COOPERATION ANTITERRORISTE TRANSATLANTIQUE : SÛRETE AÉRIENNE, TRANSFERTS DE DONNÉES PERSONNELLES ET NÉGOCIATION DE L'ACCORD *PASSENGER NAME RECORD*

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

En matière de lutte contre le terrorisme, les États-Unis ont développé une doctrine spécifique liée à la protection de l'intégrité territoriale et de la souveraineté nationale. La mise en œuvre de cette politique de la « sécurité intérieure » (« *Homeland Security* ») a néanmoins précédée les attaques terroristes du 11 septembre 2001. En effet, la première législation de défense de la sécurité intérieure date de 1798 lors du vote par le Congrès américain du *Alien and Sedition Act*[2]. En matière de lutte contre le terrorisme, le vote en 1917 des *Espionnage and Sedition Acts* constitue la réaction américaine au flux d'immigrants européens issus notamment d'Europe de l'Est[3]. Le jugement rendu par la Cour Suprême des États-Unis dans l'affaire *Gitlow v. New York*[4] constitue un tournant décisif quant à la mise en œuvre de la politique de sécurité intérieure et des législations fédérales car la Cour juge pour la première fois que l'État doit agir en conformité avec les dispositions du *Bill of Rights*. Le développement de la législation antiterroriste suit ainsi une évolution exponentielle et la surveillance des flux de données personnelles au sein des États-Unis devient rapidement le point focal de la législation américaine. En effet, en vertu du *Foreign Intelligence Surveillance Act* (F.I.S.A.) voté par le Congrès en 1978, les données électroniques peuvent être collectées à des fins de lutte contre le terrorisme. Dès lors, une association discursive est établie entre les notions de terrorisme, d'immigration et de frontières[5]. Cet amalgame emporte des conséquences majeures quant à la mise en œuvre de la législation américaine qui associe étroitement les agences de renseignement, notamment la *Central Intelligence Agency* (C.I.A.) et le *Federal Bureau of Investigation* (F.B.I.), aux opérations de transferts de données personnelles à des fins de lutte contre le terrorisme.

La mutation des orientations stratégiques et politiques américaines s'opère consécutivement aux attaques

[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] « *Homeland Security and Anti-Terrorism Legislation in the United States Prior to 2001 : A Brief History » in* BECKMAN James (ed.), *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, Hampshire, Ashgate, 2007, p. 13.

[3] Voir sur ce point le jugement rendu par la Cour Suprême des États-Unis dans l'affaire *Schenck v. United States*, 249 U.S. 47, January 9, 1919 (*First amendment, freedom of speech, freedom of the press, searches and seizures*) et dans l'affaire *Abrams v. United States*, 250 U.S. 616, November 10, 1919 (*criminal, first amendment, freedom of speech, freedom of the press*).

[4] *Gitlow v. New York*, 268 U.S. 652, November 23, 1923.

[5] CEYHAN Ayse, « *Défense et identités : un contexte sécuritaire global ? Terrorisme, immigration et patriotisme. Les identités sous surveillance* », *Cultures & Conflits*, n° 44, 2001, pp. 117-133.

du 11 septembre 2001. Les attentats contre le World Trade Center et le Pentagone ont cristallisé les failles des mécanismes nationaux de lutte contre le terrorisme et ont constitué un tournant dans la mise en œuvre de la politique américaine qui se traduit par l'adoption de nouvelles législations qui renforcent la sécurité intérieure. Compte tenu de cet état de fait, la présente étude concentre son analyse sur la législation américaine postérieure aux attentats de 2001. En la matière, le rôle de l'administration Bush occupe une place substantielle en ce qu'elle élève les préoccupations d'ordre sécuritaire et la lutte contre le terrorisme au rang de priorité nationale. Il est alors question du « terrorisme domestique », défini dans la nouvelle législation antiterroriste *Patriot Act* du 12 octobre 2001 comme « *toute activité qui est destinée à intimider ou à contraindre les populations civiles, influencer la politique du gouvernement par intimidation, ou coercition et affecter la conduite du gouvernement par destruction massive, assassinat ou enlèvement et qui survient essentiellement à l'intérieur de la juridiction territoriale des États-Unis* »[6]. Le concept de *Homeland Security*, qui était jusqu'à lors utilisé principalement par les militaires, est désormais largement employé par l'administration américaine afin de définir sa politique de lutte contre le terrorisme. L'utilisation d'aéronefs en tant qu'armes de destruction massive a entraîné l'application des dispositions de la législation relative à la sécurité intérieure au domaine de l'aviation civile. *De facto*, la sûreté aérienne est devenue un enjeu stratégique pour l'hermétisation des frontières américaines.

Par conséquent, une réforme de cette législation a été mise en œuvre par le biais de l'adoption du *Aviation Transportation Security Act* en 2001. Aux fins de cette présente étude, il convient de distinguer les notions de « sécurité » et de « sûreté » appliquées au domaine de l'aviation civile. La notion de sécurité aérienne, en ce qu'elle procède de l'ensemble des mesures techniques visant à réduire le risque aérien, ne sera pas abordée en l'espèce. A l'inverse, la problématique étudiée dans cette étude concerne la sûreté aérienne, entendue au sens de l'Annexe 17 à la Convention relative à l'aviation civile internationale[7] qui définit le terme comme la « *protection de l'aviation civile contre les actes d'intervention illicite* ». L'intérêt d'envisager les dispositions du *Aviation Transportation Security Act* du 19 novembre 2001, est d'observer les différentes étapes qui ont abouties à la négociation de l'accord international *Passenger Name Record* (« P.N.R. ») avec l'Union européenne. Effectivement, la gestion de la sûreté aérienne est intrinsèquement liée à l'observation des flux transfrontaliers, notamment par le biais du contrôle des individus effectué d'une part par les services nationaux de douanes aux frontières et, d'autre part, par les compagnies aériennes lors de l'embarquement. Ce faisant, ces contrôles représentent un formidable potentiel de divulgation d'informations personnelles que la présente étude s'attache à analyser. En conséquence, cette étude se concentre sur la collecte des informations personnelles concernant les passagers et exclu les renseignements relatifs aux marchandises et au fret.

[6] *H.R. 3162 Uniting and Streghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (US Patriot Act) of 2001, Titre VIII, section 802.

[7] Annexe 17 à la Convention relative à l'aviation civile internationale, Normes et pratiques recommandées internationales, Sûreté, Protection de l'aviation civile contre les actes d'intervention illicite, 8ème édition, avril 2006, Normes et pratiques recommandées internationales, Chapitre 1, Définitions, p. 1-2.

Ces informations personnelles sont contenues dans les bases de données des transporteurs aériens et principalement dans les systèmes informatisés de réservation (S.I.R.) et les systèmes de contrôle des départs (S.C.D.). Ces bases de données comportent des données dites « A.P.I. » (« *Advanced Passenger Information* ») et des données dites « P.N.R. » (« *Passenger Name Record* »). Dès lors, il s'agit de distinguer ces deux types de données, bien que les données du dossier passager (ci-après P.N.R.) comportent elles-mêmes des données A.P.I.. Tout d'abord, les données A.P.I. comprennent des données biographiques fournies directement par les passagers : ces informations sont saisies par les compagnies aériennes ou les agences de voyage. A contrario, les données P.N.R. sont des données de nature commerciale qui incluent des données biographiques simples mais aussi des informations variées ; seules les données P.N.R. peuvent inclure des données dites « sensibles » au sens de la directive européenne 95/46/CE. De plus, tandis que la transmission des données A.P.I. s'effectue après l'embarquement, l'accès aux données P.N.R. s'effectue au moment de la réservation. Selon la définition de l'Organisation de l'aviation civile internationale (O.A.C.I.), le dossier passager est « *le nom générique donné aux dossiers crées par les exploitants d'aéronefs ou leurs agents agréés pour chaque voyage réservé par un passager ou par un tiers en son nom. Ces données sont utilisées par les exploitants pour leurs propres usages commerciaux et opérationnels dans la prestation des services de transports aériens […] Un P.N.R. est constitué à partir des données fournies par le passager ou en son nom, concernant tous les segments de vols de son voyage.* »[8] Les données P.N.R. représentent donc un enjeu crucial au sein de la législation américaine relative à la sûreté de l'aviation civile. En vertu des dispositions du *Aviation Transportation Security Act*, les autorités américaines, et notamment le *Customs and Border Protection* (C.B.P.), requièrent l'accès aux données P.N.R.. Dans un premier temps, ces dispositions sont seulement appliquées aux vols domestiques ; elles sont rapidement étendues aux vols internationaux car cette législation comporte des dispositions extraterritoriales. C'est dans ce contexte qu'intervient la coopération entre l'Union européenne et les États-Unis.

La coopération transatlantique en matière de sûreté du trafic aérien et de protection des frontières précède les négociations relatives à la conclusion d'un « accord P.N.R. ». Le *Department of Homeland Security* (D.H.S.) et le C.B.P. sont ainsi les principaux interlocuteurs de l'Union européenne et ils précisent : « *[We sought] to extend our zone of security outward so that American borders are the last line of defence, not the first.* »[9] A cet effet, la coopération transatlantique s'est accentuée dès 2002 dans le cadre des mesures relatives à l'instauration des passeports biométriques. En vertu de la législation américaine, les passagers des vols à destination des États-Unis doivent posséder un passeport à lecture optique ; à défaut, ces derniers doivent obtenir un visa pour entrer aux États-Unis, même s'ils sont ressortissants d'un État partie

[8] Lignes Directrices sur les données des dossiers passagers (P.N.R.), Cir 309 AT/131, Organisation de l'aviation civile internationale, avril 2006, p. 1.
[9] SPENCE David (ed.), *The European Union and Terrorism*, London, John Harper, 2007, p. 136.

au *Visa Waiver Program*. En effet, l'Union européenne est un partenaire décisif considérant les dix à onze millions de passagers européens qui effectuent des vols à destination ou au départ des États-Unis. Pour cette raison, les autorités américaines requièrent dès 2003 l'accès aux données P.N.R. des compagnies aériennes européennes. En découle un contentieux transatlantique du fait du conflit de lois existant entre les dispositions européennes et américaines relatives à la protection des données personnelles et au droit à la vie privée. Compte tenu respectivement des dispositions de la directive 95/46/CE, de la Convention européenne des droits de l'homme (C.E.D.H.) et de la Charte des droits fondamentaux de l'Union européenne, un tel transfert de données personnelles serait contraire aux standards européens. Ces mesures appliquées à l'Union sont sans précédent dans l'histoire des relations transatlantiques et ce caractère exceptionnel s'explique tant du point de vue du volume et de la sensibilité des données concernées que du point de vue du nombre d'individus potentiellement affecté par cette législation américaine. Les difficultés sont aussi liées à la question de l'utilisation de données personnelles à des fins répressives, élément qui semble entrer en conflit avec la construction en piliers de l'Union européenne. Compte tenu des enjeux à la fois juridiques et économiques en présence, et de l'absence d'instrument juridique régissant cette problématique dans le cadre des relations avec un État tiers, des négociations ont été entamées dès 2003. L'objectif à terme est de négocier la conclusion d'un accord international qui offrirait un cadre juridique à ce type de transfert des données personnelles dans le respect des droits fondamentaux. Cette problématique de la protection des données personnelles est d'autant plus importante qu'elle intervient au moment où l'Union européenne tente d'harmoniser les procédures des États membres en la matière.

Le contexte des négociations transatlantiques concernant l'accord P.N.R. est rendu conflictuel du fait des menaces de sanctions pécuniaires qui pèsent sur les compagnies aériennes européennes qui refusent de divulguer les données du dossier passager. Néanmoins, une solution institutionnelle a été mise en application via la création en 2004 d'un forum spécialisé pour les négociations transatlantiques, le *Policy Dialogue on Borders and Transport Security* (P.D.B.T.S.). La Commission européenne a donc temporairement autorisé le transfert de ces données jusqu'à la signature d'un accord bilatéral. Cet accord a été conclu en 2004, faisant suite à la décision d'adéquation adoptée par le Commission qui constate le niveau de protection « adéquat » offert par le C.B.P. à ces données personnelles. Le Parlement a néanmoins intenté un recours en annulation de cet accord devant la Cour de Justice des Communautés européennes. La Cour ayant décidé d'annuler l'accord, de nouvelles négociations ont eu lieu afin de parvenir à la conclusion d'un accord applicable à long terme.

Actuellement, la sûreté aérienne est une composante à part entière de la défense nationale invoquée par les États-Unis. Cette législation présente un lien étroit avec le droit à la libre circulation des personnes et, en ces termes, les vols transatlantiques deviennent un véritable enjeu économique incluant des incidences juridiques majeures. Par le bais d'une analyse approfondie des enjeux juridiques qu'implique l'accord

P.N.R., cette étude vise à analyser l'impact de la législation antiterroriste américaine, appliquée au domaine de la sûreté de l'aviation civile, sur la législation de l'Union européenne. L'objectif est d'envisager plus particulièrement les conséquences en matière de protection des droits fondamentaux au sein de l'Union européenne. Dès lors, il est question d'étudier les modalités d'application de la législation américaine à l'Union européenne et de mettre en exergue les solutions avancées visant à mettre un terme au conflit juridique existant. Cette étude se fonde sur le postulat selon lequel l'échange de données personnelles entre les États au niveau international constitue une finalité nécessaire dans les sociétés démocratiques. Dans le contexte actuel de la lutte contre le terrorisme, la mise en œuvre de systèmes de profilage des individus à risque est un outil efficace afin de prévenir des actes illicites contre l'aviation civile. L'Union européenne elle-même met en œuvre des systèmes de transfert de données personnelles au sein des États membres[10]. Néanmoins, la lutte contre le terrorisme implique une variété de sources à partir desquelles sont constituées ces bases de données ; les informations issues des services de renseignement des États ou bien des autorités policières doivent faire l'objet d'un encadrement juridique lors de leur traitement. A fortiori lorsqu'il est question de données de nature commerciale, dès lors que leur traitement ne poursuit pas la même finalité que celle pour laquelle elles ont été collectées. Telle est la position de l'O.A.C.I. qui confirme la nécessité d'appliquer des standards internationaux de protection des donnés personnelles dans ce contexte de « renseignement de masse ». En l'espèce, l'enjeu est de taille et concerne la protection des droits fondamentaux des individus et, plus largement, l'effectivité de l'État de droit.

La doctrine s'est principalement attachée à étudier les problématiques liées à l'utilisation des technologies de biométrie et les conséquences de cette pratique, notamment au travers de la constitution de « listes noires ». A l'inverse, la question du transfert de données personnelles de nature commerciale de l'Union européenne vers les États-Unis et ce, à des fins répressives, a été étudiée dans une moindre mesure. Les études existantes en la matière rejettent pour la plupart le principe même de l'utilisation de données commerciales à des fins de lutte contre le terrorisme, arguant la constitution d'un mécanisme de surveillance global qui viole les droits fondamentaux. A l'évidence, l'expérience des relations transatlantiques dans ce domaine révèle des difficultés majeures. A titre d'exemple, le scandale de l'affaire SWIFT, qui concernait l'utilisation secrète de données bancaires de citoyens européens par la C.I.A., est venu entacher durablement la nature de la coopération transatlantique. Ce contexte général conforte une perception négative du partenariat euro-américain dans le cadre de la lutte contre le terrorisme et explique les réticences des institutions de l'Union à l'encontre du transfert de données personnelles. Pourtant, ce contexte révèle aussi la nécessité d'un cadre juridique en la matière. Il est nécessaire de déterminer dans quelle mesure le droit à la vie privée et à la protection des données sont appliqués dans le contexte des systèmes automatisés de traitement des informations personnelles utilisés par l'Union et les États Unis.

[10] Système de fichiers automatisés S.I.S. issu des accords de Schengen, voir CHEVALLIER-GOVERS Constance, *De la coopération à l'intégration policière dans l'Union européenne*, Bruxelles, Bruylant, 1999, p. 161.

I. - Sûreté de l'aviation civile et « Homeland Security »

Le renforcement de la législation antiterroriste relative à la sûreté représente une nécessité commune à la fois pour les États-Unis et l'Union européenne (U.E.): il est dès lors question de la protection de l'intégrité territoriale et de la souveraineté nationale de chacun. L'attaque du World Trade Center marque un tournant décisif quant à la gestion de la sûreté aérienne. Concernant les États-Unis, une nouvelle politique a été mise en œuvre, impliquant des contrôles de sécurité renforcés au sol mais aussi en vol[11] tels qu'illustrés par le renforcement du programme *Sky Marshals*[12] destiné à faire face aux détournements d'avions. En parallèle, le Congrès américain préconise, en tant que mesure de prévention, l'utilisation du système informatisé C.A.P.P.S., qui inclue le dépistage et le profilage des passagers. Quant à l'Union européenne, l'expérience des détournements d'aéronefs dès les années 1970 et notamment l'explosion en vol d'un avion de la compagnie Pan Am à Lockerbie en 1988, a entraîné une prise de conscience concernant l'utilisation des aéronefs en tant qu'armes de destruction de masse. *De facto*, le renforcement de la sûreté est aussi devenu une priorité européenne et est illustré par l'élaboration par la Conférence européenne de l'aviation civile (C.E.A.C.) en 1988 de recommandations[13] aux États pour élaborer un programme national de sûreté de l'aviation (en matière de contrôle des passagers, des bagages et du fret). C'est dans ce contexte de développement exponentiel de ce type de législation que se pose la question de la coopération transatlantique.

L'entrée en vigueur du *Patriot Act* en 2001, du *Patriot Act II* en 2003 et du *Homeland Security Act* en 2001, atteste d'un lien étroit existant entre les préoccupations de sécurité intérieure et de défense. Ces textes législatifs comportent une dimension « intrusive » vis-à-vis du droit à la vie privée consacré par le Quatrième Amendement, intrusion justifiée par l'impératif de sécurité publique. En vertu de ces législations, l'accès aux communications électroniques privées est ainsi autorisé notamment par le biais des *National Security Letters*[14]. La problématique invoquée par les associations de protection des libertés civiles réside en l'absence de contrôle lors de l'interception de communications privées, autorisée même

[11] Pour la définition du terme « en vol », voir la Convention pour la répression des actes illicites contre la sécurité de l'Aviation Civile, 18 juillet 1975, n°14118, article 2 (a) : « *Un aéronef est considéré comme étant en vol depuis le moment où, l'embarque ment étant terminé, toutes ses portes extérieures ont été fermées jusqu'au moment où l'une de ses portes est ouverte en vue du débarquement ; en cas d'atterrissage forcé, le vol est censé se poursuivre jusqu'à ce que l'autorité compétente prenne en charge l'aéronef, ainsi que les personnes et les biens à bord* » ; disponible à http://www.un.org/french/pubs/chronique/2001/numero3/0301p74.html.

[12] Le programme *Sky Marshal* a débuté en 1968, sous l'autorité de l'Administration fédérale de l'aviation, et ne concernait que les vols domestiques. Le programme a été étendu en 1985 (suite au détournement du vol TWA 847) aux vols internationaux effectués par des aéronefs américains. Après les attentats du 11 septembre, le Président G.W. Bush a multiplié les effectifs et le budget de ce programme qui, en vertu de la loi sur la sûreté de l'aviation civile et des transports, est désormais sous l'autorité de l'Administration de la sûreté aérienne.

[13] Déclaration de politique de la CEAC dans le domaine de la Facilitation de l'aviation civile, ECAC. CEAC Doc. n° 30, 10ème édition, décembre 2006.

[14] BECKMAN James (ed.), *Comparative Legal Approaches to Homeland Security And Anti-Terrorism*, Hampshire, Ashgate, 2007, p. 32.

« sans cause sérieuse » selon le *Foreign Intelligence Act* de 1978. Dès lors, la doctrine de la « sécurité intérieure » consiste en un quadrillage sécuritaire du territoire américain et implique environ quarante-six agences de sécurité locales, étatiques et fédérales. La mission qui est assignée en vertu du *Homeland Security Act* est « *la défense des populations civiles de tout ennemi sur le sol américain et inclut, pour ce faire, tout ce qui va du contrôle des frontières à la protection des infrastructures vitales et stratégiques comme l'électricité, l'eau ou les usines chimiques* »[15]. Ce concept, qui est implicitement inscrit dans la Constitution américaine, est réitéré dans le rapport de la Commission sur la sécurité nationale de 2001[16].

A. - La réforme de la structure et de la législation relative à la sûreté aérienne

L'attaque terroriste du World Trade Center constitue une atteinte à l'intégrité territoriale et à la souveraineté nationale des États-Unis qui représente un tournant dans la politique antiterroriste américaine en ce que la sûreté de l'aviation civile est devenue une réelle problématique de défense nationale. En effet, une réforme quasi immédiate de l'organisation de la sûreté aérienne s'en est suivie, avec pour fondement juridique la loi sur la sûreté de l'aviation et des transports du 19 novembre 2001.

1. Les fondements posés par le *Aviation Transportation Security Act*, 2001

Antérieurement au 11 septembre, l'Administration fédérale de l'aviation (*Federal Aviation Agency*, F.A.A.) était compétente en matière de sûreté et sécurité du transport aérien aux États-Unis en tant qu'administration intégrée au Ministère des transports. Postérieurement aux attentats de 2001, la création de l'Administration de la sûreté aérienne (*Transportation Security Administration*, T.S.A.) constitue une réforme du système car la T.S.A. possède désormais la majorité des compétences en la matière tandis que la F.A.A. voit son contrôle réduit au domaine des marchandises dangereuses.

a. Création de la *Transportation Security Administration* et renforcement du mandat du C.B.P.

A l'origine, la F.A.A.[17] est l'organe responsable de la sûreté et de la sécurité du transport aérien. Dès 1973, cette administration confie la responsabilité du filtrage des passagers aux compagnies aériennes. Selon le rapport de 1997 du *Government Accountability Office* (G.A.O) : « *la F.A.A. continue d'assumer la responsabilité et la mise en œuvre des règlements publics, des procédures ainsi que de l'identification des*

[15] DOBBS Michael, "*Homeland Security: New Challenges for an Old Responsibility*", ANSER, November 1st, 2001. Voir aussi, WALKER David M., "*Homeland Security: A Framework for Addressing the Nation's Efforts*", Washington, GAO/01-11581, 2001 et "*Homeland Security, Challenges and Strategies in Addressing Short and Long Term National Needs*", GAO/02-1605, 2001.

[16] *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States*, 10 October 2001, §1.2 *Improvising a Homeland Defense*, p. 31.

[17] *Federal Aviation Act*, 1958, 72 Stat.767, 49 U.S.C.A, portant création de la F.A.A. Sur la F.A.A. voir aussi FIELDS Louis, « The Evolution of U.S. Counter-Terrorist Policy » *in* BASSIOUNI Cherif M. (ed.), *Legal Responses to International Terrorism: U.S. Procedural Aspects*, Martinus Nijhoff, 1988 , p. 282.

menaces potentielles et de la prise des mesures appropriées. Les compagnies aériennes assument la responsabilité du contrôle et des autres mesures de sûreté applicables aux passagers, aux bagages et au fret. »[18]. Face à la menace terroriste grandissante et considérant les différents dysfonctionnements institutionnels affectant la sûreté aérienne, l'action de la F.A.A. est considérée comme insuffisante. La création de la T.S.A. en 2001 emporte des conséquences en terme d'organisation institutionnelle et de répartition des compétences. Initialement, la T.S.A. était intégrée au sein du Ministère des transports. Dès 2002[19], la T.S.A. est intégrée au sein du Ministère de la sûreté intérieure (*Department of Homeland Security*, D.H.S.). *De facto*, le Ministère des transports a été privé de ses compétences en matière de sûreté aérienne. Cette réforme substantielle témoigne de la spécificité de la politique américaine : la sûreté aérienne est ainsi intrinsèquement liée à la sûreté intérieure et comporte un aspect militaire. Par ailleurs, la T.S.A., à la différence de la F.A.A., édicte les règlements dans le cadre des lois relatives à la sûreté aérienne et contrôle leur application. Les compagnies aériennes ne sont donc plus en charge de la mise en œuvre des règles de sûreté. Du point de vue de la répartition des compétences, celles-ci sont réparties entre deux administrations. En effet, la T.S.A. est en charge de la mise en œuvre des mesures de sûreté de l'aviation civile concernant les vols domestiques tandis que le Services des douanes et de protection des frontières (*Customs and Border Protection*, C.B.P.) est compétent quant à l'application des mesures de sûreté pour les vols internationaux effectués par des transporteurs américains.

En vertu de la loi sur la sûreté de l'aviation et des transports, il est fait obligation aux compagnies aériennes de mettre à disposition du C.B.P. les informations contenues dans le système automatisé de réservation et incluant les renseignements inscrits dans le dossier passager (*Passenger Name Record*, P.N.R.)[20]. Ces informations incluent le nom de chaque passager, la date de naissance, le sexe, le numéro de passeport et le pays de délivrance, le numéro du visa américain ou le numéro de carte d'étranger et « *Such other information as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety."*[21] Cette obligation de transfert se fonde sur la seule requête exprimée par le C.B.P. *(« upon request* »). Cette loi est renforcée par un règlement émanant du C.B.P. en date du 25 juin 2002[22] qui précise les données P.N.R. requises. De plus, la loi du 14 mai 2002[23]

[18] « *FAA's Actions to Study Responsibilities and Funding for Airport Security and to Certify Screening Companies* », GAO, Février 1999, *in* Rapport d'information déposé par la Délégation de l'Assemblée Nationale pour l'Union européenne sur la sûreté du transport aérien en Europe, n° 2241, 12 avril 2005, p. 29.

[19] Section 423, Functions of Transportation Security Administration, 6 USC 233, *Homeland Security Act*, 25 November 2002, Public Law 107–296, 107th Congress, p. 51 ; disponible à l'adresse suivante http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm.

[20] *Aviation and Transportation Security Act*, 49 USC 40101, Nov. 19, 2001, [S. 1447], Public Law 107–71 107th Congress, (3) *Passenger Name Record*, p. 27.

[21] *Ibid*., Sec. 115. Passenger manifests, (2) (F), p. 27.

[22] *Passenger Name Record Information Requered for Passengers on Flights in Foreign Air Transportation to or from the United States; U.S.Customs Service*, Department of the Treasury 19 CFR Part 122, T.D. 02-33, Federal Register, 25 June 2002.

[23] Pour une liste complète des données voir *Enhanced Border Security and Visa Entry Reform Act*, Sec. 402. Passenger manifests, Public Law 107-173-May. 14, 2001, (C) Contents of Manifests; disponible à l'adresse suivante http://www.fas.org/irp/congress/2002_cr/h031202.html.

impose la communication de ce type de données aux services fédéraux de l'immigration (*Immigration and Naturalization Service*, I.N.S.) avant l'arrivée sur le territoire américain via le Système avancé d'information sur les passagers (*Advanced Passenger Information System*, A.P.I.S.). Le non-respect de cette obligation implique l'imposition d'amendes et la perte du droit d'atterrissage pour les compagnies aériennes[24]. Afin d'agir en conformité avec ces législations, les compagnies aériennes américaines ont donné accès au C.B.P. au dossier passager. Le P.N.R. est créé à chaque fois qu'un passager effectue une réservation de vol et il est conservé au sein des systèmes de réservation des compagnies aériennes. Le nombre et la nature de ces données varient donc selon les compagnies aériennes. De nombreuses compagnies américaines ont divulgué les mots de passe de leurs bases de données au C.B.P. qui peut désormais accéder directement (méthode « *pull* ») aux données plutôt que de sélectionner celles qui correspondent aux éléments requis par ses propres réglementations internes (méthode « *push* »). Ainsi, les transporteurs aériens qui assurent des liaisons à destination, au départ ou à travers le territoire des États-Unis accordent aux autorités douanières américaines ainsi qu'aux services fédéraux de l'immigration un accès électronique aux données contenues dans leurs systèmes automatiques de réservation et de contrôle des départs. Concernant les vols internationaux, les dispositions d'exécution du *Aviation Transportation Security Act* incluent la mise en œuvre l' *Aviation Security Screening Records*[25] qui oblige les compagnies aériennes opérant en Europe à accorder l'accès aux données commerciales reprises dans le dossier passager.

b. Utilisation accrue des « *no fly list* » et « *selectee list* » par la T.S.A.

La F.A.A. et la T.S.A. utilisent les listes d'interdiction de vol et les « listes sélectives » en tant qu'outil de prévention des actes de terrorisme. La liste d'interdiction de vol est une liste comprenant les noms de personnes qui sont interdites d'embarquer tandis que les « listes sélectives » comportent le nom de personnes autorisées à embarquer mais seulement après un contrôle approfondi[26]. Ce mécanisme se fonde sur le profilage des individus à risque ; cette analyse du risque s'effectue sur la base de critères juridiques flous dans la mesure où les informations retenues afin de déterminer le degré de dangerosité émanent des services de renseignements, notamment la C.I.A. et le F.B.I. Ce mécanisme de transfert de données personnelles vers le C.B.P. s'effectue, à l'origine, via le système automatisé C.A.P.S.S., utilisé comme instrument de prévention et d'anticipation des menaces terroristes par la création de profils de comportements à risque. Ce type de système informatisé est caractérisé par son interconnexion avec les bases de données des organes fédéraux de lutte antiterroriste. A terme, ce système devait permettre le dépistage et le profilage des passagers afin que les compagnies aériennes soient en mesure d'interdire à

[24] *Ibid*., (10) (g).

[25] *Federal Register* 68 FR 2101, « *TSA intends to use this system of records to facilitate TSA's passenger and aviation security screening program under the Aviation and Transportation Security Act.* ». Le *Aviation Security Screening Records* est utilisé par le Département américain des Transports, sous l'égide de la T.S.A.

[26] MEEKS Brock N., "*Faces of the 'No Fly' list: Why are they suspect until proven innocent?",* 26 July 2005, *MSNBC.*

certaines personnes d'être embarquées et de procéder à un second contrôle de dépistage de certains autres passagers. Tandis que le principe même de l'utilisation de ces listes est dénoncé par des associations américaines telles que l'*American Civil Liberties Union* (A.C.L.U.) ou encore l'*Electronic Privacy Information Center* (E.P.I.C), la T.S.A. justifie son utilisation[27] en se fondant sur les recommandations de la Commission d'enquête sur le 11 septembre 2001. Cette Commission d'enquête a été créée en 2002 par le biais de législations votées par le Congrès américain[28]. Cette Commission présidée par Thomas H. Kean avait pour mandat d'effectuer un rapport d'enquête concernant les attentats du 11 septembre et d'effectuer des recommandations, en vue de prévenir d'éventuelles attaques. Dans son rapport final du 22 juillet 2002, la Commission préconise[29] le développement et l'alimentation de ces listes considérées comme moyen le plus efficace d'empêcher les personnes « à risque » de pénétrer un aéronef. L'obligation incombe alors aux compagnies aériennes de confronter ces listes à celle de leurs passagers embarqués.

Du point de vue de l'A.C.L.U., l'utilisation de ces listes est inappropriée. Tout d'abord, car la définition même des no fly lists - « *persons who may be at risk to civil aviation* »[30]- est trop large pour que ce règlement soit considéré comme prévisible par le citoyen américain. Une simple suspicion justifierait alors l'arrestation et la poursuite d'un individu. Par ailleurs, le fait que ces listes contiennent les noms de personnes mais ne sont pas accompagnées d'une description physique ne constitue pas des informations suffisantes pour arrêter un individu. En atteste les différents cas d'homonymie[31], et notamment le cas du sénateur Edward Kennedy, qui démontrent que des personnes peuvent être arrêtées sur la seule base d'un nom similaire à celui d'un suspect inscrit sur les listes d'interdiction de vol. De plus, les citoyens n'ont pas connaissance de leur inscription sur ces listes, jusqu'à ce qu'ils soient arrêtés à l'aéroport. Cela implique qu'ils ne disposent pas d'un droit de recours effectif. Le seul moyen d'action, lors d'une arrestation basée sur des informations erronées, est un procédé de nature administrative afin que le Bureau des réparations de la sûreté des transports (*Office of Transportation Security Redress*) étudie la fiche de vérification d'identité du voyageur (*Traveler Identity Verification Form*) et modifie les informations le concernant. Du point de vue de la légalité de ce système, l'A.C.L.U. considère que les listes d'interdiction de vol et les « listes sélectives » sont inconstitutionnelles considérant le Cinquième Amendement (« *freedom of due*

[27] *Memo from Acting Associate Under Secretary, Transportation Security Intelligence to Associate Under Secretary*, Security Regulation and Policy, Re: TSA "Watchlists", Oct. 16, 2002.

[28] *Act to authorize appropriations for fiscal year 2003 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes*, November 27, 2002, Public Law 107-306, 107th Congress; available at http://govinfo.library.unt.edu/911/about/107-306.htm; *Act to extend the final report date and termination date of the National Commission on Terrorist Attacks Upon the United States, to provide additional funding for the Commission, and for other purposes*, Public Law 108-207; disponible sur http://govinfo.library.unt.edu/911/about/index.htm.

[29] *Final report of the National Commission on Terrorist Attacks Upon the United States*, 22 July 2004, 3.3 …

[30] A.C.L.U., "*Are the No Fly List and Selectee List accurate?",* 26 October 2005 ; disponible sur http://www.aclu.org/safefree/general/21164res20051026.html.

[31] CNIL, « *Gros plan sur les listes américaines d'interdiction de vol ou No fly lists* », 28 juin 2006 ; disponible à http://www.cnil.fr/index.php?id=2037.

process »)[32] et le Sixième Amendement (« *right to a trial* »). Ce faisant, National A.C.L.U. et A.C.L.U. Washington ont intenté une action en justice en avril 2004[33]. La Cour de District de Seattle a estimé au mois de janvier 2005 que la violation du principe de « *due process* » n'était pas fondée. Néanmoins, le Congrès a voté une loi en décembre 2004[34] qui oblige la T.S.A. à constituer ces listes selon des procédures précises, « *that will not produce a large number of false positives*", et à instaurer une procédure judiciaire en vue d'offrir aux citoyens un moyen juridique en vue de supprimer leur inscription à ces listes.

2. Les modalités d'application de la législation américaine à l'Union européenne

La spécificité de la législation américaine semble résider en ce que nombre de ses dispositions comportent une dimension extraterritoriale. La législation relative à la sûreté aérienne, appliquée aux vols internationaux, est porteuse de nouvelles obligations incombant aux compagnies aériennes basées au sein de l'Union européenne. La réglementation du C.B.P. et les diverses réglementations de la T.S.A. s'appliquent à l'Union notamment concernant le transfert des données P.N.R. Du point de vue du principe de la sécurité juridique, les modalités d'application des législations américaines à l'Union demeurent incertaines et engagent l'intégrité des données à caractère personnel.

a. La pratique des *emergency amendments*

Les mesures prises au sein des États-Unis visent à renforcer la sûreté des vols domestiques mais aussi à accroître les contrôles concernant les vols internationaux. En effet, l'administration Bush a proclamé l'état de guerre depuis les attentats du 11 septembre et mis en application la politique de « *war on terror* » qui justifie le renforcement de la doctrine de « *Homeland Security* » sur le territoire national. L'une des conséquences de l'élévation de la lutte contre le terrorisme international au rang de priorité nationale est que le Département d'État est mandaté par le Congrès afin de présenter des rapports annuels concernant l'évolution globale du phénomène terroriste[35]. Car la lutte extérieure contre le terrorisme est aussi présentée comme un moyen d'assurer la sécurité intérieure des États-Unis[36]. La réponse américaine aux attaques du 11 septembre concerne différents domaines politiques, incluant le renforcement des ressources

[32] *Bill of Rights, Amendement V*: « *No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation* ». ; disponible à http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.

[33] Affaire *Green contre T.S.A*.

[34] *Intelligence Reform and Terrorism Prevention Act* of 2004, P.L. 108-458, 118 Stat. 3714, 4012 (A), amending 49 U.S.C. 44903(j)(2).

[35] CAMERON Fraser, « Transatlantic Relations and Terrorism, Policy Dilemmas » *in* SPENCE David (ed.), *The European Union and Terrorism*, London, John Harper, 2007, p. 129.

[36] BECKMAN James, *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, Hampshire, Ashgate, 2007, p. 39.

législatives visant la sécurité intérieure et l'accroissement du mandat des agences fédérales. Cette orientation politique affecte tant le Département d'État, le Ministère de la Justice, le Ministère du Trésor (*Department of The Treasury*) et le Ministère du Commerce[37]. La coordination des actions des autorités fédérales en matière de lutte antiterroriste est aussi renforcée depuis les recommandations effectuées par la Commission d'enquête du 11 septembre qui exhortait l'administration Bush à accentuer la cohérence des initiatives des différents ministères et des différentes agences. *De facto*, les mesures internes de lutte contre le terrorisme incluent des dispositions à caractère extraterritorial, particulièrement dans le domaine de la sûreté de l'aviation civile. L'application des dispositions de la législation américaine relative à la sûreté aérienne aux compagnies étrangères par le biais d'une procédure d'urgence - *emergency amendments* - a suscité une certaine tension dans les relations transatlantiques entre 2002 et 2003. Le principe même de cette procédure d'urgence est posé par le *Aviation and Transportation Security Act.*

Le paragraphe 114 de cette loi autorise le Sous-secrétaire d'État aux transports à édicter un règlement ou une directive en matière de sûreté sans que ces textes ne fassent l'objet d'une publication ou de commentaires de la part du public préalablement à leur publication[38]. En ces termes, cette loi constitue une législation d'exception et déroge à la procédure habituelle qui inclue normalement le principe de publicité de la loi et sa présentation au Congrès afin d'envisager des éventuels amendements selon la procédure démocratique. L'approche américaine nécessite que les compagnies aériennes étrangères appliquent les lois et règlements américains pour desservir les États-Unis. Cette application extensive de la doctrine de la sécurité intérieure réduit substantiellement la marge de manœuvre de l'Union européenne. Ce faisant, l'administration américaine notifie l'existence de ces directives ou règlements aux compagnies aériennes et non pas directement aux États européens, considérant qu'une telle procédure est favorable à une harmonisation des procédures. Néanmoins, cette pratique a largement été critiquée par les États membres de l'Union qui affirment que leur souveraineté nationale s'en trouve affectée.

b. L'adhésion de l'U.E. aux principes du *Safe Harbor*

Précédant la réforme de la législation relative à la sûreté aérienne, une réorganisation des dispositions relatives à la protection des données personnelles dans le secteur privé a été mise en œuvre par l'administration américaine. Bien que cette réforme soit antérieure au 11 septembre 2001, elle est essentielle afin de circonscrire les spécificités de la démarche américaine en matière de protection des données personnelles. Cette réorganisation a pour origine la spécificité de la coopération transatlantique en la matière et trouve un fondement commun avec le dossier P.N.R. En effet, les principes du *Safe Harbor* concernent le transfert des données personnelles dans le cadre du secteur privé et l'utilisation de ces

[37] *Idem,* p. 132

[38] Rapport d'information déposé par la Délégation de l'Assemblée Nationale pour l'Union européenne sur la sûreté du transport aérien en Europe, n° 2241, 12 avril 2005, p. 36.

données issues des entreprises revêt une importance particulière en terme de lutte contre le financement du terrorisme. En effet, contrairement à l'Union européenne qui met en application une législation spécifique en matière de protection des données personnelles, notamment par le biais de la directive 95/46/CE, les États-Unis adoptent une approche sectorielle régie par un corpus juridique combinant codes de conduite et autres instruments d'autorégulation[39]. Compte tenu de l'entrée en vigueur de la directive européenne le 25 octobre 1998, la coopération transatlantique apparaissait problématique dans la mesure où l'article 25 (1) de la directive requiert que le transfert de données personnelles vers des pays tiers s'effectue à condition que ces derniers offrent un niveau de protection « adéquat ». Ce faisant, un vide juridique persistait lors de l'évaluation des opérations de transfert de données personnelles entre l'Union européenne et les États-Unis. Tenant compte des obligations posées par la directive 95/46/CE, le Département du Commerce américain a entamé des négociations avec l'Union européenne dès 1998[40] afin de déterminer des principes internationaux de la sphère de sécurité relatifs à la protection des données transférées par un État membre vers les États-Unis. Néanmoins, les principes du *Safe Harbor* proclamés le 21 juillet 2000 constituent une législation d'exception par rapport à la législation américaine, ce qui entraîne une application peu uniforme par les entreprises. A titre d'exemple, si la notion d'origine ethnique est considérée comme une donnée dite « sensible » au sens du *Safe Harbor*[41], tel n'est pas le cas en vertu des dispositions américaines. La décision de la Commission en date du 17 mars 2000[42] a entraîné l'adhésion de l'Union européenne aux principes du *Safe Harbor*[43].

Concernant le contenu de ces principes, la problématique demeure la définition des concepts fondamentaux tels que la notion de « données personnelles » qui est définie en terme flous, faisant référence au champ d'application de la directive européenne sans pour autant garantir que les principes du

[39] *Safe Harbor privacy principles*, issued by the U.S. Department of Commerce on July 21, 2000, Export. Gov; disponible à http://www.export.gov/safeharbor/SH_Privacy.asp.

[40] Voir notamment l'Avis 1/99 concernant le niveau de protection des données à caractère personnel aux États-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain, 26 janvier 1999, W.P. 15 ; Avis 2/99 concernant la pertinence des "principes internationaux de la sphère de sécurité" publiés parle ministère du commerce des États-Unis le 19 avril 1999, 3 mai 1999, W.P. 19 ; Avis 4/99 concernant les questions souvent posées, devant être publiées par le Ministère américain du Commerce dans le cadre des principes proposés pour la "sphère de sécurité", 7 juin 1999, W.P. 21.

[41] *Safe Harbor Privacy Principles*.

[42] Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique [notifiée sous le numéro C(2000) 2441], JO L 215 du 25.8.2000, p. 7–47, Article 1 : « *Aux fins de l'article 25, paragraphe 2, de la Directive 95/46/CE, pour toutes les activités rentrant dans le domaine d'application de la Directive, il est considéré que les 'principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée', dénommés ci-après « les principes », appliqués conformément aux orientations fournies par les QSP […], assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union européenne vers des organisations établies aux Etats-Unis si et dans la mesure où les conditions suivantes sont réunies en ce qui concerne les données à transférer : (a) l'organisation destinataire des données s'est clairement et publiquement engagée à observer les principes mis en œuvre conformément aux QSP ; (b) l'organisation est soumise aux pouvoirs légaux d'un organisme public habilité à instruire les plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, quels que soient leur pays de résidence ou leur nationalité, en cas de non respect des principes.* »

[43] *Federal Trade Commission Act*, Section 5.

Safe Harbor offrent la même protection que celle contenue dans l'article 2 (a)[44]. De même, les modalités de l'obtention du consentement de l'individu concerné par la collecte des données personnelles, mentionnées au principe 2, semblent comporter un caractère moins formel que celles explicitées à l'article 2 (h) de la directive européenne. Concernant les données personnelles dites « sensibles », elles sont définit comme « la donnée spécifiant (« *specifying* ») et non, au sens large de la directive, comme celle « révélant » les données médicales, de santé, ethniques, raciales, etc.[45]. Dès lors, le manque de transparence qualifiant la définition des termes fondamentaux susmentionnés ainsi que la capacité limitée d'accès[46] ne semble pas satisfaire la totalité des critères posés par la directive 95/46/CE. L'expérience des négociations transatlantiques relatives au *Safe Harbor* met en évidence la nécessité d'un accord global, incluant les questions relatives au troisième pilier, entre les États-Unis et l'Union européenne.

B. - L'articulation entre rétention des données personnelles et protection de la vie privée

A la différence de la législation européenne, la législation américaine concernant la protection des données personnelles ne considère pas le droit à la vie privée comme un droit fondamental. La protection de la vie privée est certes évoquée par le Quatrième amendement mais elle est en réalité réglementée par des dispositions spécifiques, le *Freedom of Information Act* (F.O.I.A.) et le *Privacy Act*. En l'espèce, aucune de ces dispositions ne concerne strictement le domaine des transports. Dès lors, ce dispositif de protection n'est applicable qu'aux citoyens américains et c'est en ces termes que le principe du transfert des données P.N.R., est difficilement applicable. Effectivement, aucun texte européen ne prévoit l'obligation pour ces transporteurs aériens de transmettre ces données personnelles.

1. Le rôle prédominant du Ministère de la sécurité intérieure (D.H.S.)

Le renforcement de la mise en œuvre de la doctrine du *Homeland Security* s'est traduit le 6 juin 2002 par la proposition du Président Bush de créer un nouveau ministère, le Ministère de la sûreté intérieure (D.H.S.). Le *Homeland Security Act* de 2002, modifie substantiellement l'organisation interne et regroupe désormais vingt-deux agences et organisations fédérales au sein du Ministère[47]. La Direction de la Sécurité des frontières et des transports (*Bureau of Transportation Statistics*, B.T.S.) est l'organe décisionnel qui établit notamment la coordination de l'action et de la politique du Service des douanes et de la protection des frontières et de l'Administration des transports et de la sûreté.

[44] POULLET Yves, « Les *Safe Harbor Principles* - Une protection adéquate ? », 10/07/2000, p. 9 ; disponible à : http://www.juriscom.net/uni/doc/20000617.htm.
[45] *Idem*
[46] Voir les exceptions contenues dans la FAQ 8 [« Access principle »]: « *Under the Safe Harbor Principles, the right of access is fundamental to privacy protection.(…) Nonetheless, the obligation of an organization to provide access is subject to the principle of proportionality or reasonableness and has to be tempered in certain circumstances* », p. 11.
[47] BECKMAN James, *Comparative legal approaches to homeland security and anti-terrorism*, Hampshire, Ashgate, 2007, p. 34.

a. Encadrement du mandat du C.B.P.

La création de ce nouveau Ministère de la sécurité intérieure constitue l'une des initiatives les plus importantes de réorganisation du gouvernement fédéral depuis la création du Ministère de la Défense durant la guerre froide. *Stricto sensu*, il n'existe pas de ministère équivalent au D.H.S. au sein de l'Union européenne ou de ses États membres. Suite aux critiques émises par le Congrès américain compte tenu de l'absence d'un mandat clairement défini du D.H.S., l'administration Bush a présenté en juillet 2002 un document présentant une « Stratégie nationale pour la sécurité intérieure »[48]. La section concernant la « Sécurité des frontières et des transports » inclue une partie intitulée « Vision nationale » qui précise: "*A single entity in the Department of Homeland Security will manage who and what enters our homeland in order to prevent the entry of terrorists and the instruments of terror while facilitating the legal flow of people, goods, and services on which our economy depends. The Department and its partners will conduct border security functions abroad to the extent allowed by technology and international agreements*."[49] Les organes du D.H.S. les plus pertinents quant à la gestion des relations transatlantiques sont le Service des douanes et de la protection des frontières et la T.S.A. en ce qu'ils sont impliqués dans le filtrage des passagers des vols en provenance de l'Europe. Ce filtrage des passagers s'effectue grâce à l'utilisation des données A.P.I. (*Advanced passenger information*) et des données P.N.R.

Dès lors, il s'agit de distinguer ces deux types de données non seulement car elles présentent une nature propre mais aussi dans la mesure où la collecte de celles-ci poursuit des finalités différentes[50]. Tout d'abord, les données A.P.I. comprennent des données biographiques fournies directement par les passagers telles que le nom, la date de naissance, la nationalité et le numéro de passeport. Ces informations sont saisies par les compagnies aériennes ou les agences de voyage et sont considérées comme des informations nécessaires au franchissement des frontières. A contrario, les données P.N.R. sont des données de nature commerciale et regroupent les informations recueillies par les compagnies aériennes depuis la réservation des passagers jusqu'au paiement. Le dossier passager peut donc inclure des données biographiques simples mais aussi des informations variées (itinéraire complet, contacts à terre du passager etc.)[51]. Seules les données P.N.R. peuvent inclure des données dites « sensibles » au sens de la directive 95/46/CE: cela peut inclure des éléments concernant l'appartenance à un parti politique, la pratique religieuse (régime alimentaire) ou encore l'état de santé. De plus, tandis que la transmission des données

[48] *The National Strategy For Homeland Security: Office of Homeland Security*, July 2002 ; disponible sur http://www.whitehouse.gov/homeland/book/.
[49] *Idem*, p. 22.
[50] 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 E2487 -COM (2003) 826 final du 16/12/2003, « *Le transfert par les compagnies aériennes des données des dossiers passagers aux autorités américaines* » (E 2487), Communication écrite de M. Hubert Haenel, Justice et Affaires intérieures ; disponible sur http://www.senat.fr/ue/pac/E2487.html.
[51] *Idem*.

A.P.I. s'effectue après l'embarquement, l'accès aux données P.N.R. s'effectue au moment de la réservation [52]. Concernant la finalité du transfert de ces données, la transmission des données A.P.I. concerne les personnes déjà connues des services américains alors que les données P.N.R. visent à évaluer le risque potentiel présenté par des individus inconnus de ces services. Le filtrage des données personnelles est effectué, à l'origine, via le Système informatisé ciblé (*Automated Targeting System*, A.T.S.). Ce système intranet avancé de « ciblage » a été développé conjointement par le D.H.S. et le C.B.P. et utilise une approche commune pour la gestion des données et de l'analyse. L'A.T.S. est utilisé principalement par le C.B.P. afin d'utiliser, analyser et diffuser les informations recueillies en vue de cibler, identifier et d'empêcher les terroristes potentiels de pénétrer le sol américain. En effet, le système A.T.S. est constitué d'un module A.T.S. - Passenger (« *travelers and conveyances* (*air, ship, and rail*)»)[53] qui reçoit directement les informations contenues dans le dossier passager. L'accès aux données P.N.R. par le C.B.P. s'effectue en vertu du Code des règlements fédéraux[54].

b. Le Bureau de la confidentialité du D.H.S.

Le mandat du Bureau (« *Privacy Office* ») est de maintenir les protections garanties aux individus et de garantir la transparence des opérations effectuées par le gouvernement américain lorsqu'il met en œuvre des missions relevant de la compétence du Ministère de la sécurité intérieure. Tout d'abord, le Bureau agit en vertu du *Privacy Act* de 1974 et garanti l'application du Code des principes d'information équitable qui gouverne la collecte, le stockage, l'utilisation et la diffusion des informations personnelles par les agences fédérales[55]. De plus, le Bureau s'assure que les évaluations concernant la vie privée (« *Privacy Impact Assessments* », P.I.A.) sont bien effectuées par les agences fédérales lorsque sont mises en œuvre des nouvelles collectes d'informations personnelles ou bien lorsque de nouvelles technologies sont appliquées à des données personnelles[56]. Enfin, le Bureau s'assure que le droit fondamental des individus d'avoir connaissance des activités du gouvernement est respecté[57]. Concernant la mise en œuvre de ce mandat, le *Homeland Security Act* de 2002[58] porte création du poste de Haut responsable de la protection de la vie privée (*Chief Privacy Officer*). En vertu du paragraphe 5 de la section 222 de la loi américaine de 2002 sur la sécurité intérieure[59], le *Chief Privacy Officer* doit soumettre au Congrès un rapport annuel portant sur les activités du D.H.S. ayant une incidence sur la protection de la vie privée, et faire état des plaintes

[52] *The Passenger Name Record (PNR) Framework Decision*. Report with Evidence, UK House of Lords, European Union Committee, 15th Report of Session 2007, p. 22 ; disponible sur www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf.

[53] *Privacy impact assessment for the Automated targeting system,* August 3, 2007, U.S. Department of Homeland Security, p. 5.

[54] *Code of Federal Regulations,* Title 19, Volume 1, [Revised as of April 1, 2005], 19CFR122.49d, Sec. 122.49d Passenger Name Record (PNR) information ; disponible sur http://edocket.access.gpo.gov/cfr_2006/aprqtr/19cfr122.49d.htm.

[55] *Privacy Act,* Public Law No. 93-579, 88 Stat. 1897 (Dec. 31, 1974), as amended (5 U.S.C. § 552a).

[56] *E-government Act*, Public Law 107-347, H.R. 2458/S. 803, 17 December 2002.

[57] *Freedom of Information Act* of 1966, Public Law No. 110-175, 121 Stat. 2524, as amended (5 U.S.C § 552), 4 July 1966.

[58] *Homeland Security Act*, Public Law 107–296, 107th Congress, 116 STAT. 2135, Section 222(a)(2).

[59] *Idem*.

éventuelles pour atteinte à la vie privée. Ce faisant, le mandat du Bureau de la confidentialité est clairement défini par la loi et semble être un organe impartial considérant le caractère diversifié et proportionnel de la représentation au sein des différents comités consultatifs et notamment le Comité consultatif sur la confidentialité et l'intégrité des données (*Data Privacy and Integrity Advisory Committee*). Cependant, le fait que le Bureau présente un rattachement institutionnel étroit avec le D.H.S. compromet le caractère indépendant de cet organe, ne serait-ce qu'en application de la théorie des apparences. Qui plus est, le mandat des membres de ce comité est de quatre ans et le mode d'élection consiste en la nomination des membres par le Secrétariat du D.H.S.[60], élément qui constitue difficilement une garantie d'indépendance.

Les principales actions de profilage des passagers des vols commerciaux sont effectuées par la T.S.A. et le C.B.P. néanmoins ces administrations sont placées sous l'autorité du D.H.S. En ces termes, ces deux administrations dépendent du Bureau de la confidentialité pour toutes les questions et litiges relatifs à la protection de la vie privée des passagers. En vertu du rapport d'évaluation sur la vie privée, rendu par le D.H.S. le 3 août 2007[61], les données P.N.R. contenues dans le module A.T.S. - P. ne satisfont pas à la définition adoptée par le Congrès[62] du terme « fouille de données » (« *data mining* »). Car selon le D.H.S., les données P.N.R., sont fondées sur des informations prévisibles et contextuelles et elles ne sont pas utilisées afin de déterminer le degré de dangerosité mais plutôt vise un procédé de comparaison avec d'autres bases de données : « […] *A.T.S. - P compares P.N.R. and information […] against lookouts and patterns of suspicious activity identified through past investigation and intelligence* ». En quelque sorte, le D.H.S. affirme ne pas utiliser les données P.N.R. afin d'augmenter le nombre de profils à risque ; l'objectif est plutôt l'identification d'activités illégales. Au départ, le système A.T.S. est complété par le programme C.A.P.P.S. qui est un système rudimentaire administré non pas par le gouvernement mais par les compagnies aériennes. Effectivement, les compagnies aériennes examinaient seulement quelques éléments lors de la réservation d'un vol et notamment le mode de paiement ou bien le type de voyage effectué par le passager. Dès le mois de février 2002[63], le gouvernement travaille à l'établissement du système C.A.P.P.S. II, désormais géré par l'administration fédérale. Ce système entretenu par la T.S.A. constitue un moyen de « fouille de données » en ce qu'il est utilisé comme un système d'alerte précoce (dès la réservation), afin de catégoriser les individus selon leur degré de « risque » par le biais d'informations fournies par les

[60] *Department of Homeland Security Data Privacy and Integrity Advisory Committee Charter*, 26 April 2004, Membership, p. 2.

[61] *Privacy Impact Assessment for the Automated Targeting System*, August 3, 2007, U.S. Department of Homeland Security, p. 11.

[62] *Conference Report on HR 5441, DHS Appropriations Act*, House Report No. 109-699, Sept. 28, 2006, H7784, at H7815. La définition du terme « data mining » est la suivante: « *(...) a query or search or other analysis of one or more electronic databases, whereas – (A) at least one of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement; (B) a department or agency of the Federal Government or a non-Federal entity acting on behalf of the Federal Government is conducting the query or search or other analysis to find a predictive pattern indicating terrorist or criminal activity; and (C) the search does not use a specific individual's personal identifiers to acquire information concerning that individual* » .

[63] O'HARROW Robert, "*Intricate Screening of Fliers in Works*", Washington Post, 1er février 2002

services de renseignement et de diverses données commerciales. En février 2004, le G.A.O. affirmait que C.A.P.P.S. II n'offrait pas une garantie suffisante de la protection de la vie privée des individus, compte tenu de l'échec de la T.S.A. concernant sept tests sur huit demandés par le Congrès[64]. Par conséquent, ce programme a été abandonné dès le mois de juillet 2004. Dès lors, le G.A.O. joue un rôle important quant au respect du droit à la vie privée des citoyens. En tant qu'organe indépendant du Congrès, il a pour mandat d'enquêter sur les modalités de dépenses des fonds publics par le gouvernement fédéral et sur l'aptitude du gouvernement à remplir sa mission. Pourtant, le G.A.O. ne constitue pas stricto sensu un organe dévolu à la protection des données personnelles. Ainsi, il n'existe aucune Autorité chargée de la protection des données (A.P.D.) telle que celles instituées au sein de chaque État membre de l'U.E.

2. Les garanties de la protection du droit à la vie privée

Dans le domaine du secteur public, les États-Unis ont adopté plusieurs lois permettant d'organiser le fonctionnement des agences fédérales qui ont accès à un nombre croissant de bases de données personnelles. Le *Privacy Act* de 1974[65], le *Freedom of Information Act* de 1966 et le *Intelligence Reform and Terrorism Prevention Act* de 2004 sont des lois applicables de manière générale à la collecte et à la gestion des informations personnelles, à la différence d'autres législations qui concernent des domaines spécifiques, hors du cadre de la présente étude[66]. Le *Privacy Act* et le *Freedom of Information Act* sont des législation applicables aux bases de données utilisées dans le domaine de la sûreté aérienne mais leur application est restreinte, notamment à l'encontre des ressortissants de l'Union européenne. Quant au *Intelligence Reform and Terrorism Prevention Act*, celui-ci concerne la rationalisation de la structure globale et de la coordination entre les agences de renseignement et la mise en œuvre du programme *Secure Flight* par la T.S.A.

a. Le *Privacy Act* et le *Freedom of Information Act*

En premier lieu, la loi sur la vie privée (*Privacy Act*) votée en 1974, limite l'accès aux dossiers personnels collectés par le gouvernement; le dossier P.N.R. entre donc directement dans le champ d'application de cette loi. En outre, le *Privacy Act* régi expressément la façon dont le gouvernement peut collecter et diffuser des informations sur ses citoyens. En vertu de ses dispositions, la loi affirme le respect du droit à la confidentialité et à la vie privée et garanti l'intégrité des données personnelles. De cette façon, les agences doivent rendre compte des modalités d'utilisation de ces bases de données par le bais de rapports

[64] "*Aviation Security, Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges",* U.S. G.A.O., Report to Congressional Committees, February 2004, p. 15.
[65] *Privacy Act* of 1974, 5 U.S.C. § 552a (1976).
[66] A titre d'exemple, citons le *Right to Financial Privacy Act* of 1978, 12 U.S.C. §§ 3401-22 (Supp. II 1978).

annuels[67] et assurer un droit d'accès à l'individu qui le requiert[68]. Concernant la divulgation de ces données personnelles, le *Privacy Act* dispose que l'agence fédérale doit obtenir le consentement de l'individu, à moins que cette divulgation ne réponde à une utilisation de routine[69]. La divulgation de ces informations en vue de la protection de la sécurité nationale constitue l'exception majeure à l'obtention de ce consentement[70]. Dans ce contexte, les agences fédérales sont seulement habilitées à obtenir les informations « pertinentes et nécessaires »[71] afin d'exécuter leur mission. Néanmoins, le *Privacy Act* ne s'applique pas aux bases de données détenues par la C.I.A. ni aux dossiers personnels entretenus par le *National Security Council*, le Ministère de la Défense, le Département de la Justice, le *State Department*, le Ministère du Trésor et le Ministère des Transports[72]. Concernant le champ d'application du *Privacy Act*, celui-ci concerne uniquement les citoyens américains et les résidents permanents[73]; les ressortissants étrangers, incluant les citoyens de l'Union européenne, sont donc exclus du *Privacy Act*[74].

Cette problématique a été évoquée lors des négociations des modalités de coopération entre les États-Unis et Europol[75] au lendemain du 11 septembre. Cette coopération concerne particulièrement Europol et le F.B.I. par l'entremise du *Counter Terrorism Task Force* (C.T.T.F.). Un accord de coopération a été conclu le 6 décembre 2001 portant sur l'échange d'informations mais, étant donné l'inapplicabilité aux citoyens européens des dispositions américaines relatives à la protection de la vie privée[76], les données personnelles étaient exclues de l'accord. Cette autorisation concernant l'échange de données personnelles, incluant les données sensibles, a été accordée par l'accord conclu le 20 décembre 2002. Cet accord présente des difficultés notamment car il autorise l'accès des entités et personnes privées[77] contrairement à la

[67] *Ibid*., 5 U.S.C. § 552a(e)(4).

[68] *Ibid*., 5 U.S.C. § 552a(f), § 552a(d).

[69] *Ibid*. 5 U.S.C. § 552a(b).

[70] GREENAWALT Kent, "*Legal Protections of Privacy*" 67 (Final Report to the Office of Telecommunications Policy, Executive Office of the President, August 4, 1975).

[71] *Ibid*. 5 U.S.C. § 552a(e)(1).

[72] "*Privacy Act of 1974 - Summary of Exemptions by The Authority and Agency and Privacy Act of 1974 -Summary of Systems Exempted by Agency*" *in* Fifth Annual Report of the President on the Implementation of the Privacy Act of 1974, Calendar year 1979 (1980); Ibid., 5 U.S.C. 552a(j),(k).

[73] *Ibid*. 5 U.S.C. § 552a(a)(2): "*a citizen of the United States or an alien lawfully admitted for permanent residence.*"

[74] Voir à ce propos *Department of Justice, Comments, Overview of the Privacy Act of 1974*, May 2004, « *Compared this definition with the FOIA's much broader "any person" definition* (5 U.S.C. § 552(a)(3) (2000)). See, e.g., *Fares v. INS*, No. 94-1339, 1995 WL 115809, at 4 (4th Cir. 1995) (*per curiam*) ("[*Privacy] Act only protects citizens of the United States or aliens lawfully admitted for permanent residence*."); *Raven v. Panama Canal Co.,* 583 F.2d 169, 170-71 (5th Cir. 1978) (*same as Fares, and comparing "use of the word 'individual' in the Privacy Act, as opposed to the word 'person,' as more broadly used in the FOIA*"); *Cudzich v. INS*, 886 F. Supp. 101, 105 (D.D.C. 1995) (*A plaintiff whose permanent resident status had been revoked "is not an 'individual' for the purposes of the Privacy Act […]. Plaintiff's only potential access to the requested information is therefore under the Freedom of Information Act.*"); disponible sur http://www.usdoj.gov/oip/04_7_1.html.

[75] CHEVALLIER-GOVERS Constance, *De la coopération à l'intégration policière dans l'Union européenne*, Bruxelles, Bruylant, 1999, p. 268 ; 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. 202.

[76] En violation de l'article 8, paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne.

[77] *Agreement between the United States of America and the European Police Office*, 20 December 2002, article 10 ; disponible sur http://www.europol.europa.eu/index.asp?page=agreements.

Convention Europol[78] qui assujettie le droit d'accès à un véto initial. Enfin, l'article 20 de la Convention Europol concernant la correction et la suppression des informations n'a pas été introduit dans l'accord de coopération avec les États-Unis[79].

En second lieu, le *Freedom of Information Act*[80], voté par le Congrès en juillet 1967, est une loi dévolue à la question de la divulgation des informations personnelles. Elle permet de rendre accessibles aux individus les informations collectées par les agences fédérales, sous réserve de différentes exceptions justifiées par l'impératif de sécurité nationale[81]. Dès lors, des données personnelles peuvent être protégées en vertu du *Privacy Act* mais divulguées selon les termes du *Freedom of Information Act*[82]. Parmi les neuf limites prévues par cette loi au libre accès aux documents administratifs de l'État, la septième est consacrée aux " dossiers personnels et médicaux, et les dossiers similaires dont la révélation constitue une invasion injustifiée de la vie privée "[83]. Dès 2003, lors des négociations transatlantiques, le Bureau des douanes (C.B.P) a indiqué que la divulgation de données du dossier P.N.R. auxquelles il a accès est régie d'une manière générale par le *Freedom of Information Act*. En effet, le C.B.P. affirmait considérer les informations du P.N.R. comme des données confidentielles relevant du secret commercial. Mais le Bureau des douanes prévoit dans ses règles de conduite que l'obligation de divulgation inscrite dans le F.O.I.A. ne s'applique pas à ce type de données, sous réserve de quelques exceptions restreintes dans le cas de demandes de la part des passagers concernés. Il ressort des textes[84] que le recours juridictionnel contre le rejet par le C.B.P. d'une demande de divulgation doit être précédé d'un recours administratif devant le *Appeals Officer*. Si le refus de divulgation persiste à l'issue de ce recours administratif, le demandeur peut alors introduire un recours juridictionnel devant une Cour fédérale de District, qui est compétente pour ordonner la divulgation de toute information erronément refusée par un organisme gouvernemental.

b. Rationalisation de l'architecture institutionnelle par le biais du *Intelligence Reform and Terrorism Prevention Act*

Cette nouvelle législation du 12 décembre 2004 sur la communauté du renseignement atteste d'un effort de rationalisation du système initié par le Congrès américain. Le *Intelligence Reform and Terrorism Prevention Act* porte création du *National Counterterrorism Center* (N.C.T.C.) qui coordonne l'ensemble des services pour le renseignement visant la lutte antiterroriste, clarifiant ainsi le partage des compétences.

[78] *Europol Convention - Consolidated Version* - , Article 19, Right of access; disponible sur http://www.europol.europa.eu/index.asp?page=legal.

[79] Article 20.4 of the Europol Convention: "*Any person shall have the right to ask Europol or correct or delete incorrect data concerning him*".

[80] *Freedom of Information Act* of 1966, 5 U.S.C. § 552 (1976).

[81] *Idem*, 5 U.S.C. § 552(b).

[82] D. O'BRIEN, "*Privacy, Law and Public Policy*" 218 (1979) ; *Ibid.* 5 U.S.C. § 552a(b)2.

[83] *Ibid*. 5 U.S.C. § 552(b).

[84] Titre 5, section 552(a)(4)(B) du code des États-Unis et Titre 19, section 103.7-103.9 du Code des règlements fédéraux.

Par ailleurs, le *Director of National Intelligence* (D.N.I.) supervise désormais la communauté du renseignement américain[85]. En parallèle, le programme C.A.P.P.S. II est dissout par le Congrès dès le mois de juillet 2004. La T.S.A. a donc remplacé ce programme par la base de données *Secure flight*, applicable aux vols intérieurs et aux transporteurs américains. Selon la T.S.A., cette nouvelle base de données respecte les recommandations émises par le Congrès et le G.A.O. dans la mesure où le *Secure flight* ne comporte plus de classement des passagers et ne vise plus à rapprocher l'identité des passagers avec des bases de données privées[86]. De nouveau, la T.S.A. invoque les conclusions de la Commission d'enquête sur les attentats du 11 septembre 2001 qui estime en premier lieu qu'il incombe aux compagnies aériennes d'appliquer « *les ordres du gouvernement visant à empêcher certains suspects du terrorisme identifiés de monter dans les vols commerciaux et à faire subir un second contrôle de dépistage aux autres* »[87]. En second lieu, la Commission recommande que « *les transporteurs aériens devraient être tenus de fournir les informations nécessaires à tester et mettre en pratique ce nouveau système* » et ce, afin d'élaborer les « *no fly lists* » et les « *selectee lists* »[88]. L'objectif du *Secure flight program* est donc de comparer les identités des passagers des vols domestiques aux listes de suspects contenues dans les banques de données du gouvernement. Afin de tester ce programme, la T.S.A. a édicté un règlement au mois de juin 2004[89] qui ordonne à soixante-douze compagnies aériennes américaines de lui communiquer leurs fichiers correspondant aux vols effectués au mois de juin 2004. Ce faisant, on constate qu'à l'origine de la mise en œuvre du programme *Secure flight*, le législateur n'avait pas habilité la T.S.A. à utiliser ce programme. Cette habilitation n'a été accordée que le 17 décembre 2004 par la Loi sur la réforme des services de renseignements et sur la prévention du terrorisme. La section 4012 de cette loi précise que les compagnies aériennes sont tenues de fournir les données P.N.R. à la T.S.A., une fois la phase de test achevée. Le programme de test est supposé disposer d'un accès limité aux données à caractère commercial afin de vérifier l'identité des individus[90]. Enfin, le *Secure flight program* inclue l'établissement du Bureau de la protection de l'identification (*Office of Identification Protection*) qui prévoit une procédure d'appel pour les passagers lésés par une confusion d'identité.

---

[85] DASQUIÉ Guillaume, « *Quels outils et méthodes utilisés aux Etats-Unis et au Canada pour procéder à l'analyse stratégique du renseignement de sécurité intérieure ? Comparaison des agences de renseignement de ces deux pays (organisation, missions, moyens, efficience)* », 2006 ; disponible sur www.irisfrance.org/docs/consulting/2006_renseignement.pdf.

[86] Rapport d'information n° 2241 déposé par le délégation de l'Assemblée Nationale pour l'Union européenne, sur la sûreté du transport aérien en Europe, et présenté par M. Thierry Mariani, député, « (1) Les mesures prises à l'intérieur des États-Unis, Le contrôle des passagers », 12 avril 2005.

[87] *The 9/11 Commission Report*, The National Commission on Terrorist Attacks Upon the United States, "A Layered Security System", p. 393.

[88] *Idem*.

[89] *Department of Homeland Security, Transportation Security Administration*, TSA-2004-19160, Notice of Final Order for Secure Flight Test Phase ; Response to Public Comments on Proposed Order and Secure Flight Test Records ; disponible sur http://www.tsa.gov/press/releases/2004/press_release_0537.shtm.

[90] *Briefing with Department of State's Bureau of Consular Affairs*, Oct. 23, 2003.

II. - Le renforcement de la sûreté aérienne comme fondement du partenariat euro-américain

La régulation de la sûreté aérienne est devenue une composante à part entière de la sécurité intérieure des États notamment depuis les attentats du 11 septembre. Cette atteinte sans précédent à la souveraineté et à la sécurité nationale a participé de l'émergence d'une politique européenne de sûreté de l'aviation civile, mettant en jeu des acteurs publics et privés. Au sein de l'Union européenne, la réaction aux attentats du 11 septembre en matière de sûreté aérienne révèle un mode opératoire spécifique et complémentaire d'un point de vue institutionnel. Cependant, les États se voient dessaisis d'une partie de leur gestion de la sûreté par les instances européennes (notamment la Commission) mais aussi par les organisations internationales (O.A.C.I.) en charge de la sûreté de l'aviation civile. Un phénomène parallèle s'est développé aux États-Unis et consiste en une protection renforcée des frontières, et par conséquent, en la multiplication des contrôles des individus transitant dans les aéroports internationaux. La notion de souveraineté nationale est ainsi étendue et justifiée au nom de la lutte contre le terrorisme et implique l'exportation de normes sécuritaires par le truchement d'un rapport de force économique favorable. *De facto*, la coopération internationale dans ce domaine, qui visait initialement à prévenir des actes criminels et à améliorer les conditions de poursuite et de jugement, s'est muée aujourd'hui en une régulation contraignante par le biais d'actes juridiques à caractère obligatoire.

A. - L'Union européenne sous contrainte ?

Initialement, l'Union européenne était particulièrement absente dans le domaine de la sûreté aérienne. Bien qu'elle ait pu acquérir un rôle de premier plan via l'action de la Commission, la question de la sûreté était néanmoins dévolue aux agences de police aéroportuaires. Les évènements du 11 septembre ont entraînés la négociation d'un outil juridique impliquant l'échange de données personnelles vers les États-Unis mais ces négociations ont été précipitées du fait de l'existence d'arguments économiques. En effet, la menace de sanctions économiques ou d'interdiction d'atterrissage envers les compagnies aériennes se refusant à transmettre ce type de données, a été le point de départ des négociations juridiques entre l'Union européenne et les États-Unis. Cet élément, conjugué avec les recommandations émanant des organisations internationales en charge de la sûreté de l'aviation civile, présente le cadre et les prémisses des négociations de l'accord P.N.R.

1. Au niveau international : recommandations de l'O.A.C.I. et dispositions de l'Annexe 17

L'Annexe 17 à la Convention relative à l'aviation civile internationale[91] définit la sûreté comme « la combinaison des mesures ainsi que des moyens humains et matériels visant à protéger l'aviation civile

[91] Annexe 17 à la Convention relative à l'aviation civile internationale, Normes et pratiques recommandées internationales, Sûreté, Protection de l'aviation civile contre les actes d'intervention illicite, Huitième édition, avril 2006.

contre les actes d'intervention illicite ». Les mesures de sûreté sont donc applicables au sol et en vol. L'échange des données personnelles entre les transporteurs aériens dans le cadre des données de type P.N.R. est une composante essentielle des mesures de sûreté au sol, autrement dit, des mesures mises en œuvre par les autorités aéroportuaires et les services de douanes concernant les vols internationaux.

a. Le point de départ : les données de type R.P.C.V.

Les systèmes de renseignements préalables concernant les voyageurs (R.P.C.V.) sont des systèmes d'inspection aux frontières qui visent à faciliter le contrôle des passagers. L'O.A.C.I. définit les R.P.C.V. comme des « *renseignements essentiels sur une personne mis à la disposition d'un État avant l'arrivée de la personne dans le pays. Les données clés R.P.C.V. sont : le nom complet du voyageur, sa date de naissance, son sexe, sa citoyenneté ou sa nationalité, ainsi que le type de document de voyage, le pays émetteur et le numéro du document. Le P.N.R. est différent des R.P.C.V., qui sont principalement recueillis par les exploitants au nom des États* »[92]. La Division de la Facilitation de l'Organisation de l'aviation civile internationale (O.A.C.I.) s'est particulièrement intéressée à ces données R.P.C.V., données dites A.P.I., dont l'utilisation a précédé celle des données P.N.R. En effet, la Convention de Chicago exige des États contractants qu'ils simplifient les formalités de contrôles frontaliers et qu'ils adoptent des formalités de douane et d'immigration normalisées à l'échelle internationale[93].Par ailleurs, l'Annexe 17 préconise que: « *Chaque État contractant adoptera des mesures pour que les passagers au départ de vols de transports aérien commercial et leurs bagages de cabine soient soumis à une inspection/filtrage avant l'embarquement dans un aéronef au départ d'une zone de sûreté à accès réglementé* »[94]. Une proposition concernant l'identification préalable des voyageurs a été introduite pour la première fois à l'O.A.C.I. lors de la dixième session de la Division de la facilitation en 1988[95].

L'intensification des contrôles de sûreté grâce au système R.P.C.V. est considéré comme un outil efficace de lutte contre le terrorisme ; c'est la raison pour laquelle des États ont souhaité élargir le contenu de ces données en exigeant des données supplémentaires disponibles dans les systèmes de réservation des

[92] Lignes Directrices sur les données des dossiers passagers (P.N.R.), Cir 309 AT/131, Organisation de l'aviation civile internationale, avril 2006, Annexe 3, Glossaire, p. 13.

[93] Convention relative à l'aviation civile internationale, Article 22, « Simplification des formalités », et article 23, « Formalités de douane et d'immigration », in Division de la facilitation - Douzième session, FAL/12-WP/15 13/1/04, « 2.4 : Renseignements préalables concernant les voyageurs (RPCV) ».

[94] Annexe 17 à la Convention relative à l'aviation civile internationale, « 4.4 Mesures applicables aux passagers et à leurs bagages de cabine ».

[95] La version la plus récente de cette disposition est libellée comme suit : « *Il est recommandé que, lorsqu'il y a lieu, les États contractants introduisent un système de renseignements préalables concernant les voyageurs (R.P.C.V.), qui suppose la saisie de certains renseignements figurant sur les passeports ou les visas avant le départ, la transmission de ces renseignements par des moyens électroniques à leurs pouvoirs publics, et l'analyse de ces renseignements aux fins de la gestion des risques par les pouvoirs publics avant l'arrivée, afin d'accélérer le congé. Afin de réduire au minimum les formalités à l'enregistrement, il faudrait utiliser des dispositifs de lecture des documents pour la saisie des renseignements figurant dans les documents de voyage lisibles à la machine* », Ibid., Supplément à l'Annexe 17, Extraits de l'Annexe 9 – Facilitation - , Chapitre 3 (K), « Procédures d'entrée et responsabilités », « 3.47 Pratique recommandée ».

exploitants d'aéronefs. La question de la collecte des données P.N.R. a été soulevée pour la première fois lors de la douzième session de la Division de la facilitation en 2004. La Division a alors adopté la Recommandation B/5 qui stipule : « *Il est recommandé que l'O.A.C.I. élabore des éléments indicatifs pour les États qui peuvent exiger l'accès aux données des dossiers passagers (P.N.R.) pour compléter les données d'identification reçues par le truchement d'un système R.P.C.V., notamment des directives sur la distribution, l'utilisation et le stockage des données et une liste composite d'éléments de données qui peuvent être transférés entre l'exploitant et l'État récepteur* »[96]. Dès 2004, le Secrétaire général de l'Organisation a créé un groupe d'étude du Secrétariat, le panel d'experts de l'O.A.C.I. sur la sûreté de l'aviation civile (*Aviation Security Secretariat Study Group,* A.V.S.E.C.P.) en charge de la rédaction de lignes directrices concernant le transfert des données P.N.R.

b. Standardisation des procédures de transfert des données P.N.R.

En vue d'améliorer la sûreté aérienne et d'accélérer les formalités dans les aéroports en matière de douane et d'immigration, les États-Unis, le Canada et l'Australie ont adopté des législations exigeant que les données P.N.R. soient mises à leur disposition avant le décollage. Selon la position commune de la Communauté européenne et de ses États membres[97], il apparaît nécessaire de préciser, au niveau international et dans le cadre de l'O.A.C.I., des normes et pratiques uniformes relativement au transfert des données P.N.R. entre transporteurs. Les États membres ont proposé d'examiner, sur la base des éléments existants en matière de données P.N.R., le nombre et l'étendue des données strictement nécessaires au maintien de l'ordre et à l'amélioration de la sûreté aérienne. Cette initiative européenne envisage aussi la question de la responsabilité des transporteurs aériens et d'autres opérateurs économiques concernés par le traitement de données P.N.R. : cette responsabilité doit être dégagée en cas d'omissions ou pour ce qui est de l'exactitude ou de l'authenticité des données, sur lesquelles ils n'ont aucun contrôle. Aux termes de l'article 13 de la Convention de Chicago, les lois et les règlements d'un État contractant concernant l'entrée ou la sortie de son territoire des passagers des aéronefs doivent être observés dans la mesure où les États disposent d'un pouvoir discrétionnaire sur les informations qu'ils exigent concernant les personnes qui demandent l'entrée dans leur territoire. Néanmoins, faisant suite à la proposition européenne, le Conseil de l'O.A.C.I. a adopté une pratique recommandée à inclure dans l'Annexe 9 à la Convention de Chicago : « *Il est recommandé que les États contractants qui exigent l'accès aux dossiers passagers (P.N.R.) adaptent leurs demandes de données et le traitement de ces données aux lignes directrices de l'O.A.C.I.* »[98].

[96] Avant-propos des Lignes Directrices sur les données des dossiers passagers (P.N.R.).

[97] Division de Facilitation (FAL) - Douzième session, doc. FAL/12-WP/75, « *Un cadre international pour le transfert des données PNR* », Note présentée par l'Irlande au nom de la Communauté européenne et de ses États membres, 15 mars 2004.

[98] Avant-propos des Lignes Directrices sur les données des dossiers passagers (P.N.R.).

En effet, ces lignes directrices posent le postulat selon lequel le transfert des données P.N.R. est un outil efficace de lutte contre le terrorisme et, en vertu de la recommandation 3.2, l'O.A.C.I. vise à encadrer cette procédure. Tout d'abord, les recommandations de l'O.A.C.I. concernent l'obligation de transfert qui doit être fondée sur une loi mentionnant par ailleurs les raisons de ce transfert[99]. Aussi, la collecte des éléments de données P.N.R. doit strictement viser les buts explicités à la section 2 du document (lutte contre le terrorisme, amélioration de la sûreté aérienne etc.)[100]. Considérant le traitement de ces données, il doit être limité aux fins précisées pour leur collecte[101]; l'accès aux P.N.R[102] et la période de stockage doivent être limités[103] et le niveau de protection adéquat garanti[104]. Le passager doit bénéficier d'un droit d'accès à fin de correction et modification[105] ainsi que d'un droit de recours[106]. Les lignes directrices abordent aussi la question de la méthode de transfert des données et l'O.A.C.I. préconise l'utilisation du système « *push* » qui « *confère à l'exploitant le rôle de gardien et de contrôleur des données P.N.R.* »[107]. Quant au filtrage des données, des mécanismes appropriés doivent garantir que seuls les éléments du P.N.R. sont recueillis par les exploitants d'aéronefs ou extraits par les autorités publiques compétentes[108]. Le document de l'O.A.C.I. réitère les principes généraux de la protection des données P.N.R. : l'État doit assurer que chaque autorité ayant accès aux données garanti un niveau de protection adéquat[109]. Le traitement des données sensibles doit prendre en considération l'équilibre entre les droits des passagers à la non divulgation de ces données et l'intérêt qu'elles représentent pour les autorités publiques pour ce qui est du maintien de l'ordre et de l'amélioration de la sûreté aérienne[110]. Qui plus est, la sécurité et l'intégrité des P.N.R. doivent être respectés; le traitement doit être conforme aux mesures de protection telles que l'authenticité et la confidentialité[111]. Enfin, les lignes directrices garantissent la transparence et le recours des passagers. L'exploitant d'aéronef doit aviser de façon adéquate le passager qu'il peut être amené à communiquer ses données P.N.R. aux autorités d'un État et en expliciter les raisons[112] tandis que l'État doit garantir au passager un droit d'accès à ces données, un droit de correction ou de modification[113] et un recours adéquat en cas de traitement illégitime des données P.N.R.[114]

[99] Recommandation 4.1.
[100] Recommandation 5.1.
[101] Recommandation 6.2 (a).
[102] Recommandation 6.2 (b).
[103] Recommandation 6.2 (d).
[104] Recommandation 6.2 (c).
[105] Recommandation 6.2 (e).
[106] Recommandation 6.2 (f).
[107] Recommandation 7.3.
[108] Recommandations 9.2.
[109] Recommandation 12.1.
[110] Recommandation 12.3.
[111] Recommandation 13.1.
[112] Recommandation 14.1.
[113] Recommandation 14.3.
[114] Recommandation 14.4 .

2. Au niveau européen : le Document 30 de la C.E.A.C.

La Conférence européenne de l'aviation civile (C.E.A.C.) a été créée en 1955 sur une initiative conjointe du Conseil de l'Europe et de l'O.A.C.I. En vertu de l'article 55 de la Convention de Chicago, la C.E.A.C. est un organe indépendant de l'O.A.C.I. dont elle reprend néanmoins les missions pour sa zone géographique. Son mandat consiste en l'harmonisation des politiques et pratiques de ses membres et vise l'exportation de ses standards au niveau mondial. La compétence matérielle de la C.E.A.C. dépasse celle de l'Union européenne ; celle-ci est composée de quarante-quatre États membres et constitue ainsi l'organisation relative à l'aviation civile couvrant le nombre le plus étendu d'États en Europe. Du point de vue du mode de fonctionnement, la C.E.AC. présente une légitimité et une efficacité accrues en matière de gestion de la sûreté de l'aviation civile considérant le consensus qui est nécessaire à la prise de décision en son sein à la différence du processus communautaire qui est considéré comme contraignant[115]. En matière de sûreté de l'aviation civile, l'activité de la C.E.A.C. a pour fondement le Manuel de recommandations et de résolutions, aussi appelé Document 30, adopté en 1985. Ce manuel est régulièrement mis à jour et constitue un texte de référence ; en effet, la mission de la C.E.A.C. est de s'assurer de la conformité des règlements de l'Union européenne et des Communautés européennes aux dispositions du Manuel. Le Document 30 est divisé en deux parties : la première partie est consacrée à la Déclaration de politique de la C.E.A.C. dans le domaine de la facilitation de l'aviation civile tandis que la seconde partie concerne les recommandations de l'organisation dans les domaines opérationnels et techniques. A l'origine, les recommandations de la C.E.A.C. étaient facultatives et leur mise en œuvre demeurait à la discrétion des États européens. Néanmoins, les évènements du 11 septembre 2001 ont eu un impact important sur l'évolution de la politique européenne. Depuis lors, on observe l'établissement d'une politique européenne relative à la sûreté aérienne qui tend à une uniformisation des législations des États membres et à une sécurisation accrue des frontières.

Suivant l'adoption des mesures américaines de renforcement de la sécurité intérieure, une action parallèle a été mise en œuvre par l'Union européenne. Deux étapes majeures illustrent le processus d'établissement de cette politique européenne de sûreté aérienne. En premier lieu, le règlement du Conseil du 16 décembre 2002 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile[116] rend obligatoire, à compter du 19 janvier 2003, l'application des recommandations de la C.E.A.C. contenues dans le Document 30. Par conséquent, les États membres doivent mettre en place des normes communes en matière de sûreté, incluant des dispositions relatives à l'encadrement du contrôle des passagers des vols

[115] POINCIGNON Yann, « *Aviation civile et terrorisme : naissance et enjeux d'une politique européenne de sûreté des transports aériens* », *Culture & Conflits*, n° 56, 2004, pp. 83-119, disponible sur http://www.conflits.org/index1632.html.

[116] Règlement (CE) n° 2320/2002 du Parlement européen et du Conseil du 16 décembre 2002 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile - Déclaration interinstitutionnelle, *Journal officiel* n° L 355 du 30 décembre 2002, pp. 1–22.

commerciaux. Ce règlement autorise la Commission à procéder à des inspections afin de contrôler la mise en œuvre des dispositions communautaires. La seconde étape de ce processus est marquée par l'adoption, sur une initiative de l'Espagne, de la directive du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers avant la fin de l'enregistrement[117]. De nouveau, on constate la réactivité des États membres et de l'Union européenne quant à l'élaboration de mesures renforcées de lutte contre le terrorisme. De la même façon que les États-Unis ont réactivé leur politique de sécurité intérieure à la suite de l'attaque contre le World Trade Center et le Pentagone, l'Union européenne a réagit immédiatement aux attentats de Madrid du 11 mars 2004 en accentuant les contrôles aux frontières. La méthode atteste de la volonté de faire du territoire national une zone hermétique et sécurisée. Les compagnies aériennes doivent désormais transmettre, à la demande des autorités chargées du contrôle des personnes aux frontières extérieures, les renseignements concernant les passagers. Les États membres possèdent donc la même compétence que celle que se sont octroyée les autorités américaines en demandant le transfert des données P.N.R.

Lors de la 33ème session de la Division de la Facilitation de la C.E.A.C., la déclaration de principe relative aux systèmes de renseignements préalables concernant les voyageurs a été adoptée à l'unanimité. Cette déclaration comporte quatorze principes essentiels que les États membres doivent prendre en compte afin d'introduire un système R.P.C.V. Ces principes ont été insérés comme Annexe M au Document 30, partie I. Ils visent à éviter des approches gouvernementales divergentes. Ces principes ont été utilisés pour la mise en œuvre par les États membres de la directive du Conseil du 24 avril 2004. L'objectif était de faciliter l'application des procédures R.P.C.V. pour le voyage des passagers et le contrôle aux frontières tout en constituant un outil efficace à des fins de lutte contre le terrorisme. Considérant la section 3.1[118], le Document 30 aborde la problématique du « traitement anticipé des données » et l'Annexe M[119] présente les principes essentiels à respecter quant au traitement des données de type R.P.C.V.[120]. Aussi, le Document 30 dispose que : « *Avant toute mise en œuvre opérationnelle d'un système R.P.C.V., les États membres devraient permettre aux exploitants de disposer d'un temps raisonnable pour établir une infrastructure et des procédures efficaces afin de répondre efficacement aux exigences* »[121].

[117] Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *Journal officiel* n° L 261/24 du 6 août 2004.

[118] Déclaration de politique de la CEAC dans le domaine de la facilitation de l'aviation civile, ECAC.CEAC, DOC N° 30 (Partie I), 10ème édition, décembre 2006, p. 13.

[119] *Idem*, p. 80.

[120] Les États sont invités à se reporter aux lignes directrices O.M.D. (Organisation mondiale des douanes)/I.A.T.A. (International air transport association)/O.A.C.I. de mars 2003 et à la déclaration de principes émanant du Groupe de travail de I.A.T.A. concernant les autorités de contrôle (C.A.W.G.) relative aux R.P.C.V. de novembre 2003, cf. IATA/CAWG *Statement of principles for Advance Passenger Information Systems*, ICAO, Facilitation (FAL) Division-Twelfth Session, Cairo, Egypt, 22 March to 2 April 2004, FAL/12-WP/60, p. 4.

[121] *Idem*, article 2 (vii), p. 81.

B. - L'expérience du transfert des données personnelles vers les États-Unis

Le recueil de données personnelles par les États-Unis, bien qu'autorisé dans le cadre de la législation relative à la sûreté de l'aviation civile, s'inscrit dans le contexte global de la politique antiterroriste américaine. Celle-ci est illustrée par le projet « *Total Information Awareness* » (T.I.A.) développé par le *Information Awareness Office* (I.A.O.) au sein du Pentagone depuis les attentats du 11 septembre. Ce projet consiste en la création d'un système automatisé permettant de draguer toutes les formes possibles d'information disponibles pour déceler des activités terroristes. L'I.A.O. entend respecter le droit à la vie privée en conservant les données personnelles recueillies dans une base de donnée dormante ; le traitement de ces données n'intervient que si ces dernières sont reliées à une activité terroriste[122]. Les relations transatlantiques relatives au transfert des données personnelles se situent donc dans ce contexte de renseignement de masse qui débouche de manière quasi nécessaire sur des opérations qui s'effectuent hors des cadres légaux et produisent inévitablement des violations des droits fondamentaux.

1. Un contexte général opaque entourant les relations transatlantiques

Ce contexte opaque est illustré par deux évènements marquants qui auront des répercussions sur la nature des relations diplomatiques entre l'Union européenne et les États-Unis lors de la négociation de l'accord P.N.R. Tout d'abord, il s'agit de la révélation de l'existence du réseau Échelon, système de surveillance satellitaire exploité par les États-Unis, permettant l'interception de communications privées en Europe. En second lieu, il s'agit d'évoquer l'accord secret passé entre les États-Unis et la société belge SWIFT, qui visait à permettre aux autorités américaines, via l'action de la C.I.A., d'avoir accès aux transaction financières effectuées par des centaines de milliers de citoyens de l'Union européenne par son intermédiaire.

a. Le réseau Échelon et l'utilisation des communications privées

Héritage de la guerre froide, ce système de surveillance satellitaire permettait initialement aux cinq pays membres du pacte secret « UKUSA » (États-Unis, Royaume-Uni, Canada, Nouvelle-Zélande et Australie) [123] d'intercepter les communications privées mondiales de nature électronique ou téléphonique. Peu avant le 11 septembre 2001, la révélation de l'existence de ce réseau par le comité consultatif Science and *Technology Options Assessment* (S.T.O.A.) du Parlement a fait craindre une violation de la souveraineté

[122] LEMAN-LANGLOIS Stéphane, « Le *Information Awareness Office* et le projet *Total Information Awareness* », octobre 2003, ERTA, Équipe de recherche sur le terrorisme et l'antiterrorisme ; disponible sur http://erta-tcrg.org/analyses/tia.htm.

[123] Rapport du député Schmid, 18 mai 2005, *Report on The Existence of A Global System For The Interception of Private And Commercial Communications (Echelon Interception System),* Rapport présenté au Comité temporaire sur le système d'interception Échelon, mis en place par le Parlement européen ; et Rapport préliminaire du Comité temporaire sur le système d'interception Échelon, 4 mai 2001, Section 13.2, p.9; disponible à http://vadeker.club.fr/humanite/geopolitique/rapport_echelon_controle_politique.html.

nationale des pays membres de l'Union européenne. Cette crainte a été relayée par des rapports virulents du Parlement européen dénonçant ainsi une atteinte à la protection de la vie privée et aux droits fondamentaux des citoyens européens[124]. Selon cette résolution du Parlement, utilisé à des fins de renseignement, ce système d'écoute et d'analyse des communications n'est pas *stricto sensu* contraire au droit de l'Union européenne. Néanmoins, un État membre viole le droit de l'Union en l'exploitant au profit d'objectifs commerciaux et d'espionnage de la concurrence.

Qui plus est, le Parlement rappelle que l'article 8 de la Convention européenne des droits de l'homme encadre les conditions légales d'interception de communications privées ; les activités des services de renseignement doivent donc s'effectuer dans le respect des droits fondamentaux. Les députés affirmaient déjà leur souhait de l'élaboration d'une convention entre l'Union européenne et les États-Unis garantissant le respect de la vie privée des citoyens des deux parties. Ils invitaient les États-Unis à nouer un « dialogue franc » sur la collecte de renseignements économiques avec les pays européens et appelaient enfin les institutions européennes et les administrations publiques à recourir systématiquement au cryptage. En 2002, un rapport parlementaire belge affirme que le système Échelon contrevient aux dispositions du droit communautaire dès lors qu'il est utilisé dans un but d'espionnage économique[125]. Ce rapport fait ainsi largement référence aux travaux de la commission temporaire Échelon, qui avait été mise sur pied le 5 juillet 2000 par le Parlement européen. Selon les conclusions de ce rapport, la violation du droit est le fait des pays qui interceptent les communications, mais aussi de ceux qui mettent leur territoire à la disposition de pays tiers pour qu'ils puissent se livrer à l'interception des communications[126]. Cette affirmation se fonde sur trois arguments juridiques. Tout d'abord, l'article 3 de la directive 95/46/CE sur la protection des données à caractère personnel n'exclurait pas du champ d'application de la directive le traitement de données ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités relevant du droit pénal. Le deuxième argument repose sur l'article 25 de la directive 95/46/CE qui n'autorise le transfert de données personnelles vers des pays tiers qu'à la condition que ces pays assurent un niveau de protection adéquat. Selon le rapport, cette condition n'est pas remplie car les États-Unis ne prévoient de protection que pour leurs propres citoyens. Le troisième argument se fonde sur l'article 1.3 de la Directive 97/66 sur la protection des données personnelles dans le secteur des communications électroniques. Dans ce contexte, ne sont exclues que les activités concernant la sécurité publique, la défense, la sûreté de l'État et celles relevant du droit pénal. Enfin, les auteurs du rapport estiment que l'existence d'un système d'interception de communications privées menace la réalisation des buts du Traité instituant la

[124] Résolution du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système « Échelon »), 5 septembre 2001, *J.O.,* n° C072E du 21/03/2002, pp. 221-229.

[125] Sénat et Chambre des Représentants de Belgique, Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé « Échelon », 25 février 2002.

[126] YERNAULT Dimitri, « *De la fiction à la réalité: le programme d'espionnage électronique global « Échelon » et la responsabilité internationale des États au regard de la Convention européenne des droits de l'Homme* », Rev. b. dr. Intern., 2000, pp. 134 et s.

Communauté européenne (T.C.E.) et notamment la libre circulation des marchandises, des personnes, des services et du capital. Enfin, elle viole la souveraineté de la Belgique ainsi que la Convention européenne des droits de l'homme.

b. L'affaire SWIFT et la question du transfert des données bancaires personnelles

Le 23 juin 2006, le New York Times révélait l'existence d'un programme de surveillance de la finance internationale mis en place par la C.I.A. depuis les attentats du 11 septembre[127]. Ces révélations ont notamment porté sur le fait que la C.I.A. et le Ministère du Trésor américain ont surveillé pendant des années des millions de données transitant par la Society for *Worldwide Interbank Financial Telecommunication* (SWIFT). SWIFT est une société belge de télécommunication offrant à ses clients du secteur bancaire et financier un système de messagerie sécurisée et standardisée ainsi que divers services financiers. L'essentiel des transferts bancaires internationaux transite ainsi par cette société. L'administration Bush a eu accès aux informations détenues par SWIFT dans le cadre d'un programme de recherche sur les transactions financières liées au terrorisme. Le Secrétaire d'État au Trésor confirme avoir espionné des transactions financières internationales, via SWIFT, afin de lutter contre le terrorisme[128]. Parmi les clients de SWIFT figurent de nombreuses banques européennes; Washington a donc eu accès à des informations concernant des milliers de citoyens européens, comme le rappelle le Parlement européen dans une résolution du 6 juillet 2006[129]. L'ère post-11 septembre 2001 est caractérisée par une évolution exponentielle des législations antiterroristes aux États-Unis, notamment le *Patriot Act*, qui permet l'interception des messages transitant sur le sol américain tant sur base de décisions judiciaires que sur décision des services secrets[130]. C'est dans le cadre d'une de ces législations que dès 2002, l'administration américaine demandait à SWIFT l'accès à certaines données transitant par les États-Unis.

Dès lors, SWIFT a négocié avec l'administration américaine différentes garanties. Le but était d'empêcher de trop graves atteintes à la protection des données à caractère personnel, consacrée comme un droit de l'homme à part entière par l'Union européenne depuis l'adoption de la Charte européenne des droits de l'homme en même temps que le Traité de Nice en 2000. Les institutions européennes se sont immédiatement saisies de cette question afin de se prononcer sur le soupçon de surveillance irrégulière du réseau SWIFT au regard des règles européennes de protection des données personnelles, et en particulier

[127] LICHTBLAU Eric, RISEN James, "*Bank Data Is Sifted by U.S. in Secret to Block Terror*", June 23, 2006, *The New York Times*.

[128] *Terrorist Finance Tracking Program Fact Sheet*, June 23, 2006 ; JS-4340, U.S. Department of the Treasury, disponible sur http://www.treasury.gov/press/releases/js4340.htm.

[129] Résolution du Parlement européen sur l'interception des données des virements bancaires du système SWIFT par les services secrets américains, 6 juillet 2006, P6_TA(2006)0317.

[130] 107th Congress, 24th October 2001. Sur cette mesure et d'autres, lire KERR Orin S., *Internet Surveillance Law After the USA Patriot Act : the Big Brother That Isn't*, The George Washington University Law School, Public Law and Legal Theory Working Paper No. 043.

de celles relatives aux transferts de données personnelles en direction des États-Unis. Dans un avis du 22 novembre 2006[131], le Groupe de l'article 29 a considéré que SWIFT n'a pas respecté les règles européennes de protection des données en acceptant de communiquer aux autorités américaines les données bancaires transitant par son réseau. Le Groupe a considéré que la société SWIFT n'a pas respecté plusieurs dispositions de la directive 95/46/CE en prêtant un concours actif à la mise en œuvre du programme de surveillance des données bancaires et financières par les autorités américaines. Le Groupe considère que l'absence de transparence et de mécanismes effectifs et adéquats de supervision des transferts de données de l'U.E vers la succursale de SWIFT établie aux États-Unis, puis de cette succursale aux autorités américaines, représente un manquement grave aux dispositions de la directive. Il estime que le transfert systématique, massif et à long terme de données personnelles par SWIFT aux autorités américaines, en l'absence de base juridique et sans possibilité de supervision indépendante par les autorités européennes de protection des données, constitue une violation des principes fondamentaux européens. L'avis rappelle qu'un cadre juridique international a été élaboré aux fins de lutter contre le financement du terrorisme. Celui-ci aurait dû être utilisé par les autorités américaines, plutôt que de requérir le concours d'une société européenne sans en informer les institutions de l'Union. Le Groupe considère enfin que les banques détiennent une responsabilité dans cette affaire, même si celle-ci est secondaire.

2. Le P.N.R. et l'opposition témoignée par les transporteurs européens

Après la mise en œuvre des législations américaines sur le territoire national et la demande faite aux compagnies aériennes américaines de transférer les données P.N.R. aux autorités gouvernementales compétentes, les services douaniers fédéraux ont exigé les données P.N.R. des compagnies européennes[132]. Tandis que certaines compagnies ont volontairement mis ces données à la disposition des autorités américaines, d'autres ont refusé en avançant que cela représenterait une violation des règlements communautaires de protection des données. Le choix des compagnies européennes se limite donc soit à la violation des législations américaines, entraînant des amendes élevées et la perte potentielle du droit d'atterrissage, soit à la violation des législations de l'U.E. ou bien des États membres relatives à la protection des données personnelles, entraînant aussi des amendes importantes. Il est à noter qu'une directive du Conseil du 29 avril 2004[133] oblige déjà chaque État membre de l'Union à transmettre les données A.P.I. (*Advanced Passenger Infomation*). Néanmoins, l'intérêt du P.N.R. par rapport aux données A.P.I. est qu'il est disponible avant l'embarquement (vingt quatre heures avant le départ et après

[131] Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), 01935/06/FR, Groupe de travail « Article 29 ».

[132] Cette obligation de transfert est imposée aux compagnies européennes en vertu de la loi [titre 49, section 44909(c)(3) du code des États-Unis] et de ses règlements (provisoires) de mise en œuvre (titre 19, section 122.49 b du code des règlements fédéraux).

[133] Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *Journal officiel de l'Union européenne,* n° L 261/24 du 6 août 2004.

enregistrement) ; il évalue par ailleurs des « indicateurs de risque » ne concernant pas seulement sur les personnes suspectes déjà identifiées. *De facto*, les compagnies aériennes européennes se trouvent dans une situation de vide juridique qui met en danger la liberté de circulation : il n'existe aucune base légale européenne fondant l'obligation pour les transporteurs de transférer le P.N.R. alors que la législation américaine autorise l'imputation de lourdes amendes à leur encontre pouvant atteindre dix mille dollars par vol commercial effectué. En dépit des objections de la Commission européenne, les États-Unis ont persisté à imposer des sanctions aux compagnies aériennes qui ne se conformaient pas à leur loi après le 5 mars 2003.

La compagnie British Airways s'est montrée particulièrement concernée par la nature extensive des demandes américaines qui peuvent être résumées comme suit. D'une part, l'administration requiert l'accès « en ligne » aux systèmes de réservation et de « *check-in* » des compagnies aériennes afin d'avoir connaissance des données P.N.R. Ces données sont alors divulguées aux autorités de douanes au moment de la réservation tandis qu'en parallèle, le système *Departure Control* (D.C.S.)[134] est disponible vingt-quatre heures avant le départ. D'autre part, les autorités américaines demandent l'accès aux données A.P.I. qui est le registre de bord (« *bulk manifest* ») et est envoyé quinze minutes après le départ. Toutes ces informations peuvent être obtenues « en ligne » ou à l'atterrissage ; bien que les compagnies aérienne européennes s'opposaient à l'accès en ligne du fait de la situation d'insécurité juridique que cela créé, ce dernier a été accordé suite à la déclaration conjointe de la Commission et du C.B.P. Les transporteurs européens contestent particulièrement les modalités d'obtention du consentement du passager. Ces modalités sont floues et sont appliquées de manière inégale par les compagnies ce qui créé une situation de concurrence déloyale[135]. En 2007, le trafic des vols transatlantiques commerciaux représentait cinquante-cinq millions de passagers et trois cent quatre-vingt-cinq vols par jour, opérés par quarante-cinq compagnies aériennes, dont huit compagnies américaines et vingt-six compagnies européennes[136]. De tels chiffres attestent d'une pression économique telle que les compagnies aériennes européennes se sont vues dans l'obligation d'accorder l'accès aux données P.N.R.

[134] Le D.C.S. contient la liste des passagers et des informations concernant le vol.

[135] Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures, Séminaire public, « *La protection des données depuis le 11 septembre 2001 : quelle stratégie pour l'Europe ?* » ; disponible à http://www.europarl.europa.eu/comparl/libe/elsj/events/hearings/20030325/pv_fr.htm.

[136] The Association of European Airlines, "*Open Skies: the EU-US Air Transport Agreement*".