

REQUETE EN ANNULATION

A Messieurs les Présidents,
Madame et Messieurs les Juges de la
Cour constitutionnelle
Place Royale, 7
1000 Bruxelles

POUR: L'a.s.b.l. LIGUE DES DROITS DE L'HOMME, représentée par son conseil d'administration, dont le siège social est situé Rue du Boulet, 22, à 1000 Bruxelles,

requérante,

ayant pour conseil Me Jan FERMON et Me Thomas MITEVOY avocats, à 1210 Bruxelles, Chaussée de Haecht, 55, où il est fait élection de domicile pour les besoins de la présente procédure.

La requérante a l'honneur de soumettre à votre censure, en vue de son annulation, la loi du 30 novembre 2009 portant assentiment à l'Accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au Ministère américain de la Sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007 (ci-après « la loi attaquée »).

Cette loi a été publiée au Moniteur belge du 29 décembre 2009.

LES FAITS

Une loi américaine du 19 novembre 2001 (*Aviation and Transportation Security Act* — ATSA) stipule que les compagnies aériennes qui organisent des vols de passagers au départ et à destination des États-Unis doivent mettre les informations qu'elles possèdent sur ces passagers (« *passenger name records* » ou PNR, ci-après « données PNR ») à la disposition du Bureau des douanes et de la protection des frontières (*Bureau of Customs and Border Protection* — CBP), une section du ministère américain de la sécurité intérieure (*Department of Homeland Security* , ci-après « DHS »). Les données PNR sont indispensables à toute réservation d'un vol et sont rassemblées dans des fichiers gérés par les compagnies aériennes.

Depuis février 2003, le CBP exige que chaque transporteur aérien qui organise le transport de personnes au départ et à destination des États-Unis ou à travers le territoire américain lui fournisse un accès électronique à ces données PNR, pour autant que ces données soient rassemblées et stockées dans leurs systèmes de réservation automatisés. Cette exigence des autorités américaines entraînait, pour les compagnies aériennes de l'Union européenne (UE), une violation de la directive 95/46/CE telle que transposée dans la législation des États membres, qui n'autorise pas ces transferts. Cette directive 95/46/CE interdit l'exportation de données à caractère personnel vers des pays tiers à l'UE qui n'offrent pas de niveau de protection adéquat.

Le 28 mai 2004, à la suite d'une décision préalable de la Commission du 14 mai 2004 reconnaissant le caractère adéquat de la protection des données au États-Unis¹, le Conseil de l'UE a conclu un accord entre la CE et les États-Unis sur le traitement de ces données PNR (ci-après, « l'accord de 2004 »). Le 30 mai 2006, la Cour européenne de Justice, saisie d'un recours par le Parlement européen, appuyé par le Contrôleur européen de la protection des données (ci-après « CEPD »), a annulé la décision habilitant le Conseil à conclure cet accord, en raison de sa base juridique inadéquate². La Cour a cependant maintenu les effets de cet accord jusqu'au 30 septembre 2006. Le 19 octobre 2006, un nouvel accord reprenant quasi littéralement les dispositions de l'accord de 2004, a été conclu pour une période expirant le 31 juillet 2007.

Le 23 juillet 2007, le Conseil de l'UE a conclu un nouvel accord avec les États-Unis sur le traitement et le transfert de données PNR³ (ci-après « l'accord »), qui se conforme aux législations américaines selon lesquelles les diverses agences américaines actives dans la lutte contre le terrorisme sont tenues de s'échanger des données, y compris les données PNR. L'accord est accompagné d'une lettre de Paul Rosenzweig, alors Sous-Secrétaire d'État par intérim au ministère américain de la Sécurité intérieure, qui « vise à expliquer la manière dont le (...) DHS assure la collecte, l'utilisation et le stockage des données des dossiers (...) PNR » (ci-après « la lettre du DHS »). Cette lettre précise que « Aucune des mesures exposées dans la présente lettre ne crée ni ne confère aucun droit ou avantage sur toute personne ou entité,

¹ Décision de la Commission 2004/535/CE du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique (JO L 235 du 6.7.2004, p. 11–22).

² CJCE, affaires C-317/04 et 318/04, 30 mai 2006.

³ L'accord a été publié au Journal officiel de l'Union européenne (ci-après « JOUE ») L 204 du 4 août 2007.

privée ou publique, ni aucune voie de droit autre que celle prévue dans l'accord entre l'Union européenne et les Etats-Unis sur le traitement et le transfert de données PNR par les transporteurs aériens signé le... 2007 ». En réponse à la lettre du DHS, la Présidence du Conseil envoyé un courrier dans lequel on lit le passage qui suit : « Les assurances que vous donnez à l'Union européenne telles qu'elles sont exposées dans votre lettre permettent à l'Union européenne d'estimer que, aux fins de l'accord international signé entre les Etats-Unis et l'Union européenne sur le traitement et le transfert des données PNR le... 2007, le DHS assure un niveau adéquat de protection des données PNR. En se fondant sur cette appréciation, l'UE prendra toutes les mesures nécessaires pour décourager les organisations internationales ou les pays tiers de toute intervention dans les transferts de données PNR de l'UE vers les Etats-Unis. L'UE et ses Etats membres encourageront également leurs autorités compétentes à fournir des informations analytiques provenant des données PNR au DHS et aux autres autorités américaines concernées. »

L'accord a été conclu sans consultation préalable du Groupe de travail «ARTICLE 29» sur la protection des données (ci-après « groupe 29 »)⁴, habituellement consulté sur tout projet de décision ayant un impact sur la protection des données. Le 17 août 2007, le groupe 29 a rendu un avis très critique à l'égard de l'accord⁵.

Parallèlement à la fourniture de données PNR aux Etats-Unis, la Commission européenne a présenté en novembre 2007 un projet prévoyant le traitement de données PNR à des fins répressives à l'intérieur de l'UE⁶.

Le 20 décembre 2007, le Contrôleur européen pour la protection des données a rendu un avis sur ce projet concernant des mesures similaires à celles visées dans l'accord de 2007 avec les Etats-Unis. Cet avis conclut: « *Dans son libellé actuel, la proposition n'est pas conforme aux droits fondamentaux, notamment à l'article 8 de la Charte des droits fondamentaux de l'Union, et ne devrait pas être adoptée.* »⁷

Le 1^{er} octobre 2009, le gouvernement a déposé au Sénat le projet de loi d'assentiment à l'accord⁸. Après approbation par les deux chambres, ce projet est devenu la loi du 30

⁴ Ce groupe de travail, établi par l'article 29 de la directive 95/46/CE, est l'organe consultatif indépendant de l'UE sur la protection des données et de la vie privée. Ses tâches sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE. Site web: http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

⁵ Avis du Groupe de travail Article 29 n° 5/2007 « concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure », adopté le 17 août 2007 (disponible sur

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_fr.pdf).

⁶ Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives, présentée par la Commission, COM(2007) 654 final, du 6 novembre 2007.

⁷ Avis du Contrôleur européen pour la protection des données du 20 décembre 2007 sur la proposition de décision-cadre, p 14 (disponible sur: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_FR.pdf)

⁸ « Projet de loi portant assentiment à l'Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au

novembre 2009 portant assentiment à l'Accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au Ministère américain de la Sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007.

Il s'agit de la loi attaquée.

LA RECEVABILITE

L'article 3 des statuts de la requérante se lit comme suit :

"L'association a pour objet de combattre l'injustice et toute atteinte arbitraire aux droits d'un individu ou d'une collectivité.

Elle défend les principes d'égalité, de liberté et d'humanisme sur lesquels se fondent les sociétés démocratiques et qui ont été notamment proclamés par la déclaration des Droits de l'homme et du citoyen de 1789, confirmés par la Constitution belge de 1831, la déclaration Universelle des Droits de l'homme de 1948 et les pactes relatifs aux droits civils et politiques ainsi qu'aux droits économiques, sociaux et culturels, la Convention européenne pour la sauvegarde des droits de l'homme et des libertés fondamentales de 1950 et la Charte Sociale européenne de Turin de 1961.

Elle soutient toute initiative tendant à la formation et à la promotion des droits de l'homme.

L'association poursuit ses objectifs en dehors de tout engagement partisan ou confessionnel".

La loi attaquée contient des ingérences graves de l'autorité publique dans la vie privée de certains citoyens, notamment par la collecte, la transmission, le traitement de données personnelles, parfois sensibles. Comme en témoignent les libellés des moyens ci-après exposés, la loi attaquée est manifestement contraire à l'objet social de la requérante.

A diverses reprises, dans des recours comparables au présent recours, votre Cour a estimé, (e.a. arrêts 69/2003 du 14 mai 2003, 56/2002 du 28 mars 2002, 169/2002 du 27 novembre 2002, n° 95/2008 du 26 juin 2008), que la requérante avait intérêt à solliciter l'annulation de dispositions législatives susceptibles de causer une atteinte arbitraire aux droits d'un individu ou d'une collectivité ou aux principes d'égalité, de liberté et d'humanisme sur lesquels se fondent les sociétés démocratiques ou encore contraires aux dispositions constitutionnelles ou internationales dont son objet consiste à assurer la défense. Tel est le cas de la loi attaquée.

La loi attaquée donne plein effet, dans l'ordre juridique belge, à un accord international qui permet la transmission, le traitement et la conservation pour une longue durée de données personnelles parfois sensibles de personnes, au seul motif qu'elles voyagent en provenance de

Ministère américain de la sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007 », Doc. Parl. Sénat, session 2008-2009, n° 4-1432/1.

ou vers les Etats-Unis. Cet accord a fait l'objet de fortes critiques émanant tant d'autorités nationales et internationales compétentes pour la protection des données (notamment, le Groupe de travail « article 29 », le Contrôleur européen pour la protection des données, la Commission pour la protection de la vie privée), que d'associations de défense des droits de l'homme. La requérante considère que la loi attaquée viole les principes défendus par ses statuts.

La requérante a donc intérêt à en solliciter l'annulation.

La loi attaquée a été publiée au Moniteur belge du 29 décembre 2009. Le soixantième jour du délai tombait le samedi 27 février 2010. En vertu de l'article 119 de la loi spéciale du 6 janvier 1989, le dernier jour utile permettant l'introduction de la requête était le lundi suivant, c'est-à-dire le 1^{er} mars 2010, date à laquelle la présente requête est effectivement envoyée. Celle-ci est donc recevable *ratione temporis*.

LES MOYENS

Premier moyen : l'article 2 de la loi attaquée viole l'article 22 de la Constitution, combiné avec les articles 8 et 13 de la Convention européenne des droits de l'homme en ce que les mesures qu'elle consacre ne sont pas prévues par la loi, ne poursuivent pas un objectif légitime, ne sont pas nécessaires dans une société démocratique et ne peuvent faire l'objet d'un recours effectif

I. Considérations préliminaires

I. 1. Enoncé des principes consacrés par la loi attaquée

L'accord ratifié par la loi attaquée, lu en combinaison avec la lettre du DHS, permet notamment les mesures suivantes, qui seront plus amplement décrites dans l'exposé des moyens:

- la collecte et la transmission systématique des données passagers (PNR) de toutes les personnes qui voyagent par avion de ou vers les Etats-Unis au DHS ;
- le traitement automatisé des données PNR par le DHS à des fins de lutte contre le terrorisme et la criminalité organisée mais aussi simplement « dans le cadre d'une procédure pénale ou de toute autre manière requise par la loi »⁹ et « pour préserver la sécurité publique et à des fins de maintien de l'ordre »¹⁰ ;
- la conservation des données PNR sans aucune garantie de destruction après une durée déterminée ;

⁹ Art. I de la lettre du DHS.

¹⁰ Préambule de l'accord.

- La retransmission des données PNR par le DHS à d'autres autorités des Etats-Unis, à des Etats tiers à des fins qui ne sont pas clairement définies

I. 2. Disposition constitutionnelle violée et combinaison avec les traités internationaux ayant une portée analogue

L'article 22 de la Constitution dispose:

"Chacun a droit au respect de sa vie privée et familiale, sauf dans les conditions fixées par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit".

Le second alinéa de cette disposition énonce que *"la loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit"*; les différents législateurs ont une obligation positive de rendre "effectif et concret" le droit à la vie privée¹¹.

Votre Cour considère que «lorsqu'une disposition d'un traité international liant la Belgique a une portée analogue à celle d'une des dispositions constitutionnelles dont le contrôle relève de la compétence de la Cour et dont la violation est alléguée, les garanties consacrées par cette disposition internationale constituent un ensemble indissociable avec les garanties inscrites dans les dispositions constitutionnelles concernées»¹².

L'article 22 précité doit donc être lu avec l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après Convention européenne des droits de l'homme « CEDH ») qui garantit le droit au respect de la vie privée et dont il est la « traduction » dans l'ordre constitutionnel belge¹³.

Selon l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales :

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

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

¹¹ Doc. Parl., Sénat, sess. ord. 1993-1994, n° 100-4/5°, p. 6.

¹² voir notamment les arrêts n° 12/2008; n° 61/2008 et n° 110/2008.

¹³ Arrêt n° 16/2005 et David DE ROY, Cécile DE TERWANGNE, Yves POULLET, « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », CDPK 2007, p. 331.

Les requérantes précisent, en ce qui concerne la disposition constitutionnelle, que l'objectif du Constituant a été de préserver la vie privée et familiale "*des risques d'ingérence que peuvent constituer, notamment par le biais de la modernisation constante des techniques de l'information, les mesures d'investigation, d'enquête et de contrôle menés par les pouvoirs publics et organismes privés, dans l'accomplissement de leurs fonctions ou de leurs activités*" (Doc. parl., Sénat, 1991-1992, n° 100-4/2°, p. 3).

Aux termes de l'article 8 § 2 CEDH, une ingérence de l'autorité publique dans le droit au respect de la vie privée ne peut être admise que si (i) elle est prévue par la loi, (ii) elle poursuit l'un des buts légitimes énumérés, et (iii) elle demeure proportionnée par rapport à celui-ci. Ces trois conditions sont cumulatives et doivent toutes être remplies pour qu'une restriction soit admise au sens de l'article 22 de la Constitution¹⁴.

Si le droit au respect de la vie privée n'est pas absolu, le législateur ne peut consacrer de restrictions que dans la mesure où celles-ci sont prévues par la loi. En effet, "*il est évident que tant le législateur fédéral que les législateurs fédérés doivent respecter l'article 8 de la Convention européenne des droits de l'homme. En particulier, le législateur fédéral ne peut autoriser des restrictions qui vont au-delà des prévisions du paragraphe 2 de cet article*"¹⁵.

La protection des données personnelles est une valeur dont l'importance croît avec l'impact grandissant des nouvelles technologies¹⁶ et fait partie intégrante du respect de la vie privée visé à l'article 22 de la Constitution.

Par conséquent, il convient de lire cette disposition constitutionnelle également en combinaison avec les dispositions pertinentes de la Convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel¹⁷ (ci-après, « Convention 108 »), qui doit être considérée également comme formant « un ensemble indissociable avec les garanties inscrites » dans l'article 22 précité¹⁸. La requérante rappelle en outre que la Cour Européenne des Droits de l'Homme s'est référée à de multiples reprises à cette Convention à l'occasion d'affaires touchant à l'article 8 de la CEDH.¹⁹

Il convient notamment de tenir compte des définitions de l'article 2 de cette Convention, qui se lit comme suit :

« *Aux fins de la présente Convention :*

¹⁴ Arrêt n° 202/2004.

¹⁵ R. ERGEC, *Introduction au droit public. Les droits et libertés*, t. II, 2^e édition, Bruxelles, Kluwer, 2003, p. 140.

¹⁶ Cette importance se marque par exemple par la consécration du principe dans la Charte européenne des droits fondamentaux dont l'article 8 stipule :

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

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

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

¹⁷ Convention signée à Strasbourg et approuvée par la loi du 17 juin 1991.

¹⁸ Voir notamment les arrêts n° 12/2008; n° 61/2008 et n° 110/2008.

¹⁹ Voir notamment CEDH, Z. contre Finlande, 25 février 1997, § 95 ; CEDH, Amann contre Suisse, 16 février 2000, affaire 27798/95, § 65 ; CEDH, Rotaru contre Roumanie, 4 mai 2000, R.T.D.H., 2001 § 57 et 60.

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

b) " fichier automatisé " signifie : toute ensemble d'informations faisant l'objet d'un traitement automatisé;

c) traitement automatisé " s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion;

d) " maître du fichier " signifie : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées. »

L'article 5 stipule que les « données à caractère personnel faisant l'objet d'un traitement automatisé sont :

a) obtenues et traitées loyalement et licitement;

b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;

c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;

d) exactes et si nécessaire mises à jour;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées ».

L'article 6 soumet le traitement des données « à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle » à des « garanties appropriées » prévues par le droit interne.

L'article 8 de cette même Convention octroi les droits suivants aux personnes concernées :

« a) connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier;

b) obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible;

c) obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention;

d) disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b) et c) du présent article. »

L'article 9 §2 permet des dérogations à ces droits notamment « lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société

démocratique:

a) à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;

b) à la protection de la personne concernée et des droits et libertés d'autrui. »

Enfin, l'article 10 impose aux Etats parties d'établir « des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans le présent chapitre ».

Avant d'examiner les différentes branches du moyen proprement dit, la requérante souhaite brièvement montrer que les mesures prévues par la loi attaquée entrent bien dans le champ d'application de la protection de la vie privée défini par les dispositions visées aux moyens.

I.3. Applicabilité des dispositions protectrices de la vie privée aux PNR

La requérante rappelle que la Cour européenne des droits de l'homme (ci-après « Cour EDH ») interprète de manière large la notion de « vie privée », dont le respect englobe « le droit pour l'individu de nouer et développer des relations avec ses semblables », considère que « de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de « vie privée ».²⁰ Dans l'arrêt Amann²¹, la Cour EDH a considéré que :

« Cette interprétation extensive concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, entrée en vigueur le 1^{er} octobre 1985, dont le but est « de garantir, sur le territoire de chaque Partie, à toute personne physique (...) le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1), ces dernières étant définies comme « toute information concernant une personne physique identifiée ou identifiable » (article 2) ».

Il faut donc considérer que « toute information concernant une personne physique identifiée ou identifiable » faisant l'objet d'un traitement automatisé entre dans le champ d'application de l'article 8 de la CEDH.

Il découle tant de la description des données PNR faite par l'accord et la lettre du DHS (article III), que des explications fournies dans l'exposé des motifs, que les mesures prévues par la loi attaquée permettent bien d'identifier une personne physique et qu'elles font l'objet d'un traitement automatisé systématique. La circonstance que les données PNR seraient, le plus souvent, des informations que tout passager doit fournir lorsqu'il commande ou achète un billet d'avion ne les fait donc pas échapper à la protection garantie par les dispositions visées au moyen. En effet, la Cour EDH considère que « des données de nature publique peuvent

²⁰ arrêts Niemietz c. Allemagne du 16 décembre 1992, série A n° 251-B, pp. 33-34, § 29, et Halford c. Royaume-Uni du 25 juin 1997, *Recueil des arrêts et décisions* 1997-III, p. pp. 1015-1016, § 42

²¹ Cour EDH, *Amann c. Suisse* [GC], du 16 février 2000, § 65.

relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics »²². Il faut souligner que les données PNR peuvent contenir également des données sensibles pouvant révéler notamment les convictions religieuses (à travers les demandes de régime alimentaire spécifique) ou les affinités personnelles et les relations personnelles ou professionnelles (à travers la localisation du siège occupé dans l'avion). Selon la Commission européenne, les éléments d'information issus des données PNR « sont très importants pour procéder à des évaluations de risques des personnes, pour obtenir des informations et pour établir des liens entre des personnes connues et des personnes inconnues »²³.

Il n'est donc pas contestable que les mesures prises par la loi attaquée se situent dans le champ de la vie privée des individus.

I.4. Existence d'une ingérence dans le droit à la vie privée

Selon la Cour EDH, « tant la mémorisation par une autorité publique de données relatives à la vie privée d'un individu que leur utilisation et le refus d'accorder la faculté de les réfuter constituent une ingérence dans le droit au respect de sa vie privée garanti par l'article 8 § 1 de la Convention »²⁴.

La réalité de l'atteinte au droit à la vie privée visé au moyen n'est pas contestable.

Selon l'exposé des motifs de la loi attaquée, « L'Accord institue donc une obligation légale de transférer directement aux autorités américaines des données PNR (collectées dans l'UE pour des motifs commerciaux) dans le cadre de la lutte contre le terrorisme.²⁵ ». Selon le gouvernement, « la législation belge en la matière autorise pareils transferts, mais ne comporte pas de garanties en matière de protection des données. »²⁶

Or, selon l'article 8, § 2, de la Convention européenne, le législateur ne peut prévoir une ingérence d'une autorité publique dans l'exercice des droits au respect de la vie privée "*que pour autant que cette ingérence (...) constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui*".

²² Cour EDH, Rotaru c. Roumanie, du 4 mai 2000, § 43. La Cour EDH a confirmé sa jurisprudence dans l'affaire Segerstedt-Wiberg et autres c. Suède du 6 juin 2006, § 72.

²³ Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives, présentée par la Commission, COM(2007) 654 final, du 6 novembre 2007, p 3.

²⁴ Arrêts Leander précité, p. 22, § 48, Kopp c. Suisse du 25 mars 1998, *Recueil* 1998-II, p. 540, § 53, et *Amann* précité, §§ 69 et 80, Rotaru précité, § 46.

²⁵ Exposé des motifs, Doc. Parl. Sénat, session 2008-2009, n° 4-1432/1, pp. 7-8.

²⁶ Exposé des motifs, Doc. Parl. Sénat, session 2008-2009, n° 4-1432/1, p 8 sans aucune précision quant à ladite législation.

II. Première branche du moyen : l'ingérence n'est pas « prévue par la loi »

Selon une jurisprudence constante de la Cour européenne des droits de l'homme²⁷, le principe de légalité visé à l'article 8 § 2 de la Convention consacre trois exigences. Premièrement, la limitation aux droits et libertés doit avoir une base légale dans le droit de l'Etat concerné. Deuxièmement, cette base légale doit être accessible. Troisièmement, cette base légale doit être prévisible.

Pour la Cour EDH, les mots « prévue par la loi » imposent non seulement que la mesure incriminée ait une base en droit interne, mais visent aussi la qualité de la loi en cause : ainsi, celle-ci doit être accessible au justiciable et prévisible²⁸. Une norme est « prévisible » lorsqu'elle est rédigée avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite. Ceci implique que la loi doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique au droit à la vie privée. Elle souligne que le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret. Il convient par conséquent de définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire. »²⁹

L'expression "prévue par la loi" figurant à l'article 8 de la Convention "veut d'abord que l'ingérence ait une base en droit interne, mais l'observation de celui-ci ne suffit pas: la loi en cause doit être accessible à l'intéressé, qui en outre doit pouvoir en prévoir les conséquences pour lui".³⁰ La possibilité pour l'intéressé de prévoir les conséquences de l'application de la loi concerne la prévisibilité de la mesure interne autorisant l'immixtion de l'autorité dans la sphère privée individuelle. En effet, selon la Cour européenne des droits de l'homme, "l'expression" prévues par la loi "figurant aux articles 8 à 11 de la Convention non seulement exige que la mesure incriminée ait une base en droit interne, mais vise aussi la qualité de la loi en cause : ainsi, celle-ci doit être suffisamment accessible et prévisible, c'est-à-dire énoncée avec assez de précision pour permettre à l'individu – en s'entourant au besoin de conseils éclairés – de régler sa conduite".³¹ Autrement dit, "la loi doit user de termes assez clairs pour leur {les citoyens} indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée".³²

Cette jurisprudence est constante dans le chef de la Cour.³³

Afin de vérifier si la condition de prévisibilité est remplie par la législation interne, "la Cour se montre particulièrement exigeante quant "aux garanties contre les abus "attendues de la législation interne. Celle-ci doit fournir suffisamment d'indications quant à l'étendue et les

²⁷ Notamment, arrêts *Amann c. Suisse* et *Rotaru c. Roumanie* respectivement du 16 février 2000 et du 4 mai 2000.

²⁸ Voir notamment l'arrêt *Amann* précité, § 50.

²⁹ Cour EDH, *Malone c. Royaume-Uni* du 2 août 1984, § 67, repris dans l'arrêt *Amann* précité, § 56 et *Rotaru* précité, § 55).

³⁰ C.E.D.H., arrêt *Leander c. Suède* du 26 mars 1987, § 50.

³¹ C.E.D.H., arrêt *Hassan et Tchaouch c. Bulgarie* du 26 octobre 2000, § 84.

³² *Leander c. Suède*, précité, § 51.

³³ *Silver et autres c. Royaume Uni*, arrêt du 25 mars 1983, § 88 ; *Hertel c. Suisse*, arrêt du 25 août 1998, § 35 ; *Rotaru c. Roumanie*, arrêt du 4 mai 2000, § 55 ; *N.F. c. Italie*, précité, § 29.

modalités des pouvoirs conférés aux autorités (arrêt Amman, § 76), et doit à cet égard préciser "les informations qui peuvent être mémorisées et les mentions éventuellement interdites" (Amman, § 76), "les catégories de personnes susceptibles de faire l'objet de la surveillance" (arrêt Rotaru c. Roumanie du 4 mai 2000, §57), "les circonstances dans lesquelles peuvent être adoptées ces mesures" (Rotaru, § 57), la finalité de celles-ci (Rotaru, § 58), la procédure à suivre (Amman, § 76), et l'identité des personnes autorisées à consulter les dossiers constitués (Rotaru, § 58). Des précisions doivent encore être fournies par la loi concernant l'ancienneté des informations susceptibles d'être mémorisées et la durée de leur conservation (Rotaru, § 57)."³⁴

Si, concernant l'exigence de légalité, la Cour européenne des droits de l'homme adopte une interprétation large du terme "loi" visé à l'article 8 § 2 de la Convention, dans la mesure où se trouve visée toute norme de droit écrit ou non écrit en vigueur dans l'ordre juridique concerné, le titre II de la Constitution exprime quant à lui un principe de réserve à la loi au sens formel, œuvre d'un législateur. En vertu de l'article 53 de la Convention européenne des droits de l'homme, le régime de droit national plus favorable à la protection des droits de l'homme doit prévaloir.

Votre Cour a déjà pu confirmer ceci : « l'exigence d'une loi au sens formel s'impose en Belgique pour autoriser une ingérence dans ces droits, en vertu de l'article 53 de la Convention. Cet article prévoit que lorsqu'un droit ou une liberté est davantage protégé par les dispositions nationales que par la Convention, c'est à ces dispositions nationales qu'il convient d'avoir égard »³⁵ et en a déduit que : « Bien que l'article 8.2. de la Convention européenne précitée n'exige pas que l'ingérence qu'il permet soit prévue par une « loi » au sens formel du terme, le même mot utilisé à l'article 22 de la Constitution désigne une disposition législative »³⁶.

II.1. A TITRE PRINCIPAL : Les ingérences au droit à la vie privée ne sont pas « prévues par la loi » parce que la lettre du DHS n'est pas contraignante et ne peut donc être qualifiée de « loi » au sens des dispositions visées au moyen

Le texte de l'accord ne contient aucune règle normative permettant au citoyen d'être informé sur la portée et les conditions de l'ingérence faite à sa vie privée.

En effet, le texte de l'accord lui-même ne contient aucune information concernant notamment les points essentiels suivants :

- la définition des données PNR (définies à l'article III de la lettre du DHS) ;
- les objectifs et les modalités du traitement des données ;
- la durée de conservation des données ;

³⁴ S. Van Drooghenbroeck, *La Convention européenne des droits de l'homme. Trois années d'ejurisprudence des droits de l'homme*, Dossier du J.T., p. 145.

³⁵ arrêt n° 202/2004

³⁶ arrêt n° 131/2005 du 19 juillet 2005

L'article 3 de l'accord se limite à affirmer que « le DHS traite les données PNR reçues et les personnes concernées par ce traitement conformément aux lois et exigences constitutionnelles américaines applicables » qui ne sont pas autrement définies.

L'article 22 de la Constitution exige que l'ingérence au droit à la vie privée soit prévue par une loi au sens formel, ce qui signifie par définition que cette loi doit revêtir une force contraignante.

L'accord ne se réfère en effet à cette déclaration d'engagement que dans les termes suivants : « 1. *Se fondant sur les assurances données dans la lettre d'explication du DHS sur la protection des données PNR l'Union européenne veillera à ce que les transporteurs aériens assurant un service de transport international de passagers à destination des Etats-Unis rendent disponibles les données PNR stockées dans leurs systèmes de réservation comme l'exige le DHS* ». et « 3. *Le DHS traite les données PNR reçues et les personnes concernées par ce traitement conformément aux lois et exigences constitutionnelles américaines applicables, sans discrimination illégitime, en particulier sur la base de la nationalité et du pays de résidence. La lettre du DHS expose ces garanties ainsi que d'autres.* »

Selon le gouvernement « du fait qu'une référence explicite auxdites Assurances figure dans l'Accord, la lettre du DHS et les garanties qui y sont décrites en font partie intégrante, et se voient dotées d'un caractère contraignant (et non unilatéral). »³⁷

Ceci relève de l'affirmation péremptoire. D'autres observateurs qualifiés qui ont examiné l'accord ont émis des doutes sérieux sur la portée obligatoire de la lettre du DHS. Ainsi, selon le Contrôleur européen pour la protection des données, « *Le caractère obligatoire des engagements du CBP (lire : DHS, note de la requérante) n'est pas clair, certains éléments décisifs de l'accord étant inclus dans une lettre séparée. Cela pourrait constituer un risque d'interprétation unilatérale par les USA de leurs obligations* »³⁸. Pour sa part, le groupe 29 considère que « *l'accord crée le risque que toute modification de la législation américaine puisse affecter unilatéralement le niveau de protection des données prévu dans le nouvel accord PNR.* »³⁹

L'analyse des textes de l'accord et de la lettre du DHS démontre que celle-ci est dépourvue de tout effet obligatoire et ne contient que des engagements pouvant être librement modifiés ou rétractés par les autorités américaines.

³⁷ Exposé des motifs, Doc. Parl. Sénat, session 2008-2009, n° 4-1432/1, p 8.

³⁸ Texte original : « The binding character of CBP's commitments is not clear, as some decisive elements of the agreement are included in a side letter. This could raise a risk of unilateral interpretation by the US of their obligations ». Voir: "Comments of the EDPS on different international agreements, notably the EU-US and EU-AUS PNR agreements, the EU-US TFTP agreement, and the need of a comprehensive approach to international data exchange agreements", 25 janvier 2010, p 2, disponible sur: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-01-25_EU_US_data_exchange_EN.pdf

³⁹ Avis du Groupe de travail Article 29 n° 5/2007 « concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure », adopté le 17 août 2007 (disponible sur

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_fr.pdf).

En vertu de l'accord, les autorités des Etats-Unis se limitent à une promesse de respecter la constitution et les lois américaines. Aucun engagement formel n'est pris par la partie états-unienne de respecter aussi les mesures mentionnées dans la dite lettre d'explications. Il est impossible, pour le citoyen belge, de savoir, sans effectuer de longues et coûteuses recherches, si les « garanties » contenues dans la lettre du DHS se retrouvent également dans des instruments juridiques contraignants en vigueur au Etats-Unis.

Il est intéressant à cet égard de comparer le présent accord avec l'accord similaire conclu en 2004. L'accord PNR de 2004 avait donné lieu à deux décisions différentes. La première était la décision 2004/496/CE du Conseil concernant la conclusion de l'accord. La seconde était la décision 2004/535/CE de la Commission relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des Etats-Unis d'Amérique.⁴⁰

A cette dernière décision était annexée une déclaration d'engagement du bureau des douanes et de la protection des frontières du Ministère de la sécurité intérieure. Il s'agissait d'une lettre aux objectifs similaires à celle du DHS annexée à l'accord de 2007.

Contrairement à l'accord conclu en 2007, celui de 2004 subordonnait, dans ces paragraphes 1 et 2, l'obligation de traitement des données à l'application stricte de la décision d'adéquation laquelle se réfère à son tour explicitement à la dite déclaration d'engagement dans son 11^{ème} considérant. Aux termes du paragraphe 3 de l'accord de 2004 les autorités américaines s'engagent « à mettre en œuvre les engagements annexés à ladite décision ». L'accord de 2007 ne contient aucun engagement similaire de la part des autorités américaines de telle sorte qu'en ce qui concerne celui-ci il faut conclure que la lettre du DHS qui y est annexée ne peut être considérée comme créant des obligations dans le chef des autorités américaines.

Ceci est également démontré par la différence significative entre les régimes de sanctions du non respect éventuel des obligations, découlant des lettres envoyées des autorités compétentes américaines respectivement en 2004 et en 2007. Alors que la décision d'adéquation de 2004 prévoyait dans ses articles 3, 4 et 5 un régime permettant aux états membres de l'Union européenne de suspendre le transfert des données PNR vers les autorités américaines en cas de non-respect des engagements pris par ceux-ci et qu'en outre l'accord de 2004 se réfère (dans son article 5) à la décision d'adéquation, l'accord de 2007 ne prévoit rien de tel.

L'article 8 de l'accord se lit comme suit : « Au cas où l'UE constaterait que les Etats-Unis ont violé le présent accord, la seule voie de droit est la dénonciation de celui-ci et la rétractation de la présomption relative au niveau adéquat de protection visée au point 6 »⁴¹.

En droit international, la dénonciation d'un accord est une conséquence toujours possible de la violation de ses dispositions⁴². Le fait de ne pas faire référence, dans cette disposition à la

⁴⁰ Les deux décisions avaient été annulées par un arrêt de la Cour de Justice du 30 mai 2006 ce qui a d'ailleurs été à l'origine de la conclusion du nouvel accord sur lequel porte la loi d'assentiment.

⁴¹ Souligné par la requérante.

⁴² L'article 40 §1^{er} de la Convention de Vienne du 23 mai 1969 sur le droit des traités dispose : « 1. Une violation substantielle d'un traité bilatéral par l'une des parties autorise l'autre partie à invoquer la violation comme motif pour mettre fin au traité ou suspendre son application en totalité ou en partie. » (23 mai 1969)

lettre du DHS et de ne prévoir aucune autre sanction confirme le caractère non contraignant de celle-ci, à la différence de ce qui était prévu par l'accord de 2004.

Compte tenu de ce que le texte de l'accord lui-même n'est pas suffisamment clair ni accessible ni prévisible au sens de l'article 8 de la CEDH, et du fait que les seules « garanties » entourant le traitement des données PNR sont contenues dans la lettre du DHS qui n'a pas de force contraignante, il faut en conclure que les ingérences au droit à la vie privée, instaurée par la loi attaquée, ne sont pas « prévues par la loi », ce qui devrait suffire à Votre Cour pour l'annuler.

II. 2. A TITRE SUBSIDIAIRE : Si, par impossible, la Cour devait considérer que la lettre du DHS était revêtue d'une force contraignante (quod non), il faudrait en tout état de cause considérer que les « assurances » contenues dans la lettre du DHS ne sont pas « prévues par la loi » au sens des dispositions visées au moyen

Si la Cour devait, par impossible, suivre la thèse du gouvernement et considérer que la lettre du DHS faisait partie intégrante de l'accord et était par conséquent dotée d'une force contraignante, ceci ne permettrait pas, selon la requérante, d'en conclure que les ingérences visées par la loi attaquée seraient pour autant « prévues par la loi ».

La requérante entend analyser le contenu des prétendues « garanties » mentionnées dans la lettre du DHS pour démontrer que celles-ci ne peuvent remplir les critères d'accessibilité, de prévisibilité et de clarté prévus par la jurisprudence de la Cour EDH mentionnée plus haut.

II.2.1) La définition des PNR n'est pas suffisamment claire

Selon la lettre du DHS , les types de données PNR de l'UE collectées sont les suivantes:

- « 1. Code repère du dossier PNR (record locator code)
2. Date de réservation/d'émission du billet
3. Date(s) prévue(s) du voyage
4. Nom(s)
5. Informations disponibles sur « les grands voyageurs » et les programmes de fidélisation (c'est-à-dire billets gratuits, surclassement, etc...)
6. Autres noms figurant dans le PNR, y compris nombre de voyageurs dans le PNR
7. Toutes les informations de contact disponibles (y compris les informations sur la source)
8. Toutes les informations disponibles relatives au paiement/à la facturation disponibles (les autres détails de l'opération liés à la carte de crédit ou au compte et n'ayant pas de lien avec l'opération relative au voyage non inclus)
9. Itinéraire de voyage pour le PNR spécifique
10. Agence de voyage/agent de voyage
11. Informations sur le partage de codes
12. Informations « PNR scindé/divisé »
13. Statut du voyageur (y compris confirmations et statut d'enregistrement)
14. Informations sur l'établissement des billets, y compris le numéro du billet, billets aller

simple et données Automated Ticketing Fare Quote (prix du billet)

15. Toutes les informations relatives aux bagages

16. Informations relatives au siège, y compris numéro du siège occupé

17. Remarques générales, y compris données OSI, SSI et SSR

18. Toutes les informations APIS recueillies

19. Historique de tous les changements apportés au PNR assortis des numéros de rubriques 1 à 18 »

Il faut noter que certaines définitions, par leur formulation vague, ne permettent pas précisément de connaître l'ampleur des informations qui sont visées.

Ainsi, au point 7, rien ne définit ce qu'il faut entendre précisément par « Toutes les informations de contact disponibles (y compris les informations sur la source) ». Le citoyen doit-il en déduire que les autorités américaines seront en possession de son adresse, numéro de téléphone, adresse e-mail si celles-ci ont été communiquées par le transporteur ? Ce n'est pas clair à la lecture du texte. Ce flou est bien entendu contraire à l'exigence de prévisibilité inhérente à l'article 8 de la CEDH.

D'autres mentions restent très vagues et indéfinissables pour le passager non initié, telles que:

« 11. Informations sur le partage de codes

12. Informations « PNR scindé/divisé » »

On peut aussi se demander si « Toutes les informations relatives aux bagages » ne recouvrent que les caractéristiques externes (poids, quantité, nombre de paquets...), ou si elles pourraient éventuellement viser le contenu des bagages, tel qu'il a par exemple été visualisé à travers les mécanismes de contrôles visuels de sécurité de l'aéroport. Ici encore, le texte ne permet pas au citoyen de se faire une idée précise de l'étendue de l'ingérence faite à sa vie privée.

Compte tenu du caractère vague de certaines définitions, la loi attaquée ne répond pas aux conditions pour permettre de qualifier les ingérences de « prévues par la loi » au sens de l'article 8 de la CEDH.

II.2.2) La finalité de l'usage des données PNR par les autorités n'est pas définie clairement

La requérante considère que la définition de la finalité pour laquelle les données PNR sont traitées ne répond pas aux conditions de clarté et de prévisibilité requises par les dispositions visées au moyen. Ceci pour les trois raisons suivantes.

II.2.2) a) Contradiction des formulations entre l'accord et la lettre du DHS

Premièrement, la requérante note que les articles de l'accord ne contiennent aucun élément concernant la finalité du traitement des données PNR. Seul le préambule se réfère à l'objectif

de « combattre efficacement le terrorisme et la criminalité transnationale », mais à celui de préserver la sécurité publique et au maintien de l'ordre, ce qui couvre un champ quasiment illimité relevant tant des activités répressives que de la police administrative. Dans un autre considérant de l'accord, on peut lire « qu'il importe de prévenir et de combattre le terrorisme et les délits qui y sont liés, ainsi que d'autres délits graves de nature transnationale, y compris la criminalité organisée », ce qui est une formule encore différente.

Selon la lettre du DHS (article I.), le DHS utilise les données PNR de l'UE seulement pour prévenir et combattre le terrorisme « et les délits qui y sont liés » (1), prévenir et combattre « d'autres délits graves de nature transnationale, y compris la criminalité organisée » (2); et pour « empêcher que des personnes se soustraient aux mandats et aux mesures de détention provisoire émis à leur encontre concernant les infractions décrites ci-dessus » (3). Cette énumération est faussement limitative puisqu'elle est suivie de la phrase suivante : « Les données PNR peuvent être utilisées, le cas échéant, pour la protection des intérêts vitaux de la personne concernée ou d'autres personnes, ou dans le cadre d'une procédure pénale ou de toute autre manière requise par la loi ».

La requérante relève que les formulations contenues dans l'accord et celles de la lettre du DHS ne sont pas identiques et ne se recouvrent que partiellement. Il convient de relever par exemple l'immensité du champ d'application que recouvre les expressions permettant l'utilisation des données PNR dans le cadre « d'une procédure pénale », même visant un délit mineur, et aussi « de toute autre manière requise par la loi » comme décrit par la lettre du DHS. Cette formule va loin au-delà de ce qui était prévu par le préambule de l'accord. Il existe donc une contradiction qui rend totalement illusoire l'exigence de prévisibilité déduite de l'article 8 de la CEDH tel que décrit plus haut.

II.2.2) b) Pas de définition claire ni commune de certaines notions

En outre, il faut noter que le texte ne donne aucune définition des infractions visées. Par exemple, le terme « terrorisme » n'est pas défini alors qu'il ne fait l'objet d'aucune définition consensuelle au niveau international. Il en va de même pour la nature précise des délits qui y seraient liés et des « délits graves de nature transnationale, y compris la criminalité organisée ». Il est possible que ces notions recouvrent des réalités différentes aux Etats-Unis et dans l'UE. La possibilité de traiter les données PNR « de toute autre manière requise par la loi » peut s'appliquer de manière indéterminable.

Le groupe de travail « article 29 » s'est inquiété du caractère très vague de cette définition de la finalité et il attendait « de la Commission qu'elle apporte des éclaircissements par écrit, spécifiant les cas dans lesquels les données peuvent servir à des fins autres que celles mentionnées aux points 1, 2 et 3 ci-dessus »⁴³.

II.2.2) c) Caractère évolutif des finalités et absence d'obligation d'information du citoyen

⁴³ Avis 5/2007 concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure, conclu en juillet 2007, 17 août 2007, p 8, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_fr.pdf.

Il découle de la lettre du DHS que l'expression « de toute autre manière requise par la loi » pourra viser non seulement les lois existantes lors de la conclusion de l'accord mais aussi les lois qui seront adoptées dans le futur. Compte tenu de ce champ excessivement large, il est dès lors impossible pour le citoyen de connaître précisément la finalité du traitement qui justifie la collecte de ses données PNR. La circonstance que « le DHS informera l'UE de l'adoption de toute législation américaine qui affecte matériellement les déclarations faites dans la présente lettre » ne remet pas ce constat en cause. D'une part, parce que, cette formule n'est pas contenue dans un instrument contraignant. D'autre part, parce qu'elle contient une promesse d'information entre les Etats-Unis et l'UE mais pas d'obligation d'information vis-à-vis du citoyen. Rien dans l'accord n'oblige les Etats-Unis ni l'UE à fournir au citoyen une liste actualisée de toutes les lois qui permettent le traitement des données PNR.

II.2.3) Les modalités du traitement des données PNR par les autorités ne sont pas définies clairement

A la lecture de l'accord et de la lettre du DHS, il n'est pas non plus possible, pour le citoyen de connaître, avec un minimum de précisions, les modalités du traitement qui seront réservées à ses données, ni par quelles autorités elles seront traitées.

Par exemple, le voyageur potentiel ne peut savoir avec quels autres éléments ses données PNR seront confrontées ou comparées, ni si elles seront utilisées dans des programmes complexes afin d'établir des profils de suspects, ni sur base de quels critères ces éventuels profils seraient établis.

II.2.3) a) Durée du traitement et de la conservation des données PNR

Selon la lettre du DHS (point VII), les données PNR de l'UE seront conservées « dans une base de données analytique active pendant sept ans ».

Ensuite les données acquerront « un statut inactif » mais pourront faire l'objet d'une consultation ou d'un traitement avec « l'accord d'un haut fonctionnaire du DHS désigné par le secrétaire à la sécurité intérieure et uniquement en réponse à une situation, une menace ou un risque déterminés », et ce pour une durée de 8 ans. La lettre prévoit que les données « devraient être détruites à la fin de cette période »⁴⁴ mais leur destruction effective reste hautement hypothétique car « la question de savoir si et quand il convient de détruire les données PNR collectées conformément à la présente lettre sera examinée par le DHS et l'Union européenne dans le cadre de discussions futures ». En réalité, cette clause enlève toute garantie de respect du délai de conservation de 15 ans qui est formellement prévu.

Il est également précisé que « Les données qui sont liées à un cas ou une enquête spécifiques peuvent être conservées dans une base de données active jusqu'à ce que le cas ou l'enquête soient archivés ». Cette prolongation n'est pas conditionnée par l'existence d'une enquête judiciaire puisque ce n'est pas précisé par le texte. En outre, la notion de « données qui sont

⁴⁴ La requérante relève que le texte original anglais de la lettre du DHS semble encore moins contraignant : « We expect that EU PNR data shall be deleted at the end of this period ».

liées à un cas » n'est pas défini. En réalité, ceci revient à autoriser la conservation dans une base de données active à la discrétion de l'administration, qui peut omettre de clôturer une enquête administrative, ou « un cas », de manière discrétionnaire.

Il découle de cette disposition que le citoyen ne dispose d'aucun moyen de connaître avec un minimum de précision le délai de conservation de ses données personnelles. Il a encore moins la garantie de voir ses données détruites dans un délai déterminé.

II.2.3) b) La transmission des données PNR à d'autres administrations ou à des Etats tiers

L'article II de la lettre du DHS permet le partage de données PNR par le DHS avec d' « autres autorités gouvernementales américaines chargées du maintien de l'ordre, de la sécurité publique ou de la lutte contre le terrorisme », qui ne sont pas définies dans les textes. La seule condition mise à ce partage est que le DHS « le juge utile » et qu'il s'effectue « conformément aux lois américaines », qui ne sont pas non plus mentionnées.

En outre, cette disposition prévoit une possibilité de partage des données « avec d'autres autorités gouvernementales de pays tiers qu'après examen de l'utilisation ou des utilisations prévues par le destinataire et de sa capacité à assurer la protection des informations ». Il n'est pas précisé qui effectue cet « examen » mais il ressort de l'économie du texte qu'il s'agit du DHS et non d'une autorité de contrôle indépendante (puisque l'article débute par « le DHS partage les données uniquement aux fins énoncées au point I »). Le contenu exact de cet « examen » de conformité n'est pas non plus précisé. Les échanges de données doivent se faire « en vertu d'engagements exprès entre les parties qui comprennent des dispositions de protection des données à caractère personnel comparables à celles qu'applique le DHS aux données PNR de l'UE ». Compte tenu des critiques émises dans le présent recours, la requérante estime que ces dispositions de protection sont insuffisantes.

En outre, il est encore plus préoccupant de constater qu'en « cas d'urgence », non autrement défini, le DHS peut partager des données, y compris sensibles, sans aucune garantie à cet égard. Dans son avis, le Conseil d'Etat a fait les observations suivantes :

« Il en résulte que, dans les cas d'urgence, le « partage de données PNR » à l'initiative du DHS vers des autorités gouvernementales de pays tiers, nécessite seulement un examen des utilisations prévues et de la capacité d'assurer la protection des informations, et non la constatation du caractère admissible de ladite utilisation, selon des critères prédéterminés.

Or, en vertu de l'article 22 de la loi du 8 décembre 1992, précitée, un transfert de données dans ces circonstances n'est possible que dans des cas limitativement énumérés, entre autres « pour la sauvegarde d'un intérêt public important ».

Le transfert des données PNR collectées et enregistrées en Belgique par le DHS ne peut au regard du droit interne se concevoir qu'à la condition qu'un intérêt public important doive être sauvegardé (1 : Voir dans le même sens, le protocole additionnel

no 181 du 8 novembre 2001, à la Convention no 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, contient une prescription analogue en son article 2, § 2, a, 2e tiret. Il a été signé par la Belgique le 30 avril 2002).

Dans l'état actuel du dossier soumis à la section de législation, il y a lieu de constater que ni l'accord ni la lettre du DHS n'apportent une telle garantie; la section de législation ne dispose par ailleurs pas d'autres informations qui permettraient de considérer qu'une telle garantie est rencontrée par la législation américaine applicable en la matière »⁴⁵.

Compte tenu de ces observations, il est impossible pour le citoyen de savoir, avec un degré raisonnable de prévisibilité, si ses données vont être transmises à des autorités publiques états-uniennes ou d'états tiers, ni dans quels buts, ni pendant combien de temps elles seront utilisées. La portée de l'ingérence dont la vie privée du voyageur peut être l'objet est donc totalement imprévisible et inaccessible sur ce point.

Compte tenu de ces lacunes portant sur des éléments essentiels du traitement de données (finalité, durée, éventuelle transmission à d'autres administrations ou à des états tiers), il faut conclure que les ingérences visées ne répondent pas aux exigences de clarté, d'accessibilité et de prévisibilité contenues dans les dispositions visées au moyen.

III. Deuxième branche du moyen : Les ingérences ne poursuivent pas un but légitime, compte tenu de la collecte généralisée des données PNR et de leur usage excessivement large et imprécis

III.1 Un but excessivement large et mal défini ne peut pas être légitime

La requérante ne conteste pas la légitimité de la lutte contre le terrorisme et la criminalité organisée. Il faut cependant rappeler que les mesures consacrées par la loi attaquée, le traitement de données personnelles de l'ensemble des voyageurs par avion en provenance et à destination des Etats-Unis, ne se limitent pas à ces deux formes de criminalité grave. Comme exposé plus haut, elles s'appliquent aussi « pour préserver la sécurité publique et à des fins de maintien de l'ordre », conformément au préambule de l'accord et, d'autre part, en vertu de la lettre du DHS, pour toute finalité quelconque, à la seule condition que l'utilisation des PNR soit « requise par la loi » aux Etats-Unis⁴⁶.

Comme déjà mentionné plus haut, aux termes de la lettre du DHS (article I) le simple fait qu'une loi, en vigueur ou à adopter, le requière, permettra l'utilisation effective de données PNR sans aucune exigence de finalité. Il n'est donc pas exclu que des données soient utilisées

⁴⁵ Avis du Conseil d'Etat n° 45.582/4 du 2 février 2009, Doc. Parl. Sénat, session 2008-2009, n° 4-1432/1, p 42.

⁴⁶ Art. III de la lettre du DHS.

en dehors de tout objectif visé par l'article 8 de la CEDH. Ceci suffirait à conclure que le but n'est pas légitime.

Selon le contrôleur européen de la protection des données, dans l'avis donné au projet visant à mettre en place, sur le territoire de l'Union européenne, le même type de traitement que ceux effectués par les autorités américaines : « Alors que l'objectif général de lutte contre le terrorisme et la criminalité organisée est en soi clair et légitime, l'objet du traitement qu'il est prévu de mettre en oeuvre ne semble pas suffisamment délimité et justifié. »⁴⁷.

Selon certains juges de la Cour EDH, « Quant à la question du but légitime, la Cour admet d'ordinaire sans difficulté la légitimité de l'objectif défini par le Gouvernement sous réserve qu'il relève de l'une des catégories visées au paragraphe 2 des articles 8 à 11. Toutefois, pour la sécurité nationale comme pour d'autres buts, j'estime qu'il doit exister au moins un lien raisonnable et réel entre les mesures portant atteinte à la vie privée et l'objectif invoqué pour que celui-ci puisse être considéré comme légitime. A mon sens, expliquer que la conservation, pour ainsi dire sans discernement, d'informations relatives à la vie privée d'individus correspond à un souci légitime de sécurité nationale pose manifestement un problème »⁴⁸.

III.2 Un but implicite illégitime : le profilage selon des critères inconnus

Même si l'utilisation devait se limiter à la lutte contre le terrorisme et la criminalité grave, il ne faudrait pas en conclure que les buts sont légitimes pour autant, compte tenu de l'efficacité douteuse, de l'ampleur et la légitimité très contestable des moyens mis en oeuvre pour atteindre ces buts.

Selon la lettre du DHS, « Le DHS peut obtenir la plupart des éléments informatifs contenus dans les données PNR en examinant le billet d'avion d'une personne et d'autres documents de voyage en vertu du pouvoir de contrôle aux frontières dont il est normalement investi, mais la capacité à recevoir ces données par voie électronique augmente de manière considérable la capacité du DHS à axer ses ressources sur les préoccupations de risque élevé, facilitant et préservant ainsi le trafic passagers légitime.»⁴⁹. Un des objectifs du traitement serait donc d'optimiser les contrôles aux frontières en les concentrant sur les personnes qui présenteraient un certain profil de risque. La manière dont les autorités définissent ce profil et identifient les personnes qui y correspondent n'est pas expliquée, ni dans l'accord, ni dans la lettre du DHS.

Selon le contrôleur européen précité, « La préoccupation majeure du CEPD est liée au fait que des décisions concernant des personnes seront prises à partir de modèles et de critères établis en faisant appel aux données relatives à l'ensemble des passagers. Il est donc possible que des décisions concernant une personne soient prises (au moins en partie) sur la base de modèles établis à partir des données relatives à d'autres personnes. Par conséquent, c'est en

⁴⁷ Avis du contrôleur européen de la protection des données sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives (2008/C 110/01), J.O.U.E. du 01/05/2008, pp. 3-4. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_FR.pdf

⁴⁸ Opinion concordante du juge Wildhaber, à laquelle M. Makarczyk, M. Türmen, M. Costa, M^{me} Tulkens, M. Casadevall et M^{me} Weber déclarent se rallier, suite à l'arrêt Rotaru précité.

⁴⁹ article III de la lettre du DHS.

faisant référence à un contexte abstrait que seront prises des décisions qui pourraient avoir des répercussions importantes pour les personnes concernées. Or, il est extrêmement difficile, pour des particuliers, de se défendre contre de telles décisions. »⁵⁰.

Le même contrôleur souligne ceci : «*La récolte de données n'est pas limitée aux personnes présentant un risque : l'accord autorise une collecte généralisée de données personnelles et une évaluation du risque s'appliquant d'une façon indifférenciée à tous les individus, y compris donc un traitement de données personnelles sur une grande majorité de personnes innocentes.* » (p.1).⁵¹

Il apparaît que l'objectif des autorités américaines consiste notamment à réaliser des opérations de profilage, permettant d'identifier des suspects potentiels sur base d'éléments socio-démographiques et statistiques.

La requérante attire l'attention de Votre Cour sur le fait que de telles opérations de profilage ont déjà été jugées contraires aux droits fondamentaux, notamment par la Cour constitutionnelle allemande⁵².

Pour la requérante, l'objectif d'établir des opérations de profilage ne peut passer pour légitime au sens de l'article 8, tel qu'interprété ci-dessus.

La deuxième branche du moyen est donc fondée.

IV. Troisième branche du moyen : Les ingérences ne sont pas nécessaires dans une société démocratique

IV.1. La récolte et le traitement systématiques de données de personnes innocentes ne sont pas proportionnés

Comme on l'a décrit plus haut, les modalités du traitement ne sont pas définies mais les déclarations du DHS permettent de conclure de manière implicite mais certaine que les

⁵⁰ Avis du contrôleur européen de la protection des données sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives (2008/C 110/01), J.O.U.E. du 01/05/2008, pp. 3-4. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_FR.pdf

⁵¹ Texte original : « *the collection of data is not focused on persons presenting a risk: the agreement allows for a bulk collection of personal data and risk assessment applying in an undifferentiated way to all individuals, including therefore a processing of personal data on a great majority of innocent people.* »

⁵² Selon la Cour suprême allemande, la récolte massive de données personnelles de personnes innocentes à des fins de profilage est contraire aux droits fondamentaux. Seuls des indices basés sur des faits concrets de préparation ou de commission d'actes terroristes pourraient justifier la collecte de données. Décision du 4 avril 2006, citée par Open Society Justice initiative, *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, p 70, disponible sur:

http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/publications/profiling_20090526/profiling_20090526.pdf et par Olivier DE SCHUTTER et Julie RINGELHEIM, « Ethnic Profiling: A Rising Challenge for European Human Rights Law », *The Modern Law Review*, 2008, 71 (3), p 376.

données PNR sont utilisées notamment à des fins de profilage dans l'objectif d'« axer ses ressources sur les préoccupations de risque élevé, facilitant et préservant ainsi le trafic passagers légitime. » (point III de la lettre du DHS).

A l'égard d'une proposition de la Commission européenne visant des objectifs similaires, le contrôleur européen pour la protection des données a fait notamment les remarques suivantes : « *Le respect du principe de proportionnalité suppose non seulement que la mesure proposée soit efficace, mais aussi que l'objectif poursuivi par la proposition ne puisse être atteint au moyen d'instruments portant moins atteinte à la vie privée. L'efficacité des mesures prévues n'a pas été démontrée.* »⁵³.

La requérante attire l'attention sur le fait qu'au contraire, la méthode de la collecte de données à grande échelle (« data mining ») afin de dresser des profils de suspects potentiels a démontré son inefficacité. En effet, l'affaire susmentionnée qui a fait l'objet d'une décision de la Cour constitutionnelle allemande concernait une opération de recueil de données sensibles d'environ 8,3 millions de personnes aux profils similaires à ceux de la cellule de Hambourg, dont certains auteurs des attentats du 11 septembre 2001 faisaient partie. Une base de données d'environ 32.000 terroristes dormants potentiels a été établie par la police: des hommes entre 18 et 40 ans, (ex)étudiants, musulmans ou originaires d'un pays où l'islam est majoritaire. Ensuite, les policiers se sont focalisés sur 1.689 personnes qui ont fait l'objet d'enquêtes plus approfondies: interrogatoires de leur entourage, parfois de leur employeur, mesures de surveillance rapprochée pouvant aller jusqu'aux écoutes téléphoniques. Cette gigantesque opération n'a abouti à aucune poursuite, et encore moins à des condamnations pour terrorisme ou délits liés⁵⁴.

« La lutte contre le terrorisme peut certainement constituer un motif légitime pour appliquer des exceptions aux droits fondamentaux à la vie privée et à la protection des données. Toutefois, pour être valable, la nécessité de l'ingérence doit s'appuyer sur des éléments clairs et indéniables, et la proportionnalité du traitement doit être démontrée. Cette exigence s'impose d'autant plus dans le cas d'une atteinte considérable à la vie privée des personnes concernées, comme celle que prévoit la proposition. On ne peut que constater que la proposition ne contient aucun élément justificatif de ce type et que les tests de nécessité et de proportionnalité ne sont pas rencontrés. » (pp. 5 - 6).

IV. 2. Une durée de conservation de 15 ans sans garantie de destruction des données n'est pas proportionnée

Compte tenu des objectifs flous et très larges qui permettent l'utilisation des données (voir plus haut), il est totalement disproportionné de conserver des données personnelles dans une

⁵³ Avis du contrôleur européen de la protection des données sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives (2008/C 110/01), J.O.U.E. du 01/05/2008, p 5.

⁵⁴ Open Society Justice initiative, *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, p 68-69. Version originale en anglais: http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/publications/profiling_2_0090526/profiling_20090526.pdf. Sommaire et recommandations en français: http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/publications/profiling_2_0090526/french_20090609.pdf

base de données active pendant une période de sept ans. A titre de comparaison, on peut relever que la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, prévoit un effacement de principe « dans les vingt-quatre heures qui suivent la transmission ».⁵⁵

La requérante rappelle que la conservation peut encore se prolonger pendant au moins 8 ans, sous forme « passive » mais avec un traitement possible sur simple autorisation administrative et sans contrôle ni judiciaire ni par une autorité de contrôle similaire.

A cet égard, le groupe 29 a fait l'observation suivante : « Du point de vue de la protection des données, il n'existe aucune différence entre les périodes actives et «inactives» d'accès. Tant que les données à caractère personnel peuvent être consultées, même dans des cas très limités et restrictifs, au cours d'une période inactive, elles restent disponibles dans une base de données et peuvent être consultées et traitées par le DHS. Dès lors, dans les faits, le délai de conservation est passé de trois ans et demi (dans l'accord de 2004, N de la requérante) à quinze ans. »⁵⁶

La durée totale de conservation est donc de 15 ans, sans garantie de destruction. S'agissant de données personnelles récoltées de manière systématique sur des personnes innocentes, on ne peut que conclure à l'absence de nécessité dans une société démocratique.

IV. 3. Le traitement des données sensibles n'est pas nécessaire et potentiellement discriminatoire

Les données sensibles ne sont pas du tout exclues du traitement concernée par l'accord.

Les rubriques 17 et 18 visées à l'art. III de la lettre du DHS concernent, selon le gouvernement, des « données sensibles ». Ces dernières ne sont définies que par l'exposé des motifs dans les termes suivants :

- Données OSI : catégorie optionnelle de données. Il s'agit d'une zone de saisie libre contenant les mentions des demandes diverses exprimées par un passager; comme par exemple la fourniture d'une chaise roulante à l'arrivée.
- Données SSI/SSR (Special Service Request) : il s'agit de demandes de services spécifiques en fonction notamment des préférences alimentaires, de l'état de santé ou de l'âge (par exemple : végétarien, diabétique, sans sel, sans porc, assistance médicale).
- Informations APIS (Advance Passenger Information System) : il s'agit de données concernant tous les passagers et les membres de l'équipage. La liste de ces données se situe à l'article 3, 2o, de la directive 2004/82/CE du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers. Ces données dites APIS doivent être transmises avant la fin de l'enregistrement »⁵⁷.

⁵⁵ Article 6 §1^{er} al. 3 (JOCE L 261 du 6 août 2004).

⁵⁶ Avis du groupe 29 du 17 août 2007 précité.

⁵⁷ Exposé des motifs, Doc. Parl. Sénat, session 2008-2009, n° 4-1432/1, p 13.

Selon la lettre du DHS, les données à caractère personnel « qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle de la personne (...) sont incluses dans les types susmentionnés de données PNR » et donc transmises au DHS.

Il va de soi que les informations concernant, par exemple, les repas pris dans l'avion peuvent révéler une conviction religieuse ou philosophique. Combinée avec les « informations de contact », l'occupation des sièges, les informations sur la réservation, il devient dès lors possible de dresser un tableau permettant de connaître les affinités d'un groupe de personnes, les fréquences de leurs voyages, etc. Il s'agit donc d'informations dont la connaissance et la conservation constituent de très sérieuses ingérences dans la vie privée.

Comme mentionné plus haut, l'article 6 de la Convention n°108 de 1981 soumet le traitement automatisé de ces données à des garanties appropriées.

Sur ce point, une comparaison des garanties offertes par l'accord PNR précédant de 2004 et le présent accord de 2007 est également intéressante. L'accord de 2007 ne contient rien à cet égard. La lettre d'explications du DHS (laquelle est tel qu'exposé ci-dessus dépourvue de tout effet contraignant pour les autorités américaines) contient dans son article III certaines considérations quant à l'utilisation des données dites sensibles. Le DHS affirme qu'il aura recours à un système automatisé qui filtre les codes et termes PNR sensibles. Il affirme en outre qu'il n'utilisera pas ces informations et qu'il supprimera ces données « dans les meilleurs délais ». Ces promesses sont néanmoins immédiatement suivies d'une exception qui met en réalité à néant la crédibilité des promesses précitées. En effet, dans des cas exceptionnels qu'ils sont les seuls à pouvoir estimer, sans contrôle d'une autorité indépendante de protection des données, les fonctionnaires du DHS peuvent avoir accès à ces données, y compris celles qui sont sensibles. Cela implique dès lors que ces données ne seront pas filtrées par un système automatisé et seront effectivement stockées. Toujours selon la lettre du DHS, ces données seront détruites 30 jours après que les fins pour lesquelles elles ont été consultées ont été atteintes « sauf si leur conservation est exigée par la loi », sans autre précision.

Ensuite, la lettre contient la clause suivante « *Le DHS fera normalement savoir à la Commission européenne dans les quarante-huit heures que ces données ... ont été consultées.* »⁵⁸. Il est évident que de par la présence du mot « normalement » sans que pour le surplus on ne définisse ce qui est normal ou pas, rend cette communication totalement aléatoire et dépourvue de toute effectivité.

La déclaration du bureau des douanes et de la protection des frontières du DHS, annexée à la décision 2004/535/CE de la Commission relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des Etats-Unis d'Amérique, que les autorités américaines s'étaient engagées formellement à respecter dans l'art. 3 de l'accord PNR de 2004, disait, dans son point 9, que les autorités américaines compétentes s'engageaient à ne

⁵⁸

souligné par la requérante.

pas utiliser lesdites données sensibles figurant dans les PNR. Aucune exception n'était prévue⁵⁹.

Il ressort de l'accord et de la lettre du DHS que les autorités des Etats-Unis ont la possibilité de traiter, de conserver et de transférer des données sensibles sans réelles garanties quant au tri effectif et à l'effacement de ces données, ni à la durée de la conservation, ni à leur destruction effective après leur utilisation. Ce traitement de données sensibles de personnes qui ne sont pas soupçonnées de délits, sans contrôle effectif, ne peut passer pour nécessaire dans une société démocratique.

IV. 4. Le traitement de certaines données n'est absolument pas pertinent en vue des objectifs déclarés

Comme déjà examiné plus haut, les données PNR comprennent notamment les informations suivantes :

« 5. Informations disponibles sur « les grands voyageurs » et les programmes de fidélisation (c'est-à-dire billets gratuits, surclassement, etc...) » ; et

14. Informations sur l'établissement des billets, y compris le numéro du billet, billets aller simple et données Automated Ticketing Fare Quote (prix du billet) »

La requérante n'aperçoit pas dans quelle mesure le traitement de ces informations de nature commerciale pourrait s'avérer pertinent pour lutter contre le terrorisme, la criminalité grave de nature transnationale ou pour préserver la sécurité publique. La requérante n'a trouvé aucune explication convaincante à cet égard, ni dans l'accord, ni dans la lettre du DHS, ni dans l'exposé des motifs de la loi attaquée. Il faut donc en conclure que le traitement de ces informations n'est manifestement pas nécessaire dans une société démocratique.

IV. 5. La présomption de « niveau adéquat de protection » conférée au DHS par l'accord n'est conforme à la réalité et peut porter atteinte à la prééminence du droit

Il résulte des dispositions visées au moyen qu'un transfert de données personnelles vers un pays tiers ne peut être considéré comme « nécessaire dans une société démocratique » que si ce pays présente un niveau de protection « adéquat » en matière de protection des données personnelles.

L'article 6 de l'accord prévoit que « le DHS est réputé assurer un niveau adéquat de protection des données PNR transférées de l'Union européenne ».

⁵⁹ L'exception prévue au point 5 de la dite lettre ne concerne que les autres informations contenues dans les rubriques « OSI » et « SSI/SSR » à l'exception des données sensibles. Cela ressort de l'absence de toute exception aux points 9, 10 et 11 de la dite lettre lesquels concernent précisément les données sensibles.

IV. 5.1) La présomption de niveau adéquat n'est pas conforme à la réalité

L'accord n'explique pas sur quels éléments se fonde la présomption de niveau adéquat de protection conférée au DHS. L'article 1, permettant la transmission des données PNR par les transporteurs aériens, se fonde « sur les assurances données dans la lettre d'explication du DHS sur la protection des données PNR ». A maints égards, la requérante a démontré dans le présent recours, que ces prétendues assurances sont totalement illusoire et ne permettent pas d'assurer un niveau satisfaisant de protection de la vie privée.

Par ailleurs, la requérante constate qu'il est manifestement déraisonnable de parler de niveau de protection adéquat concernant le niveau de protection des données personnelles aux États-Unis.

Selon Yves Poullet et Antoinette Rouvroy, « Le critère habituel, aux États-Unis, adopté et appliqué par la Cour suprême pour décider de l'existence d'un droit à la protection de la vie privée dans des secteurs de l'existence humaine où ce droit était revendiqué contre l'intrusion gouvernementale, est le critère sociologique plutôt que normatif de l'existence de legitimate expectations of *privacy* (ou d'attentes légitimes du public à ce que telle ou telle activité, tel pan de l'existence humaine, soit exempt de la surveillance ou de l'intrusion) dans le domaine ou les circonstances visées. »⁶⁰ On a pu montrer, « en comparant la manière dont les juges aux États-Unis et en Allemagne identifient les cas de violation du droit à la protection de la vie privée, qu'en présence de mesures techniques de surveillance, le standard des « legitimate expectations of privacy » protégeait beaucoup moins l'individu confronté à cette surveillance que ne le protègent les principes normatifs (tels que le principe du respect dû à la dignité humaine, et le principe suivant lequel les individus ont un domaine inviolable dans lequel ils peuvent développer librement leur personnalité) sur lesquels s'appuie la Cour constitutionnelle allemande »⁶¹

Compte tenu de ces éléments, la requérante considère qu'on ne peut conclure de manière raisonnable au niveau de protection adéquat. Ce constat ne peut qu'aboutir au constat d'absence de nécessité des mesures visées par la loi attaquée dans une société démocratique.

IV. 5.1) La présomption de niveau adéquat de protection permet la violation du droit

En outre, l'article IX de la lettre du DHS mentionne que « le DHS favorisera le transfert d'informations analytiques provenant des données PNR par les autorités américaines compétentes aux services de police et aux autorités judiciaires des États membres et, le cas échéant, à Europol et à Eurojust ». Il est indéniable qu'en vertu de l'accord, les autorités américaines disposent de quantités très importantes de données personnelles concernant des citoyens ou résidents de l'Union européenne, qui, à l'heure actuelle ne peuvent pas être récoltées par la plupart des services de police et des autorités judiciaires européennes. En effet, dans de nombreux pays de l'UE dont la Belgique, ceux-ci ne disposent pas de base légale suffisante leur permettant de recueillir et de traiter de telles quantités de données concernant des citoyens qui ne font pas l'objet d'une enquête. Dans l'état actuel du droit, ce

⁶⁰ Yves Poullet et Antoinette Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », Karim Benyekhlef, Pierre Trudel (ed.), *Etat de droit et virtualité*, Montreal, Themis, 2009, p 164 et la référence citée.

⁶¹ Ibid.

passage de la lettre du DHS contient le risque que ces autorités puissent entrer en possession des données PNR via les autorités américaines, en violation du droit et des procédures actuellement en vigueur, et ce sans que la nécessité de ces transferts ne soit démontrée.

Comme le relevait le groupe 29, on ne sait pas exactement ce que ces « informations analytiques » contiendront et si elles incluront des données à caractère personnel⁶². Selon Thomas Hammarberg, commissaire aux droits de l'homme du Conseil de l'Europe, « les données à caractère personnel collectées pour un besoin de police particulier (parer une menace, par exemple) ne peuvent être utilisées à d'autres fins (enquêter sur une infraction, par exemple) que si elles auraient pu être recueillies dans ce second but de manière indépendante »⁶³. Le mécanisme décrit par l'article IX de la lettre du DHS permet de contourner totalement ce principe.

En raison du risque décrit ci-dessus, il faut considérer que les mesures prévues par la loi attaquée, qui permettent une forme de rétro-transmission d'une grande quantité de données personnelles sans base légale vers des autorités policières et judiciaires de l'UE, ne sont pas nécessaires dans une société démocratique.

IV. 6 La transmission des données PNR à d'autres administrations ou à des Etats tiers n'est pas proportionnée

Comme on l'a vu au point II. 2. 4), le DHS peut transférer des données personnelles à d'autres administrations et même à des Etats tiers sans réelles garanties concernant la finalité, les modalités et la durée du traitement. Rien dans l'accord, ni dans la lettre du DHS n'interdit que des données sensibles fassent l'objet d'un tel transfert. Rien non plus ne limite le champ d'application de ces transferts, qui peuvent avoir lieu tant dans le cadre de la lutte contre le terrorisme que dans le cadre de « la protection des intérêts vitaux (...) d'autres personnes » ou « de toute autre manière requise par la loi. ». La personne concernée n'a aucune garantie d'être informée de ces transferts. Dans la rédaction du texte, rien n'empêcherait par exemple le DHS de transmettre des données personnelles sensibles concernant les opinions politiques ou les convictions religieuses d'un voyageur reconnu réfugié, au pays vis-à-vis duquel il a été établi qu'il risquait des persécutions.

Compte tenu de ces éléments, la requérante ne peut que conclure au caractère disproportionné de ces possibilités de transferts, et donc à l'absence de nécessité dans une société démocratique.

IV. 7 Une ingérence ne peut pas être considérée comme nécessaire en l'absence de recours effectif

Pour la Cour EDH, le refus d'informer les personnes de l'intégralité des renseignements à leur sujet qui sont conservés dans un fichier secret d'une autorité publique s'analyse en une

⁶² Avis 5/2007 du Groupe 29, se référant à GT 136 «Avis 4/2007 sur le concept de données à caractère personnel», adopté le 20 juin 2007.

⁶³ Commissaire aux droits de l'homme du Conseil de l'Europe, Lutte contre le terrorisme et protection du droit au respect de la vie privée, CommDH/IssuePaper(2008)3, p 9.

ingérence dans l'exercice de leur droit au respect de leur vie privée⁶⁴. L'existence d'un recours effectif permettant d'obtenir l'accès, la rectification et l'effacement de données est requise par l'article 22 de la Constitution en combinaison avec les articles 8 et 13 de la CEDH, ainsi qu'avec les articles 8, 9 et 10 de la Convention 108.

La requérante constate tout d'abord que le texte de l'accord ne contient aucune obligation de prévoir un recours accessible et effectif. La seule disposition de l'accord (article 7), se limite à mentionner que « Les Etats-Unis et l'UE coopéreront avec les parties intéressées de l'industrie aéronautique pour mieux faire connaître les avis décrivant les systèmes de données PNR (y compris les pratiques en matière de collecte et de rectification) aux voyageurs et encouragera les compagnies aériennes à mentionner ces avis et à les intégrer dans le contrat officiel de transport. ». Il est évident que le citoyen ne peut tirer aucun droit subjectif au recours d'une telle disposition.

Le point IV de la lettre du DHS est consacré au « Droit d'accès et droit de regard ».

Ce point prévoit que « Le DHS a pris une décision politique visant à étendre les protections administratives prévues par la loi sur le respect de la vie privée (Privacy Act) aux données PNR stockées dans le système automatisé de ciblage (ATS) quels que soient la nationalité ou le pays de résidence de la personne concernée, y compris aux données relatives aux citoyens européens » (souligné par la requérante). Il est évident que si la possibilité pour le citoyen belge ou européen d'avoir accès à ses données dépend d'une décision politique, pareille décision peut être remise en cause sans préavis et ne constitue pas une véritable garantie.

Par ailleurs, ce passage de la lettre du DHS renvoie aussi à la loi américaine sur le respect de la vie privée (Privacy Act) et à la loi américaine sur la liberté de l'information (Freedom of Information Act, ci-après dénommé « FOIA ») ainsi qu'au site Internet du DHS, où, en pratique, il est extrêmement difficile de trouver l'information pertinente. La lettre mentionne également une adresse où les demandes d'accès « aux données personnellement identifiables contenues dans les PNR fournies par le demandeur » peuvent être envoyées. Il découle de cette formulation que le citoyen ne pourra avoir accès qu'aux données qu'il a lui-même fournies, et non pas à l'entièreté des données qui le concernent et qui peuvent être en possession des autorités américaines, notamment des « données analytiques » mentionnées précédemment. Ceci limite déjà considérablement l'utilité du recours.

En outre, il existe de nombreuses considérations qui permettent au DHS de refuser ou retarder la divulgation de la totalité ou d'une partie du dossier PNR à un demandeur.

La requérante fait également observer que les citoyens n'ont pas un accès égal au recours. L'introduction d'un recours auprès des autorités américaines nécessite la connaissance de l'anglais. La technicité et la complexité des lois américaines rend nécessaire l'intervention d'un avocat en cas de refus d'accès. Aucun droit à l'aide juridique n'est prévu dans l'accord. L'accord ne contient rien sur le contenu que doit revêtir l'avis d'information que le DHS communiquera au voyageur, ni la langue dans laquelle celui-ci sera rédigé.

A cet égard, le contrôleur européen pour la protection des données notait récemment ceci : *“Bien que des possibilités de rectification soient prévues dans l'accord, l'exercice de ses*

⁶⁴ Cour ECH Segerstedt-Wiberg et autres c. Suède du 6 juin 2006, § 99.

droits par l'individu en pratique, et particulièrement le droit d'avoir accès aux données personnelles, reste un défi : les exceptions liées à des raisons de sécurité pourraient empêcher l'exercice effectif de ces droits. »⁶⁵

Compte tenu de ces observations, l'effectivité de ce recours est inexistante.

En ne prévoyant pas de recours effectif permettant d'assurer au citoyen le respect des normes de protection de la vie privée, le législateur a violé les dispositions visées au moyen.

Second moyen: Violation de l'article 22 de la Constitution combiné avec le principe général de sécurité juridique et le principe général de non rétroactivité de la loi

La fin du point VII de la lettre du DHS mentionne que « Les périodes de conservation mentionnées ci-dessus s'appliquent aussi aux données PNR de l'UE collectées sur la base des accords entre l'UE et les Etats-Unis du 28 mai 2004 et du 19 octobre 2006. »

Pour rappel, ce point prévoit une durée de conservation de 15 ans sans garantie crédible d'effacement des données. L'accord de 2004 prévoyait une durée de conservation ne pouvant pas dépasser trois ans et demi⁶⁶.

Les personnes qui ont voyagé en provenance ou à destination des Etats-Unis avant l'entrée en vigueur de l'accord de 2007 pouvaient légitimement s'attendre à ce que leurs données ne soient traitées que pour une durée maximale de trois ans et demi. Le point précité aura pour effet en pratique de prolonger – en réalité, plus que quadrupler - la durée de conservation de ces données, récoltées sous l'empire de l'accord de 2004.

Selon la jurisprudence de Votre Cour, « La non-rétroactivité des lois est une garantie ayant pour but de prévenir l'insécurité juridique. Cette garantie exige que le contenu du droit soit prévisible et accessible, de sorte que le justiciable puisse prévoir, à un degré raisonnable, les conséquences d'un acte déterminé au moment où cet acte est accompli »⁶⁷.

Il découle de ce principe que « la rétroactivité peut uniquement être justifiée lorsqu'elle est indispensable à la réalisation d'un objectif d'intérêt général. »⁶⁸

La requérante n'a trouvé, ni dans l'accord, ni dans la lettre du DHS, ni dans l'exposé des motifs, une forme d'explication convaincante permettant de justifier une atteinte à ce principe.

⁶⁵ Texte original : « although redress possibilities are foreseen in the agreement, the exercise of rights by the individual in practice, and especially the right to access personal data, remains a challenge: exceptions linked with security reasons could prevent effective exercise of rights. » Contrôleur européen de la protection des données, communiqué du 25 janvier 2010, disponible sur http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-01-25_EU_US_data_exchange_EN.pdf.

⁶⁶ Pour une comparaison détaillée des deux accords, voir l'avis du groupe 29 du 17 août 2007 précité.

⁶⁷ Voir, parmi beaucoup d'autres, l'arrêt n° 178/2009 du 12 novembre 2009, point B.6.

⁶⁸ Ibid. souligné par la requérante.

Elle n'aperçoit aucun argument permettant de justifier en quoi la rétroactivité prévue par la loi attaquée concernant la durée de conservation serait « indispensable » à la réalisation des objectifs poursuivis.

En prolongeant a posteriori une durée de conservation des données personnelles récoltées sous l'empire d'un accord prévoyant une durée plus de quatre fois plus courte, la loi attaquée viole de manière flagrante l'article 22 de la Constitution combiné avec le principe le principe général de sécurité juridique et le principe général de non rétroactivité de la loi.

A CES CAUSES

La requérante vous prie,

Messieurs les Présidents, Messieurs les Juges,

d'annuler la loi du 30 novembre 2009 portant assentiment à l'Accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au Ministère américain de la Sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007 (publiée au Moniteur belge du 29 décembre 2009).

Bruxelles, le 1^{er} mars 2010

Pour la requérante,
un de leurs conseils,
Thomas MITEVOY

Annexes :

- 1) Loi attaquée (copie du Moniteur belge du 29 décembre 2009, pp. 82126 à 82138)
- 2) Décision du Conseil d'administration de l'asbl Ligue des droits de l'homme d'introduire le présent recours, du 21 janvier 2010.
- 3) Copie des statuts de l'asbl Ligue des droits de l'homme.
- 4) Avis du Groupe de travail Article 29 n° 5/2007 « concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure », adopté le 17 août 2007 (également disponible sur:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_fr.pdf).

- 5) Avis du Contrôleur européen pour la protection des données du 20 décembre 2007 sur la proposition de décision-cadre COM (2007) 654, (disponible également sur: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_FR.pdf)