèmes de contrôle des départs (S.C.D.)[77].

Du point de vue du respect du principe de proportionnalité, les données A.P.I. sont déjà collectées en Europe conformément au règlement du Conseil instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation[78] et peuvent donc être transférés aux États-Unis sur la base d'un régime comparable contrairement aux données P.N.R. Quant à la durée de conservation des données, les autorités américaines ont initialement proposé qu'elles soient conservées durant cinquante ans. En 2004, les États-Unis ont accepté de ramener cette période à une durée de trois ans et six mois. L'accord de 2004 ainsi que l'accord de 2007 établissent une distinction entre « conservation active » et « conservation inactive ». Concernant la conservation active des données, l'accord de 2004 autorisait l'accès en ligne du C.B.P. aux données P.N.R. pour une durée de sept jours, période au terme de laquelle le nombre de fonctionnaires autorisés à consulter ces données était restreint pendant une période de trois ans et six mois à compter de la date d'accès aux données dans le système de réservation ou de la date de réception des données[79]. Au terme de cette période, les données P.N.R. non-consultées étaient supposées être détruites. A l'inverse, les données consultées manuellement durant cette période étaient transférées par le C.B.P. vers

[75] Il faut entendre le terme « traitement » comme « *[…] toute opération ou série d'opérations exécutées sur les données P.N.R., telles que la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou l'altération, le rappel, la récupération, la consultation, l'utilisation, le transfert, la diffusion ou la mise à disposition sous toute autre forme, l'alignement ou la combinaison, le groupage, l'effacement ou le destruction.* », Cf. Lignes Directrices sur les données des dossiers passagers (P.N.R.), Glossaire, p. 13.

[76] Proposition de Décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* -PNR) à des fins répressives, présentée par la Commission, 2007/0237 (CNS), 6 novembre 2007, « Système informatisé de réservation » : « *système interne d'inventaire du transporteur aérien dans lequel les données PNR sont collectées à partir des réservations faites par le biais de systèmes informatisés de réservation tels que définis par le règlement (CEE) n° 2299/89 instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation, ou par des canaux de réservation directe comme les sites Internet des lignes aériennes, les centres d'appel ou les points de vente.* »

[77] Lignes Directrices sur les données des dossiers passagers (P.N.R.), Glossaire, p. 13, « Système de contrôle des départs » : « *Système utilisé pour enregistrer les passagers à l'embarquement. Le SCD contient des données sur l'enregistrement telles que le numéro de siège te les renseignements sur les bagages.*»

[78] Règlement (CE) nº 323/1999 du Conseil, du 8 février 1999, modifiant le règlement (CEE) nº 2299/89 instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation (SIR).

[79] Titre 44, sections 2101 et suivantes du Code des États-Unis.

un « fichier de dossiers supprimés » au sein duquel elles étaient conservées durant huit ans puis détruites. Cette « base de conservation inactive » permettait le stockage des informations sous forme de données brutes ne pouvant être exploitées à l'occasion d'enquêtes traditionnelles, et était uniquement accessible au personnel habilité du Bureau des affaires internes (*Office of Internal Affairs*) du C.B.P. La problématique résidait en ce que ces délais ne s'appliquaient pas aux données P.N.R. en rapport avec un dossier répressif, qui demeuraient accessibles jusqu'à ce que le dossier en question soit archivé. L'accord de 2007 prévoit une « conservation active » par le D.H.S. pendant sept ans. Les données sont par la suite transférées vers une base de « conservation inactive » pour une durée supplémentaire de huit ans pendant laquelle l'accès ne sera possible que dans les situations "exceptionnelles" et sous réserve de "conditions strictes"[80]. Il est intéressant de constater que l'accord de 2007 ne règle pas définitivement la question de la destruction de ces données au terme du délai supplémentaire de conservation inactive. Si le D.H.S. précise que les données liées à une enquête policière sont conservées dans une base de données active jusqu'à la clôture des investigations[81], l'accord dispose que des négociations supplémentaires seront nécessaires afin de déterminer « si et quand il convient de détruire les données P.N.R. »[82]

2. Système d'exportation et données sensibles : quelles limites au pouvoir accordé au D.H.S. ?

La détermination des mécanismes d'extraction est cruciale notamment du point de vue de la protection des données sensibles. A ce propos, il semble pertinent de souligner qu'une évaluation collective (« *joint review* ») a été organisée en septembre 2005 concernant l'état de la mise en œuvre des engagements du C.B.P. Dans son rapport final du le 21 septembre 2005, l'équipe européenne constatait une conformité substantielle aux engagements américains, ce qui n'était pas le cas au mois de mai 2005. En effet, le C.B.P. n'avait mis en œuvre le système de filtrage des données sensibles que le 15 mars 2005, raison pour laquelle l'équipe européenne recommandait à l'administration américaine de supprimer les données P.N.R. collectées par le C.B.P. entre le 28 mai 2004 et le 15 mars 2005[83]. Ce faisant, l'accord de 2007 apporte une amorce ce clarification concernant la méthode d'extraction de ces données mais l'incertitude demeure quant au traitement des données sensibles.

a. La coexistence des méthodes d'extraction « *push* » et « *pull* »

Initialement, l'accord P.N.R. de 2004 disposait que le transfert des données P.N.R. vers le C.B.P. devait

[80] Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007, p. 10

[81] *Op. cit.*

[82] *Ibid*.

[83] GUILD, Elspeth et BROUWER, Evelien, « The Political Life Of Data. The ECJ Decision On The PNR Agreement Between The EU And The US », Center for European Policy Studies, Policy Brief, n° 109, juillet 2006, p. 2. Disponible à l'adresse suivante : http://www.ceps.eu/files/book/1363.pdf.

s'effectuer par le biais de la méthode dite « *pull* ». Selon l'O.A.C.I., cette méthode signifie que « *Les autorités publiques de l'État demandant les données peuvent accéder aux systèmes des exploitants et extraire de leurs bases de données une copie des données requises* »[84]. Ce faisant, ce système d'extraction ne satisfait pas au principe de sécurité juridique ne serait-ce que dans la mesure où les critères de transfert sont imprévisibles. En effet, au sein de ce système, la mise en œuvre de mécanismes de filtrage des rubriques de données transférables ne saurait être totalement effective dès lors qu'elle est subordonnée au pouvoir discrétionnaire dont pourrait disposer les autorités américaines afin de recueillir un nombre maximum de données personnelles. Compte tenu du contexte de lutte contre le terrorisme et de la nécessité d'établir des profils de suspects, la collecte d'un nombre élevé d'informations est un élément essentiel pour la sûreté nationale des États, et pas seulement celle des États-Unis. Dès lors, il est essentiel que le champ d'action des États, lors de l'opération de collecte des données P.N.R., soit clairement délimité et encadré afin d'éviter toute mise en œuvre d'un pouvoir arbitraire. Par ailleurs, il est nécessaire de souligner que lors des négociations transatlantiques en 2003, les autorités américaines ont émis le souhait d'intégrer la criminalité interne dans les finalités poursuivies par la collecte des données P.N.R., et non pas de les limiter à la seule prévention contre le terrorisme. Bien que la Commission ait obtenu par la suite un engagement de principe de la part des États-Unis afin d'exclure cet élément, il semble audacieux du point de vue du principe de nécessité et de proportionnalité de consacrer au sein d'un accord international la méthode d'extraction la moins transparente. Partant de ce principe, et compte tenu du rôle accru des agences nationales de renseignement dans la lutte contre le terrorisme, il n'existerait donc aucun moyen juridique valide de vérifier que les données recueillies sont effectivement conformes à la finalité poursuivie et n'outrepassent pas le cadre de ce qui est considéré comme strictement nécessaire. Pour cette raison, l'O.A.C.I. recommande l'utilisation de la méthode «*push* »[85].

A l'inverse, la méthode dite « *push »* est consacrée par l'accord P.N.R. de 2007 et permet que « *Les exploitants transfèrent eux-mêmes les données P.N.R. requises dans les bases de données des autorités qui les demandent* »[86]. Ce système permet de contrôler les flux de données au sein de l'Union partants des systèmes de réservation ou des transporteurs aériens vers le Ministère de la sécurité intérieure. Désormais, il incombe aux compagnies aériennes de mettre en œuvre les moyens techniques nécessaires afin d'amorcer la transition et d'instaurer le système « *push* ». L'accord P.N.R. prévoit que le D.H.S. utilise cette méthode d'extraction au plus tard le 1er janvier 2008, mais seulement envers les transporteurs aériens qui ce sont conformés aux exigences techniques de ce système[87]. A défaut, la coexistence avec le système

[84] Lignes Directrices sur les données des dossiers passagers (P.N.R.), Cir 309 AT/131, Organisation de l'aviation civile internationale, avril 2006, article 7.1, « Méthodes de transfert des données PNR ».

[85] Article 7.3.

[86] *Ibid.*

[87] 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 du dossier passager (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), p. 10.

« *pull* » est prévue jusqu'à ce que les transporteurs aériens aient mis en œuvre un système conforme aux exigences techniques du D.H.S. Comme l'a souligné récemment le Parlement européen, la coexistence des deux systèmes pourrait entraîner une distorsion de concurrence entre les transporteurs aériens européens[88] et affecter le droit à la vie privée ainsi que le protection des données personnelles. Cette confusion dans l'application des méthodes d'extraction est étroitement liée au coût financier qu'implique le passage du système « *pull* » au système « *push* » pour les compagnies aériennes. L'industrie aéronautique subit donc de plein fouet les conséquences financières de l'accord P.N.R. ; l'investissement concernant cette mise en conformité des systèmes représente environ cinq millions d'euros. A l'heure actuelle, la mise en œuvre des mesures de lutte contre le terrorisme représente 25% des dépenses effectuées au sein des aéroports européens. Dès lors, les compagnies aériennes affirment que la lutte antiterroriste correspond à l'obligation de sécurité nationale qui incombe à l'État : les gouvernements devraient donc être impliqués dans le financement de ces mesures[89].

b. Données sensibles accessibles en cas de circonstances exceptionnelles

La question de l'accès du D.H.S. aux données dites « sensibles » inclues dans les données du dossier passager constitue l'une des principales pierres d'achoppement entre les États-Unis et l'Union européenne. En effet, ce type de données peut révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et les données relatives à la santé ou à la vie sexuelle du passager[90]. Différentes informations du P.N.R. peuvent aussi renseigner les autorités étatiques sur les pratiques du passager appartenant néanmoins à sa propre sphère privée. Par exemple, les données S.S.R. (« *Special Service Request* ») peuvent inclure des informations notamment concernant la nature des repas commandés à bord de l'aéronef, information renvoyant directement à la pratique de certaines religions. Considérant la nature extrêmement personnelle de ces données, pouvant même aller jusqu'à la prise en considération des caractéristiques de l'intégrité physique du passager ou de sa liberté d'opinion et de conscience, ces données sensibles bénéficient de la protection de l'article 8 de la Convention européenne des droits de l'homme et leur traitement devrait être interdit selon les recommandations du Groupe de travail de l'article 29. Bien que l'accord de 2007[91] souligne que le D.H.S. utilise un système automatisé qui filtre les données sensibles, dès lors non utilisables par l'administration américaine, l'accord mentionne néanmoins la possibilité pour le D.H.S. d'accéder à ces données en cas de circonstances exceptionnelles. En vertu de l'accord P.N.R. de 2007, la définition du terme « circonstances exceptionnelles » est particulièrement large et implique les « *cas exceptionnel[s] où la vie de la personne*

[88] Résolution du Parlement européen du 12 juillet 2007 sur l'accord avec les États-Unis d'Amérique concernant l'utilisation de données des dossiers des passagers aériens (PNR) ; voir aussi *Association of European Airlines*, « *Airports and airlines applaud EU moves to harmonise aviation security measures at more 'passenger-friendly' level* », 28 septembre 2006.

[89] *Eur.Activ*, "*Transports security*" ; available at http://www.euractiv.com/en/transport/transport-security/article

[90] Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007, p. 8.

[91] *Idem.*, p. 7.

concernée ou d'autres personnes pourrait être mise en danger ou subir une atteinte grave »[92]. Dans cette hypothèse, les fonctionnaires du Ministère de la sécurité intérieure peuvent collecter et traiter des données personnelles additionnelles, dont les données sensibles.

A ce propos, l'accord apparaît très permissif, allant même jusqu'à représenter un empiètement sur les pouvoirs de l'Union européenne et la souveraineté des États membres. Car le D.H.S peut consulter les données sensibles concernant les passagers sans même avoir à obtenir le consentement préalable de la Commission, qui sera « normalement » avertie quarante-huit heures après qu'elles aient été utilisées. Le caractère particulièrement évasif des engagements de l'administration américaine en la matière est ici à souligner mais aussi l'incapacité de l'Union à faire effectivement respecter les dispositions relatives à la protection des données. Que le traitement relève du premier ou du troisième pilier, la notion de consentement apparaît clairement dans les directives européennes pertinentes[93]. La seule obligation qui incombe alors au D.H.S. est la tenue d'un « registre des accès à toute donnée sensible provenant des P.N.R. de l'Union européenne ». Au-delà de l'accès à ces données, il est question de leur traitement et de leur conservation par le D.H.S. sans pour autant que des critères clairs, précis et accessibles n'aient été conjointement déterminés avec l'Union au travers de l'accord international. L'accord dispose en effet que le D.H.S « supprimera ces données dans un délai de trente jours après que les fins pour lesquelles les données ont été consultées ont été atteintes et si leur conservation n'est pas exigée par la loi. »[94] *De facto*, aucune garantie juridique n'est proposée afin de vérifier non seulement que les données sensibles ont été consultées mais aussi qu'elles ont bien été supprimées. Cet état de fait est d'autant plus problématique que, depuis le vote par le Président Bush du décret n° 13388 relatif à la coopération entre les agences du gouvernement américain en matière de lutte contre le terrorisme[95], la capacité d'accès des agences nationales de renseignement telles que la C.I.A. et le F.B.I., elles-mêmes en coopération directe avec Interpol, a été élargie[96].

Compte tenu de l'opacité des critères juridiques autorisant l'accès aux données personnelles, le droit de

[92] *Ibid.* p. 9.

[93] Voir notamment Directive 95/46/CE, Considérant 30 : « *considérant que, pour être licite, un traitement de données à caractère personnel doit en outre être fondé sur le consentement de la personne concernée [...]* »; Considérant 33 : « *considérant que les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement, sauf consentement explicite de la personne concernée* » ; article 7.1 et article 8.1 concernant les données sensibles : « *Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.* » ; Proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, article 11.2 : « *Les données à caractère personnel concernées ne font l'objet d'un traitement ultérieur pour les finalités visées au paragraphe 1, point b), qu'avec le consentement préalable de l'autorité qui a transmis les données personnelles ou les a mises à disposition.* »

[94] Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007, p. 9.

[95] *Executive Order 13388 of October 25, 2005, Further Strengthening the Sharing of Terrorism Information To Protect Americans, Presidential Documents, Federal Register* Vol. 70, No. 207, Thursday, October 27, 2005; disponible sur http://edocket.access.gpo.gov/2005/pdf/05-21571.pdf.

[96] *National Strategy For Information Sharing, Successes and Challenges In Improving Terrorism-Related Information Sharing*, Octobre 2007. Disponible sur www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.

recours de l'individu contre toute utilisation abusive des ses données personnelles devient inopérant. Dans les conditions décrites ci-dessus, le passager n'a pas connaissance de la collecte et du traitement des données sensibles le concernant et ne peut, par conséquent, exercer son droit au juge. Pourtant, les dispositions européennes garantissent ce droit, bien que la relation entre la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne ne soit pas toujours aisée à définir. L'article 6 paragraphe 2 du Traité sur l'Union européenne clarifie néanmoins cette relation[97]. Concernant plus particulièrement le droit au juge, l'article 47 de la Charte[98] définit ce droit en termes plus compréhensifs que l'article 6.1 de la C.E.D.H. Enfin, la protection offerte à l'individu en vertu de la législation communautaire est reflétée dans l'article 8 de la Charte qui envisage la question de la protection des données à caractère personnel au travers d'un organe indépendant de contrôle[99]. En conséquence, la protection des données sensibles et l'effectivité du droit au juge semblent peu satisfaisantes au regard du régime juridique de l'accord P.N.R. de 2007.

B. Les garanties associées et le droit à la vie privée régis par le principe de réciprocité

L'accord P.N.R. de 2007 présente des garanties relatives aux principes généraux régissant le traitement des données à caractère personnel et consacre le principe de disponibilité des données du dossier passager. Ces garanties sont hétérogènes et leur applicabilité est assujettie à la finalité de lutte contre le terrorisme envisagée de manière extensive. Aussi, l'accord témoigne d'une certaine imprécision concernant la définition des concepts fondamentaux et confirme le principe de réciprocité. L'Union ne requiert pas du Ministère de la sécurité intérieure une protection des données plus stricte que celle offerte par les dispositions européennes et inversement, le D.H.S ne demande pas à l'Union d'adopter des mesures plus strictes que celles existantes aux États-Unis. En outre, la proposition de décision-cadre relative à l'instauration d'un « P.N.R. européen », consécutive à la signature de l'accord transatlantique, est explicitement influencée par les caractéristiques précitées.

1. Le respect des principes généraux de traitement légal des données personnelles

[97] Les traités de Rome, Maastricht, Amsterdam et Nice, Paris, *La Documentation Française*, 2002, p. 15, article 6, paragraphe 2 : « *L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales […] et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, en tant que principes généraux du droit communautaire*. ». Voir également l'arrêt C.E.D.H., 23 mars 1995, *Loizidou c. Turquie (exceptions préliminaires)*, § 75.

[98] Charte des droits fondamentaux de l'Union européenne, Article 47 : « *Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter. Une aide juridictionnelle est accordée à ceux qui ne disposent pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l'effectivité de l'accès à la justice* ».

[99] Charte des droits fondamentaux de l'Union européenne, Article 8 : « *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* ».

Quatre grands principes généraux régissent le traitement légal des données personnelles : le principe de limitation des finalités, le principe de nécessité, le principe de proportionnalité et enfin, le principe de protection adéquate[100]. Concernant le principe de limitation des finalités, l'accord P.N.R. 2007 souligne que le Ministère de la sécurité intérieure utilise les données P.N.R. afin de prévenir le terrorisme et les crimes reliés, de combattre les crimes graves de nature transnationale - incluant la criminalité organisée - et d'empêcher que des individus se soustraient aux mandats et autres mesures appliquées en réponse aux crimes précités. L'accord ajoute que ces données peuvent être utilisées pour la protection des intérêts vitaux de la personne concernée ou d'autres personnes, mais aussi dans le cadre d'une procédure pénale ou toute autre procédure prévue par la loi[101]. En l'espèce, le fait d'énoncer différentes finalités en des termes aussi larges ne saurait constituer une limitation effective des finalités poursuivies par l'accord. Au-delà de la lutte contre le terrorisme, de nombreux crimes - et même des délits - peuvent tomber sous le coup de cet accord. Tandis que les données P.N.R. des compagnies européennes devaient originellement être collectées en vue d'assurer la sûreté de l'aviation civile, la finalité est désormais étendue aux questions plus générales ayant trait à la sécurité nationale des États-Unis. *De facto*, cette imprécision tronque l'application du principe de nécessité et de proportionnalité. Le postulat affirmé par l'Union européenne est que la collecte d'informations personnelles visant la lutte contre le terrorisme et la criminalité organisée constitue une finalité qui satisfait au principe de nécessité entendu au sens de l'article 8 de la C.E.D.H. Tel n'est pas le cas pour les autres types de crimes envisagés dans l'accord, élément qui constitue une extension des finalités aux « crimes ordinaires ». Cette approche affecte la mise en œuvre du principe de proportionnalité. Le critère de proportionnalité concerne tous les paramètres du traitement des données (éléments envisagés dans les sections précédentes). Dans le cadre du droit européen, ces évaluations doivent tenir compte des exigences résultant du principe de subsidiarité régissant les relations entre les États membres et l'Union européenne. Cela est d'autant plus nécessaire en l'espèce car la décision du Conseil entérinant l'accord P.N.R. prive les États membres de la possibilité d'intervenir. L'accord de 2007 permet le transfert par le D.H.S. des données P.N.R. transférées par les transporteurs aériens européens vers d'autres États tiers. L'accord mentionne que dans ce cas, le D.H.S. se réfère « *aux engagements exprès* » conclu entre les États-Unis et ces États tiers, sans que l'Union européenne n'ait la capacité d'intervenir afin d'évaluer le niveau d'adéquation de la protection offerte par cet État. Les États-Unis sont donc seuls juges de l'appréciation de cette adéquation et la seule garantie offerte à l'Union est

[100] Avis 10/2001 sur la nécessité d'une approche équilibrée dans la lutte contre le terrorisme, adopté le 14 décembre 2001, 0901/02/FR/Final, WP 53, p. 4 : « *Le groupe souligne également l'obligation de respecter le principe de proportionnalité concernant toute mesure restreignant le droit fondamental au respect de la vie privée selon l'article 8 de la Convention européenne des droits de l'homme et la jurisprudence s'y rapportant. Cela implique, entre autres, l'obligation de démontrer que toute mesure prise correspond à un "besoin social impératif" […]. Le groupe de travail souligne donc la nécessité d'organiser un débat approfondi sur les actions de lutte contre le terrorisme, […] en refusant notamment l'amalgame entre la lutte contre le terrorisme réel et la lutte contre la criminalité en général, et en limitant également les mesures procédurales empiétant sur la vie privée à celles qui sont absolument nécessaires. De plus, le groupe de travail rappelle que les mesures législatives limitant le droit des personnes au respect de la vie privée doivent être accessibles et prévisibles quant à leurs implications pour les personnes concernées. […]. Elles devraient notamment spécifier où ces mesures peuvent être utilisées et devraient exclure toute surveillance générale ou préliminaire et offrir une protection contre les attaques arbitraires des pouvoirs publics* ».

[101] Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007, p. 7.

que ces échanges comprennent des « *dispositions de protection comparables à celle qu'applique le D.H.S. aux données P.N.R. de l'U.E.* »[102]

Quant à la question de la protection « *adéquate* »[103], celle-ci est régie par le principe de réciprocité. De plus, le terme « *adéquate* » ne signifie pas que le D.H.S. doit mettre en œuvre des garanties équivalentes à celles énoncées par la législation européenne pertinente. Nonobstant, ce caractère adéquat est évalué en fonctions des dispositions de l'article 6 T.U.E., de l'article 8 de la Charte des droits fondamentaux de l'Union européenne et de l'article 8 de la C.E.D.H. A ce propos, il est nécessaire d'envisager le droit d'accès et le droit de recours consacrés par l'accord de 2007. Le F.O.I.A., en ce qu'il est applicable à toute personne peu importe la nationalité et le pays de résidence, garantie que les ressortissants de l'Union concernés par le transfert de données P.N.R. puissent avoir accès aux registres d'une agence fédérale des États-Unis, sauf si une dérogation au droit de divulgation est prévue par la loi. Dans ce cas, le citoyen européen dispose de recours administratifs et judiciaires afin de contester le refus de divulgation du D.H.S. La difficulté réside en ce que le *Privacy Act* n'est pas applicable aux citoyens européens. A ce sujet, l'accord de 2007 précise que le D.H.S. a pris une décision politique afin d'étendre les protections administratives prévues par le *Privacy Act* aux données P.N.R. stockées dans le système automatisé de ciblage (A.T.S.) et de les rendre applicables au citoyens européens[104]. Néanmoins, la portée juridique d'une telle décision ne confère aucune garantie effective pour les citoyens européens. Enfin, au lendemain de la signature de l'accord P.N.R., les États-Unis ont annoncé leur intention d'insérer davantage d'exceptions dans le *Privacy Act* en ce qui concerne la gestion du système A.T.S. Or tout changement dans la gestion de ce système modifie automatiquement et de manière unilatérale le contenu de l'accord P.N.R. Le projet prévoit que l'ensemble de ces données pourra faire l'objet d'une seconde inspection[105] et être consulté par d'autres agences de renseignement[106].

2. L'impact au sein de l'U.E. : la décision-cadre relative au P.N.R. européen

Une nouvelle mesure de lutte contre le terrorisme a été annoncée en 2007 par le Commissaire Franco Frattini ; ce dernier a proposé aux États membres de l'Union de se doter d'un système de stockage des données P.N.R. des passagers des vols atterrissant sur leur territoire. Ce faisant, cette décision consacre le caractère inédit de l'utilisation de données commerciales à des fins répressives au sein de l'Union. Les États membres doivent ainsi se conformer aux dispositions de cette proposition avant le 31 décembre 2010. Cette proposition reflète l'influence substantielle de la législation américaine en matière de lutte

[102] *Idem.*

[103] Voir l'article 25 de la directive 95/46/CE.

[104] *Statement by Homeland Security Secretary Michael Chertoff on a new Agreement with the European Union for Passenger Name Record Data Sharing*, July 26, 2007, DHS Press Office, (202) 282

[105] *Statewatch News Online*, "*EU-USA agreement renegociated to meet US demands*", "*Automated Targeting system*", 2007/08/06

[106] *Department of Homeland Security*, *Privacy Act of 1974, Implementation of Exceptions, Proposed Rules of the Federal Register, Notice of proposed rulemaking*, 23 août 2007.

contre le terrorisme et de sûreté de l'aviation civile. En effet, cette initiative de la Commission s'inspire directement du projet initial des autorités américaines requérant l'accès aux données P.N.R. des compagnies aériennes européennes. La question est donc de déterminer si, au-delà d'être une source d'inspiration, l'expérience des difficultés révélées par les négociations transatlantiques bénéficie à l'Union afin d'assurer une garantie effective du droit à la vie privée, de la protection des données personnelles et du droit de recours dans le contexte de la lutte antiterroriste. Car cette proposition de création d'un P.N.R. européen intervient alors qu'aucun bilan de la mise en œuvre du P.N.R. américain n'a été effectué[107].

La proposition de décision-cadre présentée par la Commission[108] implique que les transporteurs aériens communiquent par voie électronique aux Unités de Renseignements des Passagers (U.R.P.)[109], dix-neuf données P.N.R. relatives aux vols internationaux. Le traitement de ces données par les U.R.P. vise une analyse des risques que présentent les passagers, et ce en vertu des critères établis par le droit national. En vertu de l'article 5, paragraphe 4 de la proposition de décision-cadre, les données sont communiquées par les transporteurs vingt-quatre heures avant le départ et via la méthode « *push* ». La difficulté en l'espèce est que la méthode « *pull* » peut être utilisée par les U.R.P. si les transporteurs ne possèdent pas de bases de données dans un État membre de l'Union. Il en va de même pour les compagnies qui n'ont pas encore mis en place l'infrastructure technique nécessaire pour utiliser la méthode « *push* ». A défaut de communication de ces données P.N.R., les États membres sont habilités à imposer des sanctions aux compagnies aériennes pouvant aller jusqu'à l'immobilisation de l'aéronef ou encore le retrait de la licence d'exploitation[110]. Les U.R.P. des différents États membres s'échangent les données P.N.R. figurant sur leurs bases de données respectives et, à titre exceptionnel, peuvent demander l'accès à ces données plus de vingt-quatre heures avant le départ programmé d'un vol[111]. Concernant la communication de ces données à des pays tiers, l'article 8 de la décision-cadre souligne que l'État tiers doit satisfaire aux conditions et garanties prévues par la décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre du troisième pilier (coopération policière et judiciaire en matière pénale). Qui plus est, cette communication n'est rendue possible qu'à condition que les autorités répressives de l'État tiers ne les utilisent qu'à des fins de lutte contre le terrorisme et la criminalité organisée. Enfin, l'État tiers doit s'engager à ne pas transférer ces données à d'autres États tiers sans l'autorisation expresse de l'État membre.

De facto, les garanties de protection du droit à la vie privée et des données à caractère personnel semblent

[107] Voir à ce propos les commentaires de la députée néerlandaise Sophia In'd Veld rapporteur sur les questions PNR au sein de la Commission LIBE du Parlement européen ; disponible à http://www.statewatch.org/news/2007/jul/03eu-pnr.htm

[108] Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* -PNR) à des fins répressives (présentée par la Commission){SEC(2007) 1422}{SEC(2007) 1453}, 6 novembre 2007

[109] L'URP, désignée par chaque État membre, est un organisme chargé de rassembler les données PNR transmises par ces transporteurs ; elle est composée des membres de services nationaux chargés de la lutte contre le terrorisme et la criminalité organisée.

[110] Article 10.

[111] Article 7 § 4.

satisfaisantes au regard des dispositions européennes et communautaires pertinentes et conformément au principe de limitation des finalités et de proportionnalité. D'une part, les données collectées doivent être nécessaires pour prévenir et combattre les infractions terroristes et la criminalité organisée. D'autre part, le champ d'application de la proposition ne concerne que les éléments suivants, qui nécessitent une approche harmonisée: la définition de la mission des U.R.P., la nature des données collectées, les finalités poursuivies, la communication des données entre les Unités des États membres et les conditions techniques de cette communication. Le choix de l'utilisation d'une décision-cadre par la Commission permet une grande marge d'appréciation aux État en ce qui concerne les aspects techniques de sa mise en œuvre. Il n'est pas certain que cet élément soit en faveur d'une action uniforme des États membres car il est question de la création de vingt-sept guichets U.R.P. Concernant les délais de conservation des données P.N.R., l'article 9 de la décision-cadre précise qu'elles sont stockées par le U.R.P. dans une base de données active durant cinq ans puis huit années supplémentaires dans une base de données dormante, période durant laquelle l'accès est limité. Au terme de cette période, les données P.N.R. doivent être supprimées. Mais l'article 9, paragraphe 4 prévoit un régime de dérogation dans l'hypothèse où ces données sont relatives à un individu visé par une enquête criminelle. Dans ce cas, ces données ne sont effacées qu'à la clôture de l'enquête. Certains députés du Parlement européen ont témoigné leur inquiétude concernant la mise en œuvre de ce P.N.R. européen, et notamment en matière de limitation des finalités. Il apparaît dès lors important de souligner que, dans l'hypothèse où cet accord est voté avant le 31 décembre 2008, date prévue pour l'entrée en vigueur du nouveau traité, il le sera à l'unanimité avec une simple consultation du Parlement. En revanche, après cette date, le texte réclamera une procédure de codécision: le Parlement aura donc le même poids que le Conseil.

CONCLUSION

D'un point de vue institutionnel, les négociations transatlantiques ont mis en exergue le nouveau rôle assumé par la Commission. A l'origine, la Commission était absente de la gestion de la sûreté aérienne car ce domaine relevait jusqu'à lors du domaine intergouvernemental et des politiques nationales. Mais l'action proactive de la Commission au sein du forum transatlantique *Policy Dialogue on Borders and Transport Security* (P.D.B.T.S.) s'est néanmoins effectuée au détriment des États membres qui ont été écartés des débats. De plus, les négociations de l'accord P.N.R. ont mis en exergue les faiblesses de l'Union européenne qui résultent de sa construction en piliers. Des lacunes persistent concernant la protection des données personnelles dans le cadre de la coopération policière et judiciaire en matière pénale.

Le contenu de l'accord P.N.R. de 2007 reflète des progrès indéniables depuis le début des négociations en 2003 tels que la réduction du nombre de rubriques de données transférables. Différents points de cet accord sont pourtant à renégocier. La question de la conservation et de la destruction des données P.N.R.

rattachées à une enquête policière effectuée aux États-Unis constitue un enjeu majeur concernant les futures négociations, prévues dans les dispositions même de l'accord. Qui plus est, l'insécurité juridique demeure dans la mesure où il est accordé au Ministère de la sécurité intérieure un pouvoir de modification unilatérale des finalités poursuivies par l'accord. Enfin, l'accord révèle un affaiblissement des standards de protection sur trois points : l'utilisation des données sensibles est rendue possible sans l'autorisation préalable de l'Union européenne ; le droit d'accès du citoyen au données du dossier passager est soumis à un régime dérogatoire ; enfin, le droit de recours devant une Cour américaine est restreint pour les citoyens européens.

L'impact de la législation antiterroriste américaine au sein de l'Union européenne est néanmoins illustré par la proposition de décision-cadre qui permettrait l'instauration d'un P.N.R. européen, directement influencé par le modèle américain. Les États membres sont donc amenés à se prononcer sur le caractère adéquat des protections offertes par ces dispositions. Les futures négociations transatlantiques et le processus décisionnel dans son ensemble devraient être plus transparents. Cela semble compromis au regard de la révélation au mois de juin 2008[112] de négociations secrètes entre les États-Unis et l'Union européenne concernant la question du transfert des données personnelles. Nonobstant, la question de la réforme interne de l'Union européenne pourrait fortement influencer l'issue des tractations concernant les négociations additionnelles relatives à l'accord P.N.R.. Dans l'hypothèse de l'entrée en vigueur du Traité de Lisbonne, l'U.E. bénéficierait d'une position plus favorable et un rôle plus important serait accordé au Parlement dans le processus décisionnel. Dans ce contexte, un cadre multilatéral de négociation apparaît des plus nécessaire. L'Organisation de l'aviation civile internationale pourrait ainsi représenter un forum de négociation, au sein duquel le principe de réciprocité serait mis en œuvre de manière plus effective concernant les standards de protection applicables en l'espèce.

Enfin, outre le transfert de ces données commerciales à des fins répressives, les dispositions de l'accord autorisent le transfert des données personnelles vers les services fédéraux de l'immigration (*U.S. Citizenship and Immigration Services*, U.S.C.I.S.)[113]. Envisageant l'hypothèse que ces données représentent un moyen potentiel de développer les techniques de profilage racial, il s'agit d'envisager dans quelles mesures elles pourraient être utilisées et si elles pourraient avoir un impact sur la politique américaine d'immigration. A terme, il serait pertinent d'envisager la mise en œuvre du principe de non-discrimination lors du traitement de ces données par les services américains, mais aussi européens, de l'immigration.

[112] SAVAGE, Charlie, « U.S. And EU Near Deal On Sharing Data », *International Herald Tribune*, 28 juin 2008.

[113] Anciennement *Immigration and Naturalization Service* (I.N.S.).