Données des voyageurs aériens

Pérez Asinari, María Veroníca; Poullet, Yves

Published in:
Journal des Tribunaux. Droit Européen

Publication date:
2004

Document Version
le PDF de l'éditeur

Données des voyageurs aériens : le débat Europe - Etats-Unis (*)

1 Introduction

Au lendemain des événements du 11 septembre 2001, les autorités américaines ont pris unilatéralement la décision d'imposer aux compagnies aériennes de fournir à l'administration douanière américaine soit un accès direct aux données concernant les passagers et les membres d'équipage volant vers, à partir de ou à l'intérieur des Etats-Unis (système *pull*) soit de permettre le transfert de telles données (système *push*). Ces décisions ont été contestées par les autorités européennes en ce qu'elles impliquent une violation des législations européennes sur la vie privée et la protection des données à caractère personnel, ces législations étant d'ordre public.

Notre réflexion suit les étapes suivantes. Une première partie [2] évoque le cadre législatif américain complexe et récent dans lequel les décisions relatives à la vérification des données des passagers aériens venant notamment d'Europe plus largement de l'étranger ont été prises. Une deuxième partie [3] s'interroge, dans un premier temps, sur les différents prescrits européens soit généraux soit spécifiques en matière de flux transfrontières dont l'Union européenne devait tenir compte pour analyser les flux réclamés par les exigences réglementaires américaines. Dans un second temps, la deuxième partie tente de répondre à la question : « Quelle disposition parmi toutes celles évoquées pouvait justifier *in casu* de tels flux? ». Enfin, sur la base de ces considérations, la troisième partie [4] passe en revue les actions entreprises par les différents acteurs : les autorités américaines, la Commission européenne, le Parlement, le groupe de l'article 29 et la commission belge de protection de la vie privée, avant de conclure.

2 Le cadre législatif américain

1. — Le contexte législatif

Directement après la tragédie du 11 septembre 2001, le gouvernement américain prit un grand nombre de mesures afin de combattre le terrorisme. Le « Patriot Act » (1) en est sans doute l'exemple le plus connu. Cependant, des législations plus spécifiques ont également été prises afin d'éliminer les risques créés par la menace terroriste.

Dans la sphère de l'immigration et de l'admission des étrangers, l'« Enhanced Border Security and Visa Entry Reform Act » (2) a été adopté le 14 mai 2002. Dans le domaine des transports aériens, les Etats-Unis prirent l'« Aviation and Transportation Security Act » (A.T.S.A.) (3) le 19 novembre 2001. Ces législations ont été suivies par certaines réglementations ou législations dites « secondaires », notamment le document « Passenger and Crew Manifests Required for Passengers Flights in Foreign Air Transportation to the United States », publié au *Registre fédéral* (Federal Register) le 31 décembre 2001 (4) et le « Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States », publié au *Registre fédéral* le 25 juin 2002 (5).

Le but principal de toutes ces législations est d'accroître la sécurité, de lutter contre le terrorisme et de créer ce que les autorités américaines appellent la « 21st Century Smart Border » (6), qui déplace les limites de l'Etat américain au-delà des frontières physiques territoriales. En vue d'atteindre cet objectif, le gouvernement et le Parlement ont donné un mandat très large à une nouvelle autorité publique : la Transportation Security Agency (T.S.A.). Cette autorité fait partie du département de la sécurité intérieure (7) et peut prendre toutes les mesures appropriées afin d'améliorer la sécurité aérienne.

Une des décisions les plus importantes qui ont été prises dans ce contexte est d'utiliser les technologies de l'information, particulièrement des outils d'analyse des risques, pour détecter les terroristes. Toutes les données transmises par les compagnies de transport aérien seront centralisées dans une base de données, gérée à la fois par le Bureau of Customs and Border Protection et l'Immigration and Naturalization Service. De plus, un programme informatique « Secure Flight Test Records » (S.F.T.R.) est en passe d'être créé pour évaluer les risques attachés à tous les passagers de vols domestiques avant qu'ils n'embarquent à bord (8).

2. — Les mesures

Les réglementations citées ci-dessus ont créé différentes obligations pour les transporteurs aériens, lesquels puisent aussi des informations dans différents systèmes de gestion de l'information, centralisés ou non.

« The Advanced Passenger Information System » (A.P.I.S.) traite toutes les données exigées de l'ensemble des compagnies de transport aérien et transmises par celles-ci. L'A.T.S.A. stipule ce qui suit :

« [1] *In general* — Not later than 60 days after the enactment of the Aviation and Transportation Act, each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to the Commissioner of Customs by electronic transmission a passenger and crew manifest containing the information specified in paragraph [2]. Carriers may use the advanced passenger information system established under section 431 of the Tariff Act of 1930 [19 U.S.C. 1431] to provide the information required by the preceding sentence.

» [2] *Information* — A passenger and crew manifest for a flight required under paragraph [1] shall contain the following information :

» — the full name of each passenger and crew member;

» — the date of birth and citizenship of each passenger and crew member;

» — the sex of each passenger and crew member;

» — the passport number and country of issuance of each passenger and crews member if required for travel;

» — the united States visa number or resident alien card number of each passenger and crew member, as applicable;

» — such other information as the Under Secretary, in consultation with the Commissioner

(*) Cet article est une adaptation et une mise à jour des articles suivants : M.V. Perez Asinari et Y. Poullet « The airline passenger data disclosure case and the E.U.-U.S. debate », *Computer Law & Security Report*, vol. 20, n° 2, 2004, pp. 98-116; et M.V. Perez Asinari et Y. Poullet « Airline passengers' data : adoption of an adequacy decision by the European Commission - How will the story end? », *Computer Law & Security Report*, vol. 20, n° 5, 2004, pp. 370-376. Les auteurs tiennent à remercier tout particulièrement Mlle V. Straetmans et M. C. Burton, étudiants au D.G.T.I.C., pour leur traduction et le professeur-docteur Cécile De Terwangne pour la précieuse aide apportée lors de l'élaboration de ce travail.

(1) 107th Congress, 24 octobre 2001.

(2) Public Law 107-173, 107th Congress, 14 may 2001.

(3) Public Law 107-71, 107th Congress, 19 novembre 2001.

(4) Departement of Treasury, Customs Service, (66 FR 67482) T.D. 02-01.

(5) Departement of Treasury, Customs Service, (67 FR 42710) T.D. 02-33.

(6) Voy. sur ce concept la déclaration faite par A. Hutchinson, sous-secrétaire à la sécurité des frontières et des transports au département américain de la sécurité intérieur, lorsqu'elle se réfère au système américain U.S. Visit comme partie d'un vaste système d'information qui fournira aux Etats-Unis des « frontières intelligentes » qui « expedites legitimate trade and travel, but stops terrorists in their tracks ». Ce système « will be based on visas that include biometric features such as fingerprints and photographs to permit identification of foreign visitors when they arrive. (...) Through this " virtual border " we will know who violates our entry requirements, who overstays or violates the terms of their stay, and who should be welcome again ». Ensuite, elle fit remarquer que ces initiatives ne doivent pas être considérées comme un moyen d'exclure les immigrants, « [i]mmigrants still search for the American Dream. And when they find it, all American benefit », extrait de « Hutchinson says new system provides America with smart border », site web de la mission U.S. en U.E., 19 may 2003, disponible à : http ://www.useu.be/Terrorism/USResponse/May1903USVISITSystem.html, dernière visite le 08/08/2003.

(7) Le T.S.A. a été créé sous l'A.T.S.A.

(8) Department of Homeland Security, Transportation Security Administration, [Docket n° T.S.A.-2004-19160] Privacy Act of 1974 : System of Records; Secure Flight Test Records. Department of Homeland Security, Transportation Security Administration, [Docket n° T.S.A.-2004-19160] Privacy Impact Assessment; Secure Flight Test Phase.

of Customs, determines is reasonably necessary to ensure aviation safety » (9).

Le paragraphe 4 établit que la liste des passagers et de l'équipage doit être transmise au service des douanes avant le décollage de l'avion vers les Etats-Unis (10).

Le paragraphe suivant réglemente l'accès aux P.N.R. : « [4] *Passenger name records* — The carriers shall make passenger name record information available to Customs Service upon request » (11).

Comme nous l'avons mentionné, certains textes ont été publiés au *Registre fédéral* afin de préciser ces législations. « The Interim Rule » du 31 décembre 2001 a par exemple étendu les données à fournir dans le manifeste (document de bord à communiquer), en ajoutant l'obligation de les transmettre électroniquement au service des douanes : « [3] [t]he foreign airport where each passenger began his air transportation to the United States; for each passenger and crew member destined to the United States, the airport in the United States where the passenger and crew member will process through Customs and Immigration formalities; and for each passenger and crew member transiting through the United States and not clearing through Customs and Immigration formalities, the foreign airport of final destination for the passenger and crew member (12).

En ce qui concerne le P.N.R., l'« Interim rule » du 25 juin 2002 prévoit, entre autres, que : « In order to readily provide Customs with such access to requested P.N.R. data, each air carrier must ensure that its electronic reservation/departure control systems correctly interface with the Customs data Center, Customs Headquarters » (13).

Il est clair que ces données ne doivent pas nécessairement être transférées mais être rendues accessibles en ligne.

« The Interim rule » que nous commentons ci-dessus, stipule, de façon purement illustrative, que certaines données personnelles concernant chaque passager peuvent être exigées par le service des douanes (14) :

» — Last name; first name; date of birth; adress(es); and phone number(s);

» — Passenger name record locator (reservation) number;

» — Reservation date (or dates, if multiple reservations made), or if no advance reservation made (" go show ");

» — Travel agency/agent, if applicable;

» — Ticket information;

» — Form of payment for ticket;

» — Itinerary information;

» — Carrier information for the flight, including but not limited to : carrier information for each segment of the flight if not continuous; the flight number(s); and date(s) of intended travel;

» — Seating; and

» — P.N.R. history » (15).

En fait, les données P.N.R. contiennent d'autres informations, certaines d'entre elles présentant un caractère sensible. Le P.N.R., par exemple, mémorise les différentes sortes de nourriture demandées par le passager pour le vol (ces aliments peuvent avoir des connotations philosophiques, religieuses ou liées à l'état de santé); il mentionne les installations spécifiques demandées pour un handicapé (16), etc. Il indique également le nom de la personne qui paie le ticket d'avion (société privée, association, université, administration publique, etc.) et précise même le compte interne par lequel le paiement est effectué. Le champ « Itinerary Information » inclut tous les services auxiliaires que le passager demande, que ceux-ci soient liés au vol ou soient accordés en dehors du vol à proprement parler (17).

Pour être complet, il faut mentionner un autre système mis en ouvre aux Etats-Unis : le système U.S. Visit (18). Celui-ci consiste en un scanning systématique des documents de voyage de chaque visiteur aux Etats-Unis. Des photographies et empreintes digitales sont systématiquement prises et les données ainsi obtenues sont comparées à des listes reprenant les personnes interdites d'entrée sur le territoire américain pour différentes raisons (terrorisme, crimes, entrées illégales, falsification de visas) (19). Ce système permet le traitement central des données personnelles, y compris certaines données basées sur la physionomie ou d'autres données biométriques (20) (aujourd'hui : photos digitales et empreintes; demain : reconnaissance faciale et *scanning* de l'iris) (21). En vue de faciliter ces opérations, les pays qui ne délivrent pas de visas sont obligés d'utiliser des passeports impossibles à falsifier comprenant des identificateurs biométriques et ce depuis août 2004. Ces données biométriques n'étant pas exigées des compagnies aériennes, il n'y a pas lieu de développer cet aspect dans le présent article.

Par ailleurs, le T.S.A. est autorisé non seulement à utiliser les données collectées a travers ces sources mais en outre à établir une « watchlist » des individus suspectés de présenter « un risque de piratage aérien ou de terrorisme ou une menace pour la sécurité du vol ou des passagers » (22). D'autre part, les différentes compagnies aériennes ont mis au point le « Computer Assisted Pre-Screening Program (C.A.P.P.S.) », un logiciel d'analyse des passagers, ayant pour but d'identifier les passagers par un *screening* avant leur embarquement.

L'annonce d'une version améliorée du C.A.P.P.S. (23), le C.A.P.P.S. II, a soulevé aux Etats-Unis et en Europe d'importantes objections qui ont dénoncé les risques insupportables pour la vie privée liés à ce système. Au vu de telles objections, le gouvernement américain en a interrompu le développement au profit d'un nouveau programme : le « Secure Flights Test Record » (24) lequel est en phase d'évaluation.

Toutes ces mesures affectent de manière significative les compagnies d'aviation (25), « responsables de traitement de données », qui opèrent depuis les pays étrangers. De plus, il est clair que ces mesures créent de nouveaux risques pour la protection des données personnelles d'origine européenne. Le transfert par

(9) Sec. 115. Passenger Manifest, § *c*; amendment à 49 U.S.C., 44909.

(10) L'« interim rule » du 31 décembre 2001 prévoit que ce transfert devrait être fait « not later than 15 minutes after the departure of the aircraft from the last foreign port or place », p. 67483.

(11) Sec. 115. Passenger Manifest, § *c*; amendment à 49 U.S.C., 44909

(12) Voy., p. 67483.

(13) Voy., p. 42710.

(14) Voy., p. 42711.

(15) Concernant cette dernière mention, il convient de préciser que l' « histoire du P.N.R. » contient les changements et suppressions faits au P.N.R. depuis sa date de création.

(16) Dans le système P.N.R., ces champs sont appelés S.S.R. (Special Service Request).

(17) Pour une description pratique du P.N.R., voy. : « Lesson : Passenger Name Record », Advanced Worldspan, disponible à : http://globallearningcenter.wspan.com/emealearningcenter/PDFs/Student%20Workbooks/210/1101%20P.N.R.%20Lesson.pdf, dernière visite le 10 octobre 2004. Voy. aussi : E. Hasbrouck « Total Travel Information Awareness », disponible à : http://hasbrouck.org/articles/travelprivacy.html, dernière visite le 10 octobre 2004. Dans cet article nous pouvons lire : « Passenger Name Record (P.N.R.'s) maintained by airlines, computerized reservations systems or " global distribution systems " (C.R.S.'s/G.D.S.'s), and travel agencies don't just contain flight reservations and tickets records. They include car, hotel, cruise, tour, sightseeing and theater ticket bookings among other types of entries. P.N.R.'s show where you went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a particular other person, they show whether you asked for one bed or two. Through departmental and project billing codes, business travel P.N.R.'s reveal confidential internal corporate and other organizational structures and lines of authority and show which people were involved in work together, even if they travelled separately. Particulary in the aggregate, they reveal trade secrets, insider financial information, and information protected by attorney-client, journalistic, and other privileges. Through meeting codes used for convention and other discounts, P.N.R.'s reveal affiliations even with organizations whose membership lists are closely-held secrets not required to be divulged to the government (...) ». Plus spécifiquement sur le P.R.N., voy., par le même auteur, « What's in a Passenger Name Record (P.N.R.)? », disponible sur : http://hasbrouck.org/articles/P.N.R..html; dernière visite le 10 octobre 2004.

(18) « D.H.S. deployed U.S.-V.I.S.I.T. at 115 airports and 15 major seaports on January 5, 2004 », See Electronic Privacy Information Center (E.P.I.C.), United States Visitor and Immigrant Status Indicator Technology, diponible sur : http://www.epic.org/privacy/us-visit/, dernière visite le 15 octobre 2004.

(19) Le Congrès a prévu 400 millions de dollars pour mettre le système au point.

(20) Pour une approche européenne sur les techniques de biométrie, voy. : groupe de travail de l'article 29 sur la protection des données, document de travail sur la biométrie, 1er août 2003, WP80.

(21) A propos de ceci, voy. le *fact sheet* auquel Hutchinson se réfère dans l'article déjà cité note 6 : « Hutchinson says... ».

(22) En fait, les documents obtenus par l'E.P.I.C. démontrent l'existence de deux listes : la « no fly watchlist » et la « selectee list » concernant les personnes soumises à des mesures de sécurité additionnelles. Le critère pour mettre un nom sur la liste reste secret. Voy. E.P.I.C. : « Documents show errors in T.S.A.'s " no fly " watchlist », avril 2003, disponible sur : http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html, dernière visite le 10 octobre 2004.

(23) Le premier C.A.P.P.S. fut crée après l'explosion à Lockerbie d'un jet PanAm.

(24) Voy., *supra* note 8.

(25) Des amendes sont prévues à l'encontre des compagnies aériennes si elles ne se soumettent pas aux différentes dispositions américaines.

les compagnies européennes de données liées aux passagers à destination des Etats-Unis répondant aux exigences du gouvernement américain doit être compatible avec les législations nationales applicables aux activités d'enregistrement des données des compagnies aériennes dans les pays européens où les passagers font leur réservation, achètent leur ticket, prennent l'avion, etc. Les exigences réglementaires américaines mettent en question la souveraineté des Etats européens en opérant largement au-delà des frontières américaines. Afin de justifier cette approche extraterritoriale, les autorités américaines ont développé un nouveau concept de leur propre souveraineté, celle-ci n'étant plus limitée à leur frontière physique : « But in the 21st Century, border security can no longer be a coastline, or a line on the ground between two nations. It's also a line of information in a computer, telling us who is in the country, for how long, and for what reason... In the 21st Century it is not enough to place inspectors at our ports of entry to monitor the flow of goods and people. We must also have a " virtual border " that operates far beyond the land border of the United States » (26).

Cette motivation de l'action américaine hors frontières avait aussi été invoquée dans le contexte du programme « Echelon » (27), lequel est un système anglo-américain de surveillance électronique des messages échangés par satellites. On rappelle que le système Echelon a également été critiqué par le Parlement européen en ce qu'il violait le droit fondamental européen au respect de la vie privée (28).

3

Le contexte législatif européen et la multiplicité des bases légales

La nature des effets extraterritoriaux des décisions américaines a provoqué de nombreuses réactions des autorités européennes (29). Nous les commenterons dans les paragraphes qui suivent. Nous nous attacherons donc, dans un premier temps, à décrire le cadre légal européen et communautaire concernant la vie privée et la protection des données personnelles dans le but de souligner, dans un deuxième temps, les fondements légaux de l'intervention européenne et les intérêts à protéger par cette intervention. Plus particulièrement, il importe de rechercher la base légale pour une régulation de tels flux de données transfrontières (F.D.T.).

1. — Le contexte légal européen et communautaire

Lorsqu'on analyse la législation applicable relative à la vie privée et à la protection des données, il faut prendre en considération une série d'instruments adoptés à différents niveaux de pouvoirs. Il est important de comprendre leurs différents champs d'application ainsi que leur pertinence dans le contexte décrit.

Parmi les instruments internationaux, la première source à prendre en considération est certes la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (30). La vie privée est un droit fondamental garanti à l'article 8 de ce texte. Cette disposition prévoit que :

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

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

Cette disposition a été largement interprétée par la doctrine, ainsi que par la Cour européenne des droits de l'homme (31).

Par ailleurs, le Conseil de l'Europe a, sur la base de l'article 8, adopté la Convention n° 108 « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » (32) et une série de recommandations sectorielles (33). Il convient de signaler que cette Convention n° 108 revêt une grande importance pour certains domaines d'application. En effet, on le verra plus loin, une directive européenne a été adoptée également dans cette matière (34). Son champ d'application est naturellement limité au premier pilier du droit communautaire, même si les Etats membres l'ont transposée dans des lois internes qui ont un champ d'application plus étendu, englobant des domaines non couverts par la directive. Pour ces domaines, c'est spécifiquement la Convention n° 108 qui sert de référence et doit être respectée. Alors que sur ces points particuliers, la C.J.C.E. ne peut intervenir, la Cour européenne des droits de l'homme pourra être saisie des cas de violation de l'article 8 de la C.E.D.H. au niveau national.

Au niveau de l'Union européenne, la Charte européenne des droits fondamentaux (35) a inclus dans son champ d'application non seulement le droit à la vie privée mais aussi le droit à la protection des données personnelles et considère ceux-ci comme deux droits distincts :

« article 7 : Respect de la vie privée et familiale

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

» article 8 : Protection des données à caractère personnel

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

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

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

Même si, pour l'heure, la Charte n'a pas d'effets juridiques contraignants, sa philosophie affecte les trois piliers du droit européen. La Charte reconnaît la nature de droits fondamentaux de la vie privée et de la protection des

(26) Voy. l'article « Hutchinson says new system provides America with " smart border " », *op. cit.*

(27) A propos d'Echelon, voy. le site web de la fédération américaine des scientifiques : http://www.fas.org/irp/program/process/echelon.htm (dernière visite le 10 oct. 2004) et l'article de Y. Poullet et J.-M. Dinant, « Le réseau Echelon existe-t-il? Que peut-il faire? Peut-on et doit-on s'en protéger? », publié par le comité belge de surveillance, 1999, pp. 13 et s., disponible sur : http://www.droit.fundp.ac.be/textes/echelonfr.pdf

(28) Voy., la résolution du Parlement européen, 5 septembre 2001 et le Working Paper of the European Parliament temporary Committee on the Echelon Interception System (Schmidt Report), disponible sur : http://fas.org/irp/program/process/europarl.draft.pdf, dernière visite 4 septembre 2003.

(29) Ainsi que des défenseurs des libertés civiles européennes. Voy., par ex., « Campaign against the illegal transfer of European travellers' data to the U.S.A. », organisée par l'E.D.R.I. (European Digital Rights), des informations sont disponibles sur : http://www.edri.org , dernière visite 15 octobre 2004.

(30) Convention de sauvegarde des droits de l'homme et des libertés fondamentales; signée à Rome, 4 novembre 1950. D. Yernault « L'efficacité de la Convention européenne des droits de l'homme pour contester le système " Echelon " », *in* Sénat et Chambre des représentants de Belgique, rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé « Echelon », 25 février 2002. Dans cet article, les auteurs étudient la nature de la C.E.D.H. : 1) en tant qu'instrument garantissant « l'ordre public européen », considéré comme un ensemble cohérent, comme l'a qualifié la Cour de Strasbourg en 1995; 2) en tant que traité international donnant une place à la responsabilité internationale de l'Etat; et 3) comme un traité international d'une nature particulière, à cause de son article 53, en vertu duquel les Etats adhérents reconnaissent sa suprématie légale vis à vis de tout autre instrument interne ou international qui serait moins protecteur des droits fondamentaux que la Convention elle-même.

(31) Cour eur. D.H., arrêt *Amann c. Suisse*, 16 févr. 2000; arrêt *Rotaru c. Roumanie*, 4 mai 2000; arrêt *P.G. et J.H. c. Royaume-Uni*, 25 septembre 2001, etc.

(32) Convention du Conseil de l'Europe n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janv. 1981. Disponible sur http://conventions.coe.int/treaty/fr/Treaties/Html/108.htm

(33) Parmi d'autres : recommandation n° R(99) 5 pour la protection de la vie privée sur internet (23 févr. 1999); recommandation n° R(97) 18 sur la protection des données personnelles collectées et traitées à des fins statistiques (30 sept. 1997); recommandation n° R(91) 10 sur la communication à des tierces parties de données personnelles détenues par des organismes publics (9 sept. 1991) (http://cm.coe.int/ta/rec/1991/f91r10.htm); recommandation n° R(90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes (13 sept. 1990); recommandation n° R (87) 15 réglementant l'usage de données à caractère personnel dans le secteur de la police.

(34) Directive 95/46/C.E. du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *J.O.*, n° L 281, 23 nov. 1995, pp. 0031-0050, ci après dénommée « la directive ».

(35) Pour le texte complet de la Charte des droits fondamentaux de l'Union européenne, *J.O.C.E.*, C 364/1, 18 déc. 2000. Voy. aussi, groupe de travail de l'article 29, recommandation 4/99 concernant l'inclusion du droit fondamental à la protection des données dans le catalogue européen des droits fondamentaux, 7 septembre 1999.

données et les individualise, mettant en exergue leur autonomie propre. Cela prouve que ce sont des concepts essentiels pour la politique européenne et qu'ils font partie de l'ordre public européen (36).

En outre, le projet de Traité établissant une Constitution européenne (37) prévoit en son article 50 que :

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

» La loi européenne fixe les règles relatives à la protection des personnes physiques s'agissant du traitement des données à caractère personnel par les institutions, les organes et les agences de l'Union, ainsi que par les Etats membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation des données.

» 2. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

2. — Bases légales afin de trouver une solution compatible avec les exigences américaines au niveau de la protection des données.

2.1. — *La directive 95/46/C.E. est-elle applicable au transfert des données personnelles des passagers?*

La législation secondaire régulant la protection de la vie privée et des données personnelles a été adoptée dans le contexte du premier pilier du droit européen à travers deux directives : une directive générale, la 95/46/C.E., et une directive particulière, la 2002/58/C.E. (38) concernant le transfert de données personnelles et la protection de la vie privée dans le secteur des communications électroniques.

La directive 95/46/C.E. a été adoptée avec l'objectif d'empêcher les Etats membres de restreindre ou d'interdire le libre transfert de données personnelles entre eux pour des raisons liées à la protection des droits et libertés fondamentaux des personnes physiques, et en particulier leur droit à la vie privée. Dans ce sens, le texte crée un ensemble de droits et obligations concernant le traitement des données personnelles, qui garantissent un standard élevé de protection des données personnelles.

Si le traitement des données personnelles (champ d'application matériel) (39) est effectué par les compagnies aériennes (champ d'application personnel, ces compagnies étant alors considérées comme des « responsables du traitement ») (40) dans l'Union européenne (champ d'application spatial) (41), alors la directive est applicable. Dès lors, si le responsable envisage de transférer des données à l'étranger, il faut se référer aux articles 25 et 26 de la directive qui règlent les flux transnationaux de données hors de l'Union... mais ce raisonnement est-il valable?

2.2. — *Au-delà du premier pilier?*

En effet, étant donné la nature particulière de ces flux de données transfrontières, qui ne sont pas effectués par les compagnies de leur plein gré mais comme conséquence d'une exigence expresse imposée par les autorités américaines dans le but d'identifier les individus qui peuvent représenter une menace pour la sécurité de l'aviation ou la sécurité nationale (42), il convient de se demander si les articles 25 et 26 de la directive sont les bases légales adéquates pour réglementer les flux transfrontières de données (F.T.D.) dans ce cas.

En fait, il faut envisager l'éventuel rôle que les deuxième et troisième piliers du droit européen devraient jouer dans ce contexte. A propos du deuxième pilier, l'article 12 du Traité sur l'Union européenne (T.U.E.) stipule que :

« 1. L'Union définit et met en œuvre une politique étrangère et de sécurité commune couvrant tous les domaines de la politique étrangère et de sécurité, dont les objectifs sont :

» — la sauvegarde des valeurs communes, des intérêts fondamentaux, de l'indépendance et de l'intégrité de l'Union, conformément aux principes de la Charte des Nations unies,

» — le renforcement de la sécurité de l'Union sous toutes ses formes,

» — le maintien de la paix et le renforcement de la sécurité internationale, conformément aux principes de la Charte des Nations unies, ainsi qu'aux principes de l'Acte final d'Helsinki et aux objectifs de la Charte de Paris, y compris ceux relatifs aux frontières extérieures,

» — la promotion de la coopération internationale,

» — le développement et le renforcement de la démocratie et de l'Etat de droit, ainsi que le respect des droits de l'homme et des libertés fondamentales ».

Dans la sphère du troisième pilier, l'article 29 T.U.E. stipule que :

« Sans préjudice des compétences de la Communauté européenne, l'objectif de l'Union est d'offrir aux citoyens un niveau élevé de protection dans un espace de liberté, de sécurité et de justice, en élaborant une action en commun entre les Etats membres dans le domaine de la coopération policière et judiciaire en matière pénale, en prévenant le racisme et la xénophobie et en luttant contre ces phénomènes.

» Cet objectif est atteint par la prévention de la criminalité, organisée ou autres, et la lutte contre ce phénomène, notamment le terrorisme, (...) ».

Si, afin de sauvegarder ces objectifs, il est nécessaire de prendre des accords avec un pays tiers, de tels accords n'auront pas pour base une directive. Si on utilisait la directive comme instrument d'harmonisation, la base légale serait l'ancien article 100 T.C.E. (actuellement 95 T.C.E.) mais celle-ci n'est prévue que pour les décisions concernant le marché intérieur. En d'autres termes, un accord sur la base des articles 24 ou 38 T.U.E., lesquels réglementent la conclusion d'accords internationaux lorsque cela est nécessaire pour l'exécution des dispositions du T.U.E., est-il ici nécessaire? En cas de réponse positive, le recours à la directive est-il exclu comme le laisse entendre l'article 3.2 de la directive?

A notre avis, même si ce type d'accords internationaux était nécessaire, l'application de la directive ne pourrait être exclue complètement car les entités dont on exige l'envoi des données personnelles de leurs passagers sont des entités privées ayant la qualité de responsables du traitement.

Néanmoins vu les caractéristiques complexes de la situation que nous commentons, des actions complémentaires devraient être prises par l'Union européenne et ce au-delà du premier pilier. En effet, on peut légitimement s'interroger : l'U.E. peut-elle accepter que les données d'origine européenne reçues par les autorités américaines puissent être utilisées, par exemple, comme un élément de preuve dans une procédure judiciaire dont pourrait résulter une condamnation à la peine de mort? (43). Ne faut-il pas, par ailleurs, exiger une « réciprocité » des transferts dans le cas des vols provenant des Etats-Unis vers l'Europe dans certaines circonstances?, etc. Ces problèmes, parmi d'autres, peuvent faire l'objet d'un accord international basé sur les articles 24 ou 38 du T.U.E., accord qui compléterait les réglementations prises en application de la directive 95/46/C.E. Cependant, comme nous le verrons (44), ce n'est pas ce type d'instruments internationaux qui a été choisi.

2.3. — *Quelle disposition de la directive 95/46/C.E. peut légitimer de tels flux transfrontières de données?*

Considérant que la directive doit être appliquée à cette matière, l'article 25.1 doit être retenu. Il établit le principe suivant : un Etat membre ne peut autoriser un transfert de données vers un pays tiers que si celui-ci assure un niveau de protection adéquat. Ce principe général est assoupli de différentes manières. Dans le cas des données de passagers exigées par les Etats-Unis, il est nécessaire d'analyser quel est le mécanisme légal qui convient pour permettre ce transfert de manière tout à fait licite. La notion de protection « adéquate », tient compte des risques que présente un transfert au vu notamment de la nature des données.

(36) Voy. sur ce point, nos réflexions publiées dans Y. Poullet, « Pour une justification des articles 25 et 26 de la directive européenne 95/46/E.C. en matière de flux transfrontières et de protection des données», *Communications commerce électronique*, 2003, n° 12, pp. 9-26.

(37) Soumis au président du Conseil européen à Rome le 18 juillet 2003.

(38) Directive 2002/58/C.E. du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.*, n° L 201, 31 juill. 2002. L'article 3, § 1er, stipule que : « La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté. ». Le système P.N.R. ne tombe pas dans cette catégorie. Sur le champ d'application de la nouvelle directive, voy. J. Dhont et K. Rosier " Directive vie privée et communications électroniques ", *Rev. Ub.- Droit des technologies de l'information*, n° 15, avril 2003, pp. 7-46. S. Louveaux et M.V. Perez Asinari « New European Directive 2002/58/C.E. on the processing of personal data and the protection of privacy in the electronic communications sector. Some initial remarks », *Computers and Telecommunications Law Review*, vol. 9, n° 5, 2003, pp. 133-138.

(39) Article 3 de la directive 95/46/C.E.

(40) Article 2, *d*, de la directive 95/46/C.E.

(41) Article 4.1, *a*, de la directive 95/46/C.E.

(42) Nous reviendrons sur les précisions apportées par le texte américain à propos du « but » et de la finalité de cette transmission, *infra*, 4, 2.1.

(43) Dans cette optique voy. l'article 13 de l'accord sur l'extradition entre l'Union européenne et les Etats-Unis, *J.O.C.E.*, L 181/27, 19 juill. 2003.

(44) Voy. *infra*, 4, 2.2 .

2.3.1. — *L'article 26.1 est-il applicable?*

L'article 26 de la directive prévoit des cas dans lesquels un transfert ou une série de transferts de données personnelles vers un pays tiers qui ne présente pas un niveau de protection adéquat peuvent être effectués. Ainsi, le transfert est possible lorsque :

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

» ou

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

» ou

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

» ou

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

ou (...) » (45).

L'utilisation de ces dérogations ne sera pas utile pour le cas sous analyse (46). Si nous prenons le paragraphe [*a*] par exemple, nous savons que le « consentement » doit être « librement donné » pour être considéré comme valide, or cela n'est pas le cas ici car les compagnies aériennes sont obligées d'envoyer les données. Le passager n'a dès lors pas de réel choix s'il entend voyager. En effet, même si les relations entre les compagnies aériennes et les passagers sont de nature strictement privée, où l'autonomie des parties prévaut, un passager ne peut donner son consentement à une chose que la compagnie n'est pas libre de faire ou de ne pas faire. En conséquence, la responsabilité des compagnies aériennes serait systématiquement évacuée (si le gouvernement fait une mauvaise utilisation des données transférées par les compagnies aériennes et qu'un sujet des données assigne en justice la compagnie, celle-ci se défendra en invoquant que le transfert résulte d'une obligation imposée par les pouvoirs publics et ne lui est donc pas imputable).

Si on analyse le paragraphe [*b*], on constate que le but du transfert n'est pas l'exécution du contrat.

Si on envisage, le paragraphe [*d*], son application mène aux règles énoncées à l'article 13.1 de la directive. Cette disposition stipule que :

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

» *a*) la sûreté de l'Etat;

» *b*) la défense;

» *c*) la sécurité publique;

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

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

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

» *g*) la protection de la personne concernée ou des droits et libertés d'autrui » (47).

Rappelons que les exceptions sont de stricte application et d'interprétation restrictive. La démarche, visant à utiliser cet article comme base légale pour permettre l'application de la dérogation contenue à l'article 26.1(*d*) apparaît vaine. Le transfert ne vise pas la « sûreté de l'Etat » d'un Etat membre de l'Union européenne, mais est imposé par les besoins de sûreté de l'Etat d'un pays tiers. Or, la défense de la sécurité d'un Etat tiers ne semble pas être la raison d'être de l'exception prévue par le texte européen.

2.3.2. — *L'article 26.2 est-il applicable?*

Une autre voie pour effectuer un transfert licite est l'utilisation de clauses contractuelles (48). Celles-ci peuvent être proposées par le responsable du traitement (*in casu*, les compagnies aériennes) aux autorités de l'Etat membre, afin d'être approuvées. Elles peuvent aussi être élaborées par ces autorités ou par la Commission européenne afin de créer des « clauses contractuelles types ». La Commission a ainsi proposé des clauses contractuelles types pour le transfert de données personnelles à des responsables de traitement situés dans des pays tiers, selon l'article 26.4 de la directive 95/46/C.E. (49), et les clauses contractuelles types pour le transfert de données personnelles à des gestionnaires de traitement établis dans un pays tiers (50).

Cette voie n'est pas non plus satisfaisante car *in casu* le transfert de données personnelles n'est pas opéré sur la base d'initiatives volontaires prises par l'exportateur ou l'importateur de données, mais plutôt sur la base d'une obligation de transfert de données résultant de la loi américaine qui l'impose aux compagnies aériennes.

2.3.3. — *Qu'en est-il de l'application des « Safe Harbor principles? »*

La directive prévoit que la Commission européenne peut estimer qu'un pays tiers assure un niveau de protection adéquat des données personnelles et adopter une décision constatant ce caractère adéquat. Il en résultera alors une libre circulation des données dans les circonstances mentionnées dans la décision de la Commission. Etant donné les importantes différences d'approche de la protection des données personnelles et de la notion de vie privée entre l'Europe et les Etats-Unis, il n'a pas semblé possible pour la Commission européenne, même après de longues négociations avec les Etats-Unis, de déclarer que le régime de ce pays assurait un niveau de protection adéquat. Une solution partielle a été trouvée par une décision de la Commission prise sur la base de l'article 25.6 déclarant que l'acceptation volontaire par un organisme américain des règles contenues dans un document connu sous le nom de « Safe Harbor » (51), document mis en place sous l'impulsion du département américain du Commerce, garantit un niveau adéquat de protection des données personnelles transférées à partir de l'Europe. Les « Safe Harbor Principles», lesquels sont complétés par des F.A.Q. (Frequently Asked Questions), ont été publiés par le département de Commerce. Plus de 450 entreprises y ont adhéré à l'heure présente.

L'adhésion à ces principes est volontaire, mais elle est uniquement possible pour les compagnies placées sous la juridiction de certains services publics qui contrôlent la loyauté de pratiques commerciales. Or, les compagnies aériennes européennes (52) ne se trouvent pas sous la juridiction de telles entités. En outre, seules des organisations américaines peuvent adhérer à ces principes. Par conséquent, les autorités publiques américaines qui collectent et traitent des données personnelles de passagers ne rentrent pas dans le champ d'application des « Safe Harbor Principles », qui, en l'occurrence, ne pourront dès lors pas être utilisés comme base pour légitimer les transferts exigés.

2.4. — ***Une question cruciale : article 4.1, (c), article 25.1 ou les deux?***

Avant d'aller plus loin dans les développements, une autre hypothèse est à analyser : quelle sorte de système est ou sera développé par les autorités américaines pour prendre connaissance des données des passagers? Même si nous avons mentionné, plus haut, l'existence de « transferts », il faut remarquer soit que le « transfert » (système *push*) est exigé pour alimenter certaines bases de données telles que l'A.P.I.S., soit pour « l'accès direct » au P.N.R. (système *pull*), comme nous l'avons déjà signalé (*supra* pt 2, 2).

Ces deux procédures d'obtention des données (*pull* ou *push*) vont chacune déterminer un régime légal différent. Pour le « système *push* », il faut appliquer les articles 25 et 26 de la directive. Par contre pour le « système *pull* »,

(45) article 26.1 de la directive.

(46) Le groupe de travail de l'article 29 a clairement expliqué qu'il est impossible d'utiliser ces dérogations comme principe général dans le contexte des transferts des données des voyageurs par les compagnies aériennes vers les Etats-Unis. Voy. son avis n° 6/2002 « transmission par les compagnies aériennes d'informations relatives aux passagers et membres d'équipage et d'autres données aux Etats-Unis », 24 oct. 2002, *W.P.* 66.

(47) Voy. aussi, les considérants 43, 44 et 45 de la directive.

(48) Article 26.2 de la directive.

(49) Décision de la Commission 2001/16/C.E. du 15 juin 2001 sur les clauses contractuelles types pour le transfert de données personnelles vers des pays tiers sous la directive 95/46/C.E., *J.O.C.E.*, L 181/19, 4 juill. 2001.

(50) Décision de la Commission 2002/16/C.E. sur les clauses contractuelles standards pour le transfert de données personnelles vers des responsables établis dans un pays tiers, sous la directive 95/46/C.E., *J.O.C.E.*, L 006, 10 janv. 2002, pp. 52-62.

(51) Décision de la Commission 2000/520/C.E. du 27 juill. 2000 conformément à la directive 95/46/C.E. du Parlement européen et du Conseil.

(52) On doit remarquer que non seulement les compagnies aériennes européennes sont soumises à la directive 95/46/C.E. mais aussi toute compagnie traitant des données personnelles en Europe.

l'article 4.1.c s'appliquerait dans la mesure où il faut bien reconnaître la présence des facteurs de rattachement décrits dans cette dernière disposition : « utilisation d'un équipement situé dans un Etat membre ». Par suite, l'entièreté des dispositions de la loi nationale transposant la directive est à respecter (53).

L'article 4.1, *c*, prévoit en effet que le droit national transposant la directive est applicable au traitement de données personnels lorsque : « 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 Etat membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté ».

Les autorités américaines peuvent-elles être considérées comme « responsables » du traitement au sens de la directive lorsqu'elles accèdent aux données P.N.R. stockées dans un système accessible en ligne situé sur le territoire d'un Etat membre? Nous savons que le responsable du traitement est la personne qui détermine les finalités et les moyens du traitement de données à caractère personnel (54). Nous pouvons considérer que le but des autorités américaines en accédant aux P.N.R. (l'accès est, selon la définition donnée par l'article 2, *b*, de la directive, une des opérations qualifiées de traitement) est la lutte contre le terrorisme, et que les moyens qu'elles décident d'utiliser pour traiter les données des passagers afin de combattre le terrorisme est le système P.N.R. Si on raisonne en ce sens, suivant la lettre de la directive et l'interprétation du groupe de travail de l'article 29, le responsable du traitement (le gouvernement américain) devrait désigner un représentant établi sur le territoire de l'Etat membre où l'équipement est situé (art. 4.2 de la directive), qui devra remplir les obligations inscrites dans les différentes législations nationales applicables (notification, information, mesures de sécurité).

La déclaration commune (*Joint Statement*) élaborée par la Commission européenne et le service des douanes américain après les discussions sur la transmission des P.N.R. stipule au point 5.1 :

« In accessing the P.N.R. data in the territory of the Community, US Customs undertakes to respect the principles of the Data Protection Directive » (55).

Néanmoins, nous ne pouvons que constater que la portée réelle de cette affirmation n'a pas été clairement perçue : il n'entre pas du tout dans les intentions américaines de désigner un représentant établi dans le territoire de l'U.E. (l'Etat membre pertinent), représentant qui remplirait les obligations mentionnées plus haut.

Nous verrons plus loin (*infra*, 4, 2.2) que cette question délicate est résolue par l'adoption d'un traité international entre la Commission et les autorités américaines.

4 Les actions entreprises

Peu après les décisions américaines concernant les données des passagers, certains membres des autorités européennes de protection des données ont exprimé leurs doutes et inquiétudes à propos de la conformité des demandes américaines aux exigences européennes en ce qui concerne la protection des données. Le groupe de travail de l'article 29 sur la protection des données prit donc position de sa propre initiative sur ce point (56).

1. — Premières mesures

Une déclaration commune (57) (*Joint Statement*) a été signée entre la Commission européenne et le service des douanes américain, à la suite des pourparlers officiels ayant eu lieu à propos de la transmission des P.N.R. Certains engagements furent réclamés des autorités américaines dans le but de satisfaire à la directive sur la protection des données. De plus, la pleine application du « Freedom of Information Act (F.O.I.A.) » aux données collectées par les autorités américaines dans le but d'assurer aux personnes concernées un accès à leurs données. Par ailleurs, certaines limites à la transmission des données P.N.R. par les autorités douanières américaines et le T.S.A. aux autres administrations américaines ont été fixées sous la pression européenne.

Au-delà de ces points d'accord minima, il a été expressément prévu que d'autres « garde-fous » seraient proposés par les Etats-Unis à travers la conclusion d'accords supplémentaires, de façon à ce qu'une protection adéquate puisse être offerte aux données personnelles d'origine européenne et que la Commission européenne puisse prendre une décision sous l'article 25.6 de la directive (58).

La base légale de cette position commune a été sérieusement mise en cause par S. Rodota, président du groupe de travail de l'article 29 dans une lettre du 3 mars 2003 (59) adressée au président du comité du Parlement européen sur les droits et libertés des citoyens.

Le Parlement européen s'exprima également sur cette question. Il en résulte un document (60) mettant en cause non seulement le manque de protection adéquate offerte par le système réglementaire américain mais également une critique sévère adressée à la Commission européenne dans son rôle de gardienne des Traités et du droit communautaire : « It needs to verify whether there is a real basis in US law to justify access to reservation systems data or whether this is an overbroad interpretation on the part of the present Administration (...); it is continuing to postpone the verification of the US legislation required under article 25 of directive 95/46/C.E. (...); last but not least, it is failing to provide information to the public, who should be the first to know what is being done with information about them; (...) » (61).

2. — Développements récents

2.1. — *Les nouvelles « déclarations d'engagement » du Bureau of Customs and Border Protection (C.B.P.)*

Les premières « déclarations d'engagement (62) (*Undertakings*) » du C.B.P. furent critiquées par le groupe de travail de l'article 29 concernant la protection des données à caractère personnel (63), comme n'atteignant pas « un niveau de protection adéquat ».

(53) Le groupe de travail de l'article 29 sur la protection des données à caractère personnel partage le même point de vue sur ce problème particulier. Voy., groupe de travail de l'article 29 sur la protection des données à caractère personnel, avis 6/2002 sur la « Transmission par les compagnies aériennes d'informations relatives aux passagers et membres d'équipage et d'autres données aux Etats-Unis », 24 octobre 2002, *W.P.* 66, p. 7; groupe de travail de l'article 29 sur la protection des données à caractère personnel; avis 4/2003 sur le « Niveau de protection assuré aux Etats-Unis pour la transmission des données passagers », 13 juin 2003, *W.P.* 78, p. 7. Pour un éclaircissement du problème de la loi applicable voy. : groupe de travail de l'article 29 sur la protection des données à caractère personnel; document de travail sur « l'étendue international de la législation européenne sur le traitement des données à caractère personnel par des non-Européens sur Internet via des sites web », 30 mai 2002, *W.P.* 56. Voy. aussi, pour l'application de l'article 4.1, *c* : M.-H. Boulanger et C. de Terwangne, « Internet et le respect de la vie privée », in *Internet face au droit*, *Cahiers du Centre de recherches informatique et droit*, n° 12, 1997, p. 211.

(54) Article 2, *d*, de la directive.

(55) L'annexe à la position commune ajoute que : « The United States Customs Service represents that : by legal state (title 49, United States Code, section 44909, *c*, 3) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49, *b*), air carriers operating passenger flights in foreign air transportation to, from or through the United States, must provide with electronic access to P.N.R. data contained in the automated reservation/departure control systems (" reservation systems ") »; dans le paragraphe suivant, l'idée d'« access » est confirmée par la suite du texte : « With regard to the P.N.R. data which Customs accesses directly from the air carrier's reservation systems, Customs will only view P.N.R. data concerning persons whose travel includes a flight into, out of or through the United States; Customs will access air reservation systems as an accommodation to the air carriers to obviate the need for costly technical changes required to allow the air carriers to transmit the data to Customs ».

(56) Groupe de travail de l'article 29 sur la protection des données à caractère personnel, avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et membres d'équipage et d'autres données aux Etats-Unis, 24 oct. 2002, *W.P.* 66,

(57) European Commission - U.S. Customs talks on P.N.R. transmission, Joint Statement, Bruxelles, 17/18 février 2003, disponible sur : http://europea.eu.int/comm/external_relations/us/intro/pnr.htm

(58) A plus long terme, l'ensemble des parties pensent qu'il est nécessaire d'avoir un accord multilatéral sous l'égide de l'Organisation internationale de l'aviation civile (O.I.A.C.).

(59) La lettre rappelle que les autorités nationales de protection des données ne sont pas libres d'appliquer ou non la législation de protection des données et qu'« il n'a pas encore été clarifié comment l'accord pourrait fournir une base légale solide pour justifier une exception au principe ».

(60) Parlement européen, Motion pour une résolution sur le transfert des données à caractère personnel par les compagnies aux services américains de l'immigration, 6 mars 2003, B5-0000/2003.

(61) Parlement européen, Motion pour une résolution...., p. 3.

(62) Déclarations d'engagement du bureau des douanes et de la protection des frontières, disponible sur : http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78-pnrf-annex_en.pdf

(63) Voy. le groupe de travail de l'article 29 sur la protection des données; avis 6/2002 groupe de tra-

Les nouvelles « déclarations d'engagement » (64) sont le résultat de négociations entre la Commission européenne et le C.B.P.; elles fixent essentiellement les principes de contenu et de mise en œuvre de la protection, principes qui devront être respectés afin d'atteindre un niveau de protection adéquat et de permettre dès lors une « décision d'adéquation » (65).

Les nouvelles « déclarations d'engagement », qui contiennent quarante-huit points, fixent en particulier les principes suivants :

— *Principe de finalité déterminée :* le point [3], sous le titre « Utilisation des données de P.N.R. par le C.B.P. », énonce que :

« Le CBP utilise les données de P.N.R. 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 ».

Malgré cette définition claire des objectifs, on observe que les points (34) et (35) de la déclaration d'engagement, sous le titre « transmission de données de P.N.R. à d'autres autorités gouvernementales » élargissent les objectifs :

[34] « Aucune disposition de la présente déclaration d'engagement ne peut empêcher l'utilisation ou la divulgation de données de P.N.R. aux autorités gouvernementales compétentes lorsque cette divulgation est essentielle à la protection des intérêts vitaux de la personne concernée ou d'autres personnes, notamment dans le cas de risques sanitaires graves. Les divulgations effectuées dans ce contexte obéissent aux mêmes conditions que celles applicables aux transferts qui sont décrites aux paragraphes 31 et 32 »; et [35] « Aucune disposition de la présente déclaration d'engagement ne peut empêcher l'utilisation ou la divulgation de données de P.N.R. dans le cadre d'une procédure pénale ou au titre d'autres exigences prévues par la loi (...) ».

— *Principe de qualité et de proportionnalité des données :* les trente-huit données dont la communication étaient initialement prévues furent réduites à trente-quatre. En ce qui concerne les limites de temps, différentes périodes sont prévues. Le C.B.P. pourra garder les P.N.R. durant trois ans et six mois. Dans le cas où les données sont accessibles manuellement, la période de conservation sera de huit ans.

— *Principe de transparence :* le point [36] affirme : « Le C.B.P. portera à la connaissance des passagers les exigences relatives aux P.N.R. et tous les éléments liés à leur utilisation, par exemple par la publication sur le site internet du C.B.P. ou dans des dépliants à l'intention des voyageurs, de renseignements à caractère général concernant l'autorité responsable de la collecte des données, la finalité de la collecte, la protection des informations, le partage des données, l'identité du fonctionnaire responsable, les procédures de recours et les points de contact où soumettre les questions ou problèmes éventuels ».

— *Principe de sécurité :* les mesures adoptées sont décrites aux points [16] à [23] et comprennent, entre autres, l'utilisation d'un système intranet fermé et crypté de bout en bout du C.B.P. et le fait qu'aucune autre agence étrangère, fédérale, étatique ou locale ne dispose d'un accès électronique direct aux données de P.N.R. via les bases de données du C.B.P. En outre, la base de données du C.B.P. est accessible uniquement en lecture et, par ailleurs, seuls certains fonctionnaires, agents ou sous-traitants en technologies de l'information du C.B.P., peuvent accéder aux données de P.N.R. sous certaines conditions : cet accès s'opère sous la supervision du C.B.P. et n'est possible que pour des personnes qui ont satisfait à une enquête concernant leurs antécédents, qui disposent d'un compte actif et protégé par un mot de passe dans le système informatique du C.B.P. et qui sont officiellement habilités à examiner les données de P.N.R.

— *Principe de l'accès et de la rectification :* le point [37] stipule que : « Les demandes émanant des personnes concernées (aussi dénommées " demandeurs au premier chef ") et visant à obtenir une copie des informations de P.N.R. les concernant figurant dans les bases de données du C.B.P., sont traitées conformément à la loi sur la liberté de l'information (...) ». Ensuite, le point [39] dispose que « Le C.B.P. s'engage à rectifier des données à la demande de passagers ou de membres d'équipage, de compagnies aériennes ou d'autorités chargées de la protection des données d'Etats membres de l'Union européenne dans la limite du mandat conféré par la personne concernée lorsque le C.B.P. établit que de telles données figurent dans sa base de données et juge la modification justifiée et étayée par les renseignements nécessaires. Le C.B.P. informera toute autorité désignée ayant reçu les données de P.N.R. en question de toute rectification de celles-ci ».

— *Principe des limites de la transmission de données de P.N.R. à d'autres autorités gouvernementales :* le point [29] prévoit que : « Le C.B.P., à sa discrétion, ne transmettra de données de P.N.R. à d'autres autorités gouvernementales de répression ou de lutte contre le terrorisme, qu'elles soient nationales ou étrangères, qu'au cas par cas, aux fins de prévenir ou de combattre les crimes visés au paragraphe 3 (...) ».

— *Principe de non-traitement des données sensibles :* le C.B.P. déclare qu'il n'utilisera pas les « données sensibles » (...) du P.N.R. (...). Cette déclaration n'est accompagnée d'aucune garantie et la notion de données sensibles n'est pas définie.

— *Principe de l'existence de mécanismes de mise en œuvre :* au point [41] il est affirmé : « Lorsqu'une plainte ne peut être tranchée par le C.B.P., il convient de l'adresser, par écrit, au haut responsable de la protection de la vie privée auprès du ministère de la Sécurité intérieure, qui examinera la situation et s'efforcera de résoudre le litige ».

Le point [42] stipule : « De plus, le bureau de la protection de la vie privée du ministère de la Sécurité intérieure examinera en urgence les plaintes qui lui seront adressées par les autorités chargées de la protection des données dans les Etats membres de l'Union européenne pour le compte d'un résident de l'Union européenne, dans la mesure où ce résident a autorisé ces autorités à agir pour son compte et estime que sa plainte en matière de protection des données concernant les P.N.R. n'a pas été traitée à sa satisfaction par le C.B.P., conformément aux paragraphes 37 à 41, ou par le bureau de la protection de la vie privée du ministère de la Sécurité intérieure. Ledit bureau rendra compte de ses conclusions et de toute mesure à l'autorité ou aux autorités concernées (...) ».

D'autres points controversés sont abordés par le document : *C.A.P.P.S. II* : les nouvelles « déclarations d'engagement » établissent que le C.B.P. peut transférer les données P.N.R. de manière brute à l'administration de la sécurité et du transport pour tester le programme C.A.P.P.S. II. Il convient de signaler que ce programme présentait tant d'atteintes aux droits des individus qu'il a finalement été abandonné par les autorités américaines.

Engagement de réciprocité : dans l'éventualité où l'Union européenne adopte un système analogue pour les données des passagers, le C.B.P. *s'engage à encourager* les compagnies aériennes établies aux Etats-Unis à coopérer.

Absence de création de droits ou de précédents : le point [47] dispose, de manière assez contradictoire avec l'essence même de ce que constitue un engagement, que : « 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 ».

2.2. — *L'action de la Commission européenne*

Sur la base de ces nouveaux engagements américains, la Commission a rédigé une décision sur la protection adéquate des données à caractère personnel présentes dans les P.N.R. et transmises par les compagnies aériennes au bureau américain des douanes et de la protection des frontières.

Cette décision proclame le « caractère adéquat » de la protection découlant des nouvelles « déclarations d'engagement » liées au transfert de données par les compagnies aériennes aux Etats-Unis. La base légale de cette décision consacrant la protection adéquate offerte par ces « déclarations » est l'article 25.6 de la directive 95/46/C.E.

Parallèlement, la Communauté européenne a signé un accord avec les Etats-Unis sur le traitement et le transfert des données P.N.R. par les transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (66).

La base légale de cet accord est l'article 300(2) du Traité des Communautés européennes. Les

vail de l'article 29 sur la protection des données à caractère personnel; avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et membres d'équipage et d'autres données aux Etats-Unis, 24 octobre 2002, opinion n° 66. Groupe de travail de l'article 29 sur la protection des données à caractère personnel; avis 4/2003 sur le niveau de protection assuré aux Etats-Unis pour la transmission des données passagers, 13 juin 2003, opinion n° 78.

(64) Les nouvelles déclarations d'engagements sont annexées à la décision de la Commission sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers P.N.R. des passagers aériens transférés aux Etats-Unis.

(65) Les principes qui doivent être respectés se trouvent dans : groupe de travail de l'article 29, document de travail « Transfert des données à caractère personnel aux pays tiers : application des articles 25 et 26 de la directive européenne », 24 juill. 1998, *W.P.* 12.

(66) Bruxelles, 17 mars 2004, COM(2004)190 final, 2004/00645 C.N.S., disponible sur http://europa.eu.int/euro- lex/en/com/pdf/2004/com/2004_0190en01.pdf

raisons d'adopter un tel instrument sont doubles : [1] l'accès direct des autorités américaines aux bases de données P.N.R. situées en Europe implique l'exercice de la souveraineté des Etats-Unis sur le territoire de l'Union, ce qui nécessite un consentement explicite de l'Union européenne; [2] L'article 7 de la directive 95/46/C.E. établit une liste restrictive des circonstances dans lesquelles le traitement de données à caractère personnel peut avoir lieu (67).

L'accord déclare que le C.B.P. peut accéder électroniquement aux données P.N.R. provenant des systèmes de contrôle de réservations et de départs des transporteurs aériens situés sur le territoire des Etats membres de la C.E., dans le respect strict de la décision d'adéquation évoquée ci-avant, mais seulement jusqu'à ce qu'un système satisfaisant de transmission soit mis en place.

Par ailleurs, cet acte juridique, ce Traité international, crée, pour les compagnies aériennes une obligation légale de traiter les données P.N.R. en réponse aux exigences réglementaires américaines. Dès lors, cette obligation légale, née de l'accord euro-américain, légitime les communications de données exigées; l'article 7, *c*, de la directive 95/46/C.E. considère en effet que le traitement est légitime s'il exécute la « loi », en l'occurrence le Traité signé par les autorités européennes.

2.3. — *La réaction du Parlement européen*

Le Parlement européen a exprimé son désaccord à l'égard des initiatives prises par la Commission (68). Il avait demandé à la Commission de retirer la décision d'adéquation (quand elle était encore à l'état d'avant-projet). Quant au projet d'accord, le Parlement n'approuva pas la conclusion de celui-ci. Il chargea son président de se rendre au Conseil afin de s'y opposer et de s'abstenir de le conclure jusqu'à ce que la Cour de justice donne son avis sur la compatibilité avec le Traité au regard de l'article 300[6] de T.C.E.

D'une part, la majorité du Parlement européen a rejeté l'accord signé par la Commission comme étant un *light international agreement* étant donné que, le Parlement n'a été que consulté, son avis n'étant pas juridiquement contraignant dans ce cas alors que selon le Parlement, la matière de l'accord exigeait l'approbation par le Parlement.

En effet, le Parlement européen, a estimé que l'instrument choisi par la Commission européenne, c'est-à-dire une décision unilatérale de sa part n'était pas appropriée lorsqu'il est question de limiter un droit fondamental. En somme, le Parlement a remis en cause l'option choisie par la Commission.

D'autre part, l'avant-projet de décision d'adéquation fut critiqué par le Parlement européen pour différentes raisons : ainsi, selon le Parlement, cette décision se fondait sur des engagements américains de nature purement administrative. En outre, le contenu des engagements devait, de l'aveu même des autorités américaines et de la Commission, être encore amélioré, en particulier, relève le Parlement, à propos de points sensibles tels que la liste des crimes graves pour lesquels des demandes additionnelles peuvent être adressées, la liste des autorités et agences qui peuvent accéder ou obtenir les données P.N.R. et les conditions de protection des données que les tiers devraient respecter

2.4. — *L'avis du groupe de travail de l'article 29 sur la protection des données à caractère personnel*

Le groupe de travail a rendu nombre d'avis depuis que les négociations avec le C.B.P. ont commencé (68*bis*). Le troisième avis fait allusion aux nouvelles déclarations d'engagement (annexés à la décision de la Commission). Le groupe de travail est favorable à la « Sunset Clause » du point [46], qui stipule que les déclarations d'engagement s'appliqueront pour une durée de trois ans et demi et que pour l'étendre, de nouvelles discussions seront nécessaires. Il accepte aussi la procédure de révision prévue au point [43]. Cette procédure doit être effectuée une fois par an par le C.B.P. conjointement avec le ministère de la Sécurité intérieure et la Commission européenne, assistée des représentants des autorités répressives européennes et/ou les autorités de protection des données des Etats membres de l'Union européenne.

Néanmoins, l'avis insiste sur plusieurs points qui doivent encore être clarifiés pour obtenir un cadre valable pour le transfert des données P.N.R.. En particulier, parmi d'autres problèmes, le groupe de travail considère que :

1) même si sa formulation a été améliorée, le principe de finalité présente encore un certain flou, spécialement l'expression « autres crimes graves »;

2) la réduction de la liste des catégories de données P.N.R. et ce de trente-huit à trente-quatre catégories ne représente qu'une mince avancée;

3) le traitement des données sensibles est toujours problématique, surtout à propos du contenu du *free text fields* dont l'effacement devrait avoir lieu en Europe, avant que les données ne soit transférées;

4) la période de détention des données déjà réduite par rapport à la première version des engagements américains fut encore considérée comme disproportionnée;

5) une identification précise des autres organes publics américains autorisés à recevoir les données est requise;

6) les exceptions qui peuvent être opposées aux personnes concernées par les données et désireuses d'accéder à leurs données sont définies de manière trop large ou trop floue.

2.5. — *L'opinion de l'autorité belge de protection des données (commission belge de la protection de la vie privée)*

La Commission belge de la protection de la vie privée a récemment publié un avis (69) à la suite du dépôt d'une plainte par deux citoyens concernant la transmission de leur données à caractère personnel (P.N.R. et A.P.I.S.) par des compagnies aériennes (Delta Airlines, United Airlines et Continental Airlines) vers les Etats-Unis à l'occasion de différents vols en partance de Belgique.

L'autorité belge analyse les principes applicables et observe que le principe de finalité, le principe d'information et les règles concernant les flux transfrontières n'avaient pas été respectées par les compagnies.

En ce qui concerne le principe de finalité, la Commission observe que les données des passagers ont été collectées et traitées en exécution des obligations contractuelles imposées pour effectuer le transport des passagers. Par contre, la transmission de ces données aux autorités américaines va au-delà de ce but. De plus, le fait que l'obligation de transmission est prévue par la législation américaine n'en fait pas une obligation légale au regard du droit européen. Cette obligation ne peut dès lors être considérée comme une base valable pour le traitement (la transmission dans ce cas) des données. Il en sera ainsi jusqu'à ce que le droit européen crée une telle obligation (70).

Concernant le respect de l'obligation légale d'informer la personne concernée, l'autorité belge de protection des données a vérifié et constaté que deux des compagnies n'avaient pas informé les passagers que leurs données seraient transférées aux autorités américaines. La troisième compagnie l'avait fait mais cette information fut considérée comme minimale, étant donné que la compagnie n'avait pas spécifié à qui les données seraient transférées ni les buts de ce transfert. De plus, la méthode d'information n'était pas suffisamment explicite car l'information était intégrée aux conditions générales et n'était donc disponible que sur demande par internet (70*bis*).

Le dernier point analysé porte sur la conformité avec les règles relatives aux flux transfrontières de données. L'avis fait référence au fait que les Etats-Unis ne pouvaient se prévaloir à l'époque d'une décision affirmant que leur situation réglementaire garantit une protection adéquate. Et puisque, à l'estime de la Commission belge, il n'existe aucune autre base légale en droit belge pour légitimer le transfert dans le cas soumis, le transfert a été effectué de manière illégale (71).

(67) Voy., Parlement européen, rapport sur la proposition d'une décision du Conseil sur la conclusion d'un accord entre l'Union européenne et les Etats-Unis sur le traitement et le transfert des données P.N.R. par les compagnies aériennes au bureau des douanes et de la protection des frontières du ministère de la sécurité intérieure (COM[2004]190-C5-0162/2004-2004/0064[C.N.S.]), Commission sur les droits et libertés des citoyens, justice et affaires intérieures, rapporteur : Johanna L.A Boogerd-Quaak, 7 avril 2004.

(68) *Ibid.*, Parlement européen, résolution sur l'avant-projet de décision de la Commission relatif au niveau de protection adéquat requis pour les données personnelles contenues dans le « Passenger Name Records » (P.N.R.s) transférées au bureau des douanes et de la protection des frontières (2004/2011[INI]).

(68*bis*) Le dernier avis (avis 8/2004) adopté le 30 septembre 2004 concerne l'information des passagers concernant le transport des dossiers passagers.

(69) Avis n° 48/2003/A.N.O. du 18 décembre 2003. Objet : Plaintes relatives à la transmission des données à caractère personnel par certaines compagnies aériennes vers les Etats-Unis.

(70) Dans une telle hypothèse, le traitement sera fondé sur l'article 7, *c*, de la directive. Voy. le raisonnement déjà tenu sur ce point par la Commission européenne.

(70*bis*) Le contenu et les modalités d'information des passagers sont désormais « fixés » par l'avis 8/2004 adapté le 30 septembre 2004 par le groupe dit « de l'article 29 ». Cet avis prévoit une « brève note d'information » et des « F.A.Q. ».

(71) Il est à noter que l'avis de la Commission belge précédait la conclusion de l'accord entre la Commission et les autorités américaines qui donne une base légale légitimant le transfert (*supra*, 4, 2.2.)

3. Questions de fond et de forme

Il est évident qu'il subsiste encore bien des points de controverses à clarifier et à régler dans cette matière complexe et sensible. Une partie de ces controverses concerne le contenu des instruments de négociations (questions de fond). Ces questions ont non seulement trait au respect des principes d' « adéquation », mais aussi à d'autres aspects qui nécessitent de plus amples discussions comme le problème de la souveraineté de l'U.E. et de ses Etats membres, problème déjà signalé dans le contexte de l'affaire *Echelon* (72). D'autres questions controversées concernent les formalités et bases légales qui doivent être utilisées (questions de forme) pour atteindre un accord international licite. Quelques mots à ces propos avant de conclure.

3.1. — *Questions de fond*

Nous ne reprenons pas ici les reproches adressés par le groupe de travail de l'article 29 au projet de décision d'adéquation présenté par la Commission. Ces critiques ont déjà été exposées plus haut (*supra*, 4, 2.4).

Par contre, il convient d'évoquer la question de la réciprocité des engagements euro-américaines, même si ce point ne relève pas de la décision relative au niveau adéquat de la protection assurée par le pays tiers. Dans une perspective de droit international public l'exigence de réciprocité est importante car cela représente un signe de bonne foi et d'engagement mutuel pour les Etats qui s'interdisent d'exiger d'autrui ce qu'ils ne sont pas prêts à voir exiger d'eux-mêmes.

Cependant, *in casu*, le principe de réciprocité reconnu dans les nouvelles « déclarations d'engagement » et cité *supra* 4, 2.1. *in fine* ne semble pas suffisamment garanti. Le texte de l'engagement contenu dans le point [45] apparaît bien léger et atteste du manque de sérieux de l'engagement américain. En réalité, il n'y a pas de réciprocité. Un engament réciproque serait un engagement dans lequel les autorités américaines endosseraient la responsabilité d'imposer à leurs compagnies aériennes pour les voyageurs à destination de l'Europe ou en transit via l'Europe une obligation légale telle que celle que l'U.E. impose dans son territoire par l'adoption de l'accord.

3.2. — *Questions de « forme »*

La question de la validité de la base légale du Traité passé entre la Commission et les autorités américaines est aussi passablement complexe. Le problème de la transmission des données P.N.R. concerne différents « niveaux » ou « piliers » du droit européen. Il en résulte une insuffisance à la fois de la base légale traditionnellement utilisée pour les flux transfrontières : la décision d'adéquation visée par l'article 25.6 et à la fois de l'instrument juridique utilisé en l'occurrence à savoir l'accord international signé par la Commission.

La directive 95/46/C.E. est en effet une directive du premier pilier. Or, dans le cas du transfert des données des passagers, la solution doit garantir aux compagnies aériennes que le transfert fait dans ce contexte est légal ce qui ne peut exister que si une « loi » européenne légitime ce transfert. On comprend dès lors le recours à la solution de l'accord international. En outre, la solution qui légitimera ces flux transfrontières d'un type bien particulier doit garantir la validité d' un transfert des données à des administrations publiques étrangères accompli dans le but de combattre le terrorisme et de veiller au respect de la loi américaine sur l'immigration, ce qui excède notoirement le champ d'application d'une directive du premier pilier. Ceci correspond, au niveau européen, à une matière de troisième pilier, ce qui remet en cause la compétence de la Commission à agir en la matière et ce sur simple avis du Parlement européen.

Sans doute, le concept de « protection adéquate » est également d'application, selon nous, dans le cadre du troisième pilier. Le protocole additionnel à la Convention n° 108 du Conseil de l'Europe concernant les autorités de contrôle et F.D.T. (73) est applicable au troisième pilier. Ce protocole règle explicitement la question du transfert, y compris vers les autorités d'un Etat tiers, dans son article 2.1 : « Chaque partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas partie à la Convention ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré ».

D'autres instruments du troisième pilier prévoient aussi une protection adéquate pour les F.D.T. Ainsi, l'article 18 de la Convention Europol stipule :

« 1. Europol peut sous les conditions définies au paragraphe 4 communiquer les données à caractère personnel qu'il tient d'Etats tiers ou d'organes tiers dans le sens de l'article 10 [4], où : (...);

» 2. Un niveau de protection adéquat des données est assuré dans ce pays ou cet organe (...) ».

Une fois posée l'application du principe de protection adéquate dans le troisième pilier, on note que, même si le document de travail n° 12 du groupe de l'article 29 qui détermine les principes de protection adéquate a été élaboré dans le contexte de la directive 95/46/C.E., les principes y décrits devraient également être respectés dans le cadre du troisième pilier. Peut-être, faudrait-il mieux définir la base légale pour la recherche d'une solution présentant un niveau de protection adéquat tel que discuté dans ce texte. Cependant, l'adoption de solutions tirées du troisième pilier aurait nécessité de longs débats et ainsi prolonger une situation où les données auraient été transférées sans base légale et sans garantie de protection.

5 Conclusions

Il n'est pas encore possible de conclure de manière définitive le débat concernant le transfert des données des passagers, même si la décision d'adéquation prise par la Commission européenne et l'accord U.E. - Etats-Unis conclu tout récemment se présentent apparemment comme un dénouement heureux des débats et polémiques soulevés par la décision unilatérale américaine. La parole a été donnée à la Cour de justice européenne dont l'intervention a été souhaitée par le Parlement vu le caractère sensible de ce qui se joue.

Il est évidemment regrettable que des données personnelles aient été communiquées aux autorités américaines en violation des lois nationales des Etats membres, sans aucun cadre légal pour réglementer cette situation anormale.

L' affaire des P.N.R. illustre certes la dérive sécuritaire à laquelle cède la plus puissante démocratie du monde. Elle démontre clairement que nos frontières n'ont plus de réelle signification dans un monde virtuel où le contrôle douanier et policier américain débute au moment de l'accès en territoire européen à des données collectées au départ pour une finalité tout autre. Sans doute, cette réalité oblige l'Union européenne et ses Etats membres à se montrer vigilants dans la protection des libertés de leurs citoyens vis à vis de puissances situées au-delà de leurs frontières.

A cet égard il n'est pas évident que les seules dispositions des articles 25 et 26 de la directive 95/46/C.E. suffisent. Le cas des P.N.R. illustre le besoin d'une réflexion sur la nécessité de définir à propos des activités du troisième pilier des principes sans doute similaires à ceux développés à propos de la notion de « protection adéquate » de l'article 25. On pourrait, de même imaginer qu'un Traité international constitue par analogie des « clauses contractuelles » appropriées aptes à garantir l'exportation de données à des fins d'activités visées par ce troisième pilier.

La Commission semble ne pas s'être embarrassée de toutes ces considérations : elle a déclaré la protection offerte par les *Undertakings* américains adéquats, elle a signé un traité international, ne laissant ni au Parlement européen, ni aux Etats membres le soin de décider. Sans doute, sa position sacrifie-t-elle quelque peu les exigences de la protection des données mais elle évite la cacophonie qu'aurait immanquablement engendré les positions diverses des Etats membres.

Elle a, en outre, le mérite de la rapidité là où l'intervention du Parlement aurait différé longuement une solution, mais une telle position est-elle bien démocratique?

Yves POULLET
Doyen de la Faculté de droit, F.U.N.D.P.
Directeur du Centre de recherches informatiques et droit (C.R.I.D.).
Professeur ordinaire à la Faculté de droit, F.U.N.D.P. et Liège.

María Verónica PERES ASINAN
Chercheuse au C.R.I.D.

(72) A propos de ce débat délicat et du besoin d'une nouvelle approche du principe de souveraineté, voir Y. Poullet, « Le droit de savoir et le devoir de l'Union européenne et des Etats membres de veiller au respect de la protection des données dans le commerce mondial », in *The Spanish Constitution in the European Constitutionnal Context*, F. Ferandez Sagado (ed.) Madrid, Dykinson, 2003, pp. 1764 et s.

(73) Protocole additionnel à Convention pour la protection des personnes à l'égard au traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, Strasbourg, 8 novembre 2001, disponible sur : http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm