Avis n° 01 /2010 du 13 janvier 2010

Objet: avis d'initiative relatif au 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 Ministère américain de la sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu la demande d'avis du président, reçue le 27 octobre 2009 ;

Vu le rapport de Monsieur De Schutter ;

Émet d'initiative, le 13 janvier 2010, l'avis suivant :

I. INTRODUCTION

En juillet 2007, l'Union européenne a conclu un nouvel accord avec les États-Unis sur le traitement et le transfert de données à caractère personnel (notamment) de passagers au Ministère américain de la sécurité intérieure (Department of Homeland Security, ci-après "DHS"). Cet Accord a été conclu dans le cadre juridique du troisième pilier[1] et a normalement une durée de validité de sept ans[2]. Par commodité, on l'appellera ci-après "l'Accord PNR 2007", afin de le distinguer de deux anciens accords PNR[3].

L'accord a été accompagné desdites "assurances" unilatérales au nom du DHS dans une lettre adressée à la présidence de l'Union européenne, dont une copie a été adressée à la Commission européenne. L'Union européenne a ensuite déclaré que le niveau de protection des données offert par le DHS dans les Assurances était jugé adéquat[4] pour le transfert et le traitement de données PNR définis dans l'Accord. D'après l'Exposé des motifs, ces assurances ont un caractère contraignant[5].

1 Objectifs du projet de loi

Le projet de loi[6] sert principalement à approuver l'Accord PNR 2007.
Le projet de loi sert d'assentiment à l'accord et à son intégration dans l'ordre juridique belge pour ainsi octroyer une prévisibilité[7] adéquate aux ingérences dans la vie privée (article 8 de la CEDH).

---

[1] L'idée que l'Union européenne repose sur trois piliers a été introduite en avril 1991 sous la présidence Luxembourgeoise via le "non-paper" (Europe, doc. n° 1709/1710, 3 mai 1991). Ces trois piliers sont : 1° les dispositions relatives aux communautés ; 2° les dispositions relatives à une politique étrangère et de sécurité commune ; et 3° les dispositions relatives à la coopération en matière de justice et d'affaires intérieures.

[2] Voir convention 9 de l'Accord.

[3] Un premier Accord PNR était en vigueur du 28 mai 2004 jusqu'au mois d'octobre 2006. Un deuxième accord (intérimaire) du 19 octobre 2006 a été adopté après l'arrêt PNR de la Cour de Justice du 30 mai 2006 et a expiré le 31 juillet 2007.

[4] La Commission en prend acte et souligne que cette déclaration d'adéquation ne se rapporte qu'aux transferts internationaux de données PNR. Cette déclaration n'a pas la valeur d'une évaluation (réciproque) ou d'un audit indépendant du respect des droits et principes en vertu de l'article 8 de la CEDH, de la Convention 108 et (des autres dispositions) de la Directive 95/46/CE.

[5] Voir page 8 (commentaire de l'article 3) de l'Exposé des motifs, Sénat, 4-1432/1.

[6] Le 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 Ministère américain de la sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007, Sénat, 4-1432/1.

[7] Ladite "condition de prévisibilité" à laquelle la loi doit répondre signifie d'après la Cour européenne des Droits de l'Homme qu'elle soit suffisamment précise au niveau de la formulation de sorte que tout individu, dans les circonstances données, puisse prévoir raisonnablement les conséquences d'un acte déterminé. Voir notamment *CEDH, 26 mars 1987, Leander c. Suède, § 51.*

Enfin, il apparaît également qu'il y a une volonté de régulariser *de facto* la situation d'échange informel d'informations[8] et d'offrir une sécurité juridique pour les transporteurs aériens.

2. Données traitées

2.1. Données PNR : pas uniquement les passagers aériens (potentiels)

Les données à caractère personnel traitées concernent ce qu'on appelle généralement les PNR ou "Passenger Name records", ci-après "données PNR". Comme c'était déjà le cas en vertu de l'ancien Accord PNR 2007, les données PNR ne se rapportent pas uniquement aux listes de passagers au sens strict du terme, qui ne reprennent que des données d'identification des passagers telles que le prénom, le nom, l'adresse, le numéro de téléphone, la date de naissance, la nationalité, le numéro de passeport et le sexe (voir le point 2.2. ci-après).
Contrairement à ce que l'on affirme souvent, il ne s'agit pas non plus uniquement de données de vol des personnes qui sont réellement passagers. Il s'agit par exemple aussi de personnes qui réservent des services tels que des voyages en train, des nuits d'hôtel, des voitures de location, des ferrys, des assurances et d'autres données qui sont reprises dans des systèmes SIR[9] [10]. Les données de personnes autres que des voyageurs (potentiels) sont reprises comme le nom de "*la personne qui paie les tickets, les données relatives à la carte de crédit, les amis, la famille ou les collègues qui ont réservé le même trajet, le nom de l'agent de voyage et ses coordonnées*.[11]"

2.2. Les autres informations API plus détaillées

La liste finale des 34 éléments de données décrits dans des déclarations unilatérales antérieures au nom du DHS de 2004 comprend également d'autres informations sur les passagers, appelées "Advance Passenger Information" (API). Ces données concernent notamment les adresses de séjour dans le pays de destination, la description complète des déplacements, les personnes de contact et des données médicales. Sont également reprises : les données bancaires comme le mode de paiement, le numéro de carte de crédit et les habitudes alimentaires qui peuvent être un indicateur potentiel d'une conviction religieuse. L'on constate que cette liste de 34 éléments de données va également plus loin que les systèmes PNR australien et canadien (19 éléments de données).

---

[8] Page 20 *in fine* de l'Exposé des motifs.

[9] Systèmes informatisés de réservation, souvent exprimés en abrégé "SIR". Les SIR sont des systèmes informatiques pour l'enregistrement, la consultation et la diffusion d'informations de voyage et la réservation de tickets. Ce système est aussi souvent appelé "Global Distribution Systems" ou "GDS".

[10] Point 3.6.1 de l'avis du Comité économique et social européen, JO 2008/C 224/12.

[11] Point 3.6.1. de l'avis du Comité économique et social européen.

L'adaptation des 34 éléments de données en 19 éléments de données en vertu de la lettre d'accompagnement du DHS à l'Accord PNR 2007 donne l'impression, à première vue, que la liste des données complémentaires de 2004 a été réduite (voir également ci-après). Cette adaptation n'a toutefois pas empêché que les éléments de données soient encore étendus[12]. On retrouve notamment dans cette liste de données complémentaires "EU PNR" que le DHS a mentionnées dans sa lettre : la date de réservation/d'émission du billet, la date prévue du voyage, les informations disponibles sur "les grands voyageurs" et les programmes de fidélisation, toutes les informations de contact disponibles, l'agent de voyage, des remarques générales, y compris "les données OSI[13], SSI et SSR[14]", "toutes les informations APIS recueillies"[15] et toutes les informations historiques concernant ces champs.

2.3. Situation en pratique

En réalité, on ne peut néanmoins pas conclure que les SIR et d'autres banques de données PNR contiendront toujours tous les éléments PNR ou API inventoriés officiellement. On ne peut pas non plus exclure que de nombreuses banques de données PNR contiennent également d'autres données. Le fait que la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives[16] parte d'une autre définition des données PNR et API donne peut-être également lieu à une certaine confusion. Les données API sont ainsi les données des passagers et les données PNR concernent les informations plus ciblées sur le profil.

3. Absence de demande d'avis à la Commission et absence de débat parlementaire

La Commission constate qu'au cours de ces dernières années, elle n'a jamais été consultée par les autorités belges compétentes pour une demande d'avis dans cette matière. Cela aurait dû se faire lorsque le représentant belge a été associé aux négociations de l'Accord PNR 2007. La Commission déplore que son avis n'ait pas été demandé à ce moment.

---

[12] L'avis n° 05/2007 du Groupe 29 du 17 août 2007 (WP 138) se réfère à la page 11 au mécanisme d'extension en vertu de l'article III, alinéa 3 de la lettre du DHS. Cette lettre a été publiée au Sénat, 4-1432/1, page 30.

[13] Other service information (OSI).

[14] Lesdites informations "SSI" et "SSR".

[15] Voir à cet égard la consultation au sein du Comité sur l'Union européenne de la Chambre des Lords.

[16] Commission européenne, Proposition de décision-cadre du Conseil du 6 novembre 2007 *relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives*, COM (2007), 654/F, 6 novembre 2007.

On peut se référer à cet égard à l'avis du Conseil d'État n° 45.582/4 du 2 février 2009, plus particulièrement à ce qui est stipulé au point 3. des observations préalables : "*L'avis de la Commission de la protection de la vie privée mériterait d'être recueilli sur les questions de droit examinées ci-après ; elle dispose en effet d'une connaissance des pratiques en vigueur de nature à faciliter la résolution des difficultés que suscite le présent dossier, comme l'a montré son avis n° 48/2003 (…) du 18 décembre 2003, donné sur des plaintes relatives à la transmission de données à caractère personnel par certaines compagnies aériennes vers les États-Unis, avis qui reste d'actualité quant aux principes y énoncés.*"[17]

L'Exposé des motifs mentionne ce qui suit comme raison de l'absence de demande d'avis : "*Comme le souligne le Conseil d'État, le Groupe 29 a adopté le 17 août 2007 l'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 par les transporteurs aériens au ministère américain de la sécurité intérieure, conclu en juillet 2007.*
Étant donné que notre Commission de la protection de la vie privée fait partie du Groupe 29, l'avis rendu par ce dernier couvre également l'avis de la Commission belge de la vie privée. Demander à la Commission de la protection de la vie privée de s'exprimer sur ces questions reviendrait à l'interroger deux fois sur le même sujet. Son avis n'est donc plus à demander puisqu'il a déjà été rendu."[18]

La Commission souligne toutefois qu'elle a une mission qui est clairement distincte de celle du Groupe 29. Ce groupe est un groupe de travail non permanent institué en vertu de l'article 29 de la Directive 95/46/CE. Il ne remplace pas les règles de "prior checking", ni l'exigence permanente de contrôle indépendant dans les différents États membres, qui sont instituées en vertu des articles 20 et 28 de la même Directive, tels qu'exécutés aux articles 17*bis* et 29 de la LVP. L'interprétation dans l'Exposé des motifs va donc à l'encontre de l'obligation de chaque État membre d'instituer une surveillance et un contrôle continus du respect des principes de protection de la vie privée, surtout s'il s'agit de traitements qui comportent incontestablement des risques spécifiques pour les droits et libertés individuels, comme en vertu de l'exécution de l'Accord PNR 2007.

Le législateur se réfère lui-même dans l'Exposé des motifs à la cause d'exception "motif important d'intérêt public" (et "intérêt public important") au sens des articles 6 et 7 de la LVP[19]. Cette confirmation de l'existence d'un intérêt public en tant que cause d'exception rend d'autant plus nécessaire la demande d'application du "prior checking" et d'avis à la Commission.

---

[17] Avis n° 45.582 du 2 février 2009, Sénat, 4-1432/1 – 2008/2009, 39 (numéro 3).

[18] Page 17 de l'Exposé des motifs.

[19] Page 18 de l'Exposé des motifs.

L'approche belge de ce dossier contraste avec celle de nos pays voisins comme les Pays-Bas[20] et le Royaume-Uni[21], où il y a eu un rapport plus détaillé au parlement national ainsi qu'une consultation de ce dernier au sujet de l'Accord PNR 2007, à l'occasion desquels on s'est renseigné notamment sur la signification d'un certain nombre de dispositions imprécises dans cet Accord.

II. CONTEXTE DE L'ACCORD

La Commission constate par ailleurs que son dernier avis dans cette matière date de 2003 et que le contexte européen (voir ci-après à la rubrique II.) a entre-temps évolué.

La Commission souligne le fait que les différents accords PNR continuent sans cesse de faire l'objet de jugements européens indépendants critiques à la lumière de la protection de la vie privée (point 3 ci-après). En outre, l'Accord PNR 2007 peut non seulement être considéré dans son contexte réglementaire (point 1), mais il faut aussi tenir compte des sources de données (point 2) et des évolutions et constatations récentes postérieures à juillet 2007, date de la signature de l'Accord PNR 2007 (point 4).

1. Contexte réglementaire

Il existe plusieurs sources juridiques pour le transfert obligatoire de données de passagers. Outre l'accord en question, il faut également souligner le fait que le transfert de données de passagers est également régi par la Directive 2004/82/CE du 29 avril 2004[22], ci-après "Directive API". Cette directive a été transposée en droit belge par l'arrêté royal du 11 décembre 2006 *concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers*[23]. On peut par ailleurs se référer au projet de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives susmentionné[24], qui visait le règlement d'un "système PNR européen". La présidence

---

[20] Voir la correspondance entre le Ministre néerlandais de la Justice et la deuxième chambre, qui a été accompagnée d'un débat parlementaire. Voir les documents sur le site : http://parlis.nl.

[21] Voir notamment pour le Royaume-Uni le rapport détaillé du Comité sur l'Union européenne de la Chambre des Lords, publié sur le site : http://www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf.

[22] Directive 2004/82/CE du Conseil du 29 avril 2004 *concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers*, JO, 6 août 2004.

[23] M.B., 22 décembre 2006, 73824-73825.

[24] Voir point 2.3 ci-avant.

suédoise a récemment annoncé que l'on interrompait le développement d'un système PNR européen jusqu'à l'entrée en vigueur du Traité de Lisbonne[25].

Quelques constats sont importants à cet égard, comme évoqué notamment par le Contrôleur européen de la protection des données[26] et le Groupe 29 :

- malgré le lancement du dialogue transatlantique via le Groupe de contact UE/États-Unis[27] et la conclusion de quelques accords transatlantiques "ad hoc", il n'y a pas encore de cadre global pour les échanges d'informations transatlantiques ;
- pour l'instant, on ne sait pas encore clairement si un nouveau cadre général entre l'UE et les États-Unis complètera les accords existants ou s'ils resteront en l'état ;
- l'Accord PNR 2007 doit être interprété à la lumière de la jurisprudence européenne[28] en évolution, qui recherche un équilibre entre la poursuite de finalités antiterroristes et le respect des droits humains, surtout au regard du fait que l'Accord PNR 2007 offre globalement une protection moindre par rapport aux accords PNR antérieurs[29] ;
- quelques garanties importantes demandées par le Groupe 29, le CEPD et le Parlement européen n'ont jusqu'à présent pas été réalisées dans le dossier PNR (système push au lieu de pull, protection juridique effective, droit d'être entendu, …) (voir ci-après).

2. Sources de données : intégration de données (systèmes SIR) et réservations via Internet (transporteurs aériens)

Bien que la Directive API constitue formellement un instrument distinct par rapport au projet de loi portant assentiment à l'Accord PNR 2007, qu'elle poursuive d'autres finalités et soit basée sur un pilier européen différent, on ne peut ignorer que dans la pratique, il soit question d'intégration de données au niveau des systèmes de réservation, laquelle doit répondre à un nombre croissant de réglementations PNR. À cet égard, il est important de souligner que de nombreux transporteurs aériens et agences de voyages ont sous-traité la gestion de leur banque de données PNR à des prestataires de SIR. À l'heure actuelle, il n'y a que trois grandes entreprises de SIR au niveau

---

[25] Voir notamment le communiqué de presse suivant du Parlement européen du 6 octobre 2009 : "EU Passenger Name Record talks on hold in Council until Lisbon Treaty is ratified", publié sur le site http://www.europarl.europa.eu/news/expert/infopress_page/019-61958-279-10-41-902-20091006IPR61955-06-10-2009-2009-false/default_fr.htm.

[26] Avis du Contrôleur européen de la protection des données *concernant le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel*, JO C 128, 6 juin 2009.

[27] Voir le rapport publié le 26 juin 2008 : http://ec.europa.eu/justice_home/fsj/privacy/news/2008_fr.htm.

[28] Voir les affaires "Kadi et Barakaat".

[29] Avis WP 138, page 18, alinéa 1.

mondial[30], dont une, suite à une fusion en 2007, utilise encore deux plates-formes et marques distinctes, et dont une seule[31] est établie dans l'UE. Par ailleurs, plusieurs sociétés utilisent le système dit "Shares"[32]. Depuis l'arrivée d'Internet, les tickets d'avion peuvent toutefois aussi être réservés par des systèmes différents des SIR. Du fait que, dans les États membres de l'Union européenne, de plus en plus de personnes ont accès à Internet et que les technologies de réservation de voyages en ligne via les systèmes de réservation en ligne des transporteurs aériens sont toujours plus avancées, les SIR sont de moins en moins souvent la seule manière d'accéder aux informations de voyage[33].

3. Jugement critique de l'Accord PNR 2007 par les autorités européennes indépendantes de protection des données

3.1. Groupe de protection des données article 29

La problématique du transfert (notamment) de données de passagers entre l'Union européenne et les États-Unis a été jugée à plusieurs reprises de façon critique par le Groupe 29. La Commission se réfère aux avis du Groupe 29 n° 78[34], 132[35], 138[36] et 145[37].

---

[30] Il s'agit de : AMADEUS, SABRE, Galileo / Apollo (Travelport) et Worldspan (Travelport). Voir le point 2.2.1 de l'avis du Comité économique et social européen *sur la Proposition de règlement du Parlement européen et du Conseil instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation*.

[31] Amadeus a des succursales en France (marketing, recherche et développement) et en Allemagne (centre de données).

[32] Élaboré et géré par la multinationale EDS qui a été reprise en 2008 par Hewlett Packard.

[33] Point 2.32. du Comité économique et social européen.

[34] Avis 4/2003 *sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers*, approuvé le 13 juin 2003.

[35] Avis 2/2007 *concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record - PNR) aux autorités américaines*, approuvé le 15 février 2007.

[36] 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*, approuvé le 17 août 2007.

[37] Avis commun *sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives présentée par la Commission le 6 novembre 2007, adopté le 5 décembre 2007 par le Groupe article 29 et adopté le 18 décembre 2007 par le groupe de travail sur la police et la justice*.

3.2. Contrôleur européen de la protection des données (ci-après "CEPD")

Le CEPD a également émis plusieurs avis dans cette matière. La Commission se réfère aux avis du 20 décembre 2007[38] et du 11 novembre 2008[39]. Bien que ces avis se rapportent aux traitements de données à caractère personnel au niveau des institutions communautaires (application du Règlement n° 45/2001), ils font toutefois autorité dans cette matière.

3.3. Comité économique et social européen

Le Comité économique et social européen était particulièrement critique sur les accords PNR. Dans son avis du 29 mai 2008 *sur la Proposition de règlement du Parlement européen et du Conseil instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation*, il a affirmé ce qui suit *"Les accords en vigueur entre les États-Unis et l'UE sont des "engagements" qui ne sont ni exécutoires ni juridiquement contraignants*"[40].

4. Évolutions récentes

Les évolutions, jugements et discussions récents aux niveaux américain et européen démontrent en outre un certain nombre de problèmes et d'évolutions dont il faudrait tenir compte, comme :

- l'avis précité du 29 mai 2008 du Comité économique et social européen a souligné le manque d'information des voyageurs : "*La plupart du temps, le public n'est pas conscient de l'existence des SIR et de la manière dont sont utilisées les informations personnelles qu'ils traitent. Sans une telle prise de conscience, le droit d'accéder à ses propres données personnelles, tel que proposé dans le code, est vide de sens. Il est peu probable qu'un passager ait jamais demandé à un SIR d'accéder au fichier personnel le concernant, pour la simple raison que les passagers ne savent pas ce qui arrive à ces données et s'ils le savaient, il ne consentiraient pas à l'utilisation qui en est faite.*" [41] ;

[38] Avis du Contrôleur européen de la protection des données *sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives,* JO C 110, 1er mai 2008.

[39] Avis du Contrôleur européen de la protection des données *concernant le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel*, JO C 128, 6 juin 2009.

[40] Point 3.6.5 de l'avis précité.

[41] Point 4.6. de l'avis.

- un rapport public de décembre 2008[42] comportait différentes déclarations de la section vie privée du DHS qui pointent quelques problèmes graves quant au respect des demandes d'accès et de recours ("redress") concernant des données à caractère personnel, comme pourtant promis dans la lettre du DHS[43]. L'on a ainsi avoué que :
  1. il fallait généralement plus d'un an avant de répondre aux demandes d'accès aux données PNR[44], soit bien plus longtemps que ce qui est généralement prévu en vertu du Privacy Act américain et de la Directive 95/46/CE. Pour information, la LVP prévoit aux articles 10 et 12 des délais de réponse d'un mois et de 45 jours ;
  2. lorsque des individus exerçaient leur droit d'accès à l'égard de "toutes les données" conservées à leur sujet par le DHS (donc sans recherche ciblée), aucune de leurs données PNR n'était généralement communiquée en vertu du programme ATS spécifique[45] ;
  3. la majorité des demandeurs ne recevaient ainsi aucune donnée PNR alors que cela aurait dû être le cas (article IV des déclarations[46] et article 10 de la LVP) ;
  4. des données PNR ont été censurées de manière incohérente ou listées pour diffusion ;
  5. après un an, il y a une montagne de demandes non traitées ("large backlog"), en raison de sous-effectifs[47].

- contrairement à l'article 2 de l'Accord PNR 2007, on n'est pas passé au 1er janvier 2008 au système push plus respectueux de la vie privée. Le système "pull" est donc toujours en vigueur pour les données PNR (voir ci-après). Le système "push" est d'ailleurs reporté depuis le premier accord PNR de mai 2004, à la "grande préoccupation" du Groupe 29[48] ;

---

[42] Voir principalement la page 26 du rapport publié à l'adresse : http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf, et la critique y afférente à l'adresse : http://www.papersplease.org/wp/2008/12/24/dhs-admits-problems-in-disclosing-travel-surveillance-records/.

[43] Voir la rubrique IV. Droit d'accès et droit de regard, publiée au Sénat, 4-1432/1 – 2008/2009, 31. Il a ici été décidé d'étendre la protection en vertu du Privacy Act aux données PNR enregistrées dans le traitement ATS, quelle que soit la nationalité ou le pays d'établissement de la personne.

[44] Page 26 du rapport.

[45] Automated Targeting System. Il s'agit d'un programme commun du DHS et du CBP (Bureau of Customs and Border Protection).

[46] Qui mentionne "*En outre, les données PNR fournies par une personne ou en son nom sont communiquées à la dite personne conformément 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 »)*"

[47] Page 26 du rapport.

[48] WP 138, page 18, alinéa 3.

- dans la pratique, il est question d'intégration de données PNR et API au niveau mondial dans un nombre limité de systèmes SIR et dans le système "Shares". La majorité de ces banques de données se trouvent en dehors du territoire de l'Union européenne, bien que les données (notamment) de passagers transitent bien depuis l'Union européenne via par exemple des agences de voyages (voir ci-avant) ;
- le fait qu'il manque un traité mondial de protection de la vie privée et des données à caractère personnel ;
- le fait que l'on n'a pas encore pu réaliser une évaluation formelle de l'Accord PNR 2007 (comme prévu à l'article X des déclarations), et que l'Accord PNR 2007 reste vague à ce sujet (on n'a par exemple pas convenu d'un délai ou d'une suite en cas de non-évaluation)[49]. Ce, alors que la Belgique a précisément fait une déclaration officielle concernant l'importance qu'elle accorde à une telle évaluation[50]. Des sources européennes pointent notamment la modification dans l'administration américaine. Des sources officielles américaines[51] tiennent toutefois la Commission européenne pour responsable ;
- la large marge d'interprétation des différentes autorités impliquées concernant les traitements, comme le DHS ainsi que les États membres dans la transposition de la Directive API 2004/82/CE, en particulier en ce qui concerne les moyens, les points de contact pour transmettre des informations, les éléments de données requis et les critères pour déterminer quels vols sont soumis au contrôle et le fait que cette réglementation comprend aussi bien des vols intra et extra européens ;
- l'UE est de plus en plus sollicitée pour communiquer ses données PNR à des pays tiers (voir les accords avec le Canada[52] et l'Australie[53] et les demandes formelles d'entamer des négociations avec la Corée du Sud). Le niveau de protection adéquat doit être systématiquement évalué ;

---

[49] WP 138, page 15, alinéa 4. L'article X. de l'Accord PNR mentionne "réexamineront à intervalles réguliers".

[50] Voir la page 1 de l'Exposé des motifs : "*Elle souligne néanmoins l'importance qu'elle attache à une évaluation efficace et régulière de la mise en œuvre de cet accord, particulièrement en ce qui concerne les engagements américains relatifs à la protection des données privées qui sont décrits dans les Assurances. Elle demande que cet aspect soit inclus dans les modalités du processus de réexamen à déterminer entre l'UE et le DHS et que les États membres soient informés de ces modalités.*"

[51] Voir la réaction du DHS Chief Privacy Officer sur le site Internet du DHS : http://www.dhs.gov/journal/leadership/2008/12/what-passenger-name-record-report.html

[52] Décision 2006/230/CE du Conseil du 18 juillet 2005 *relative à la conclusion de l'accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données IPV/DP*, JO L 82, 21 mars 2006.

[53] Décision 2008/651/PESC/JAI du Conseil du 30 juin 2008 *relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) provenant de l'Union européenne par les transporteurs aériens au service des douanes australien*, JO L 213, 8 août 2008, page 49.

- l'impact du Traité de Lisbonne, qui engendre notamment un stand-still sur le schéma PNR européen. Le Traité de Lisbonne lèvera un certain nombre d'incertitudes juridiques quant à la séparation entre les piliers européens et garantira l'implication complète du Parlement européen ainsi que le contrôle juridique par la Cour de Justice.

III. EXAMEN GÉNÉRAL

---

1. Accessibilité et prévisibilité de la base légale (transparence au niveau de la norme)

Lors de l'examen général de l'Accord PNR 2007, la Commission souligne les exigences découlant de l'article 8 de la CEDH. L'article 8 de la CEDH est rédigé comme suit :

> "*1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
> *2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*"

Il ressort de l'interprétation de la Cour constitutionnelle[54], du Conseil d'État[55] ainsi que de la Cour européenne des Droits de l'Homme[56] que l'article 8 de la CEDH doit être interprété de manière telle que la base légale doive offrir suffisamment de prévisibilité pour pouvoir justifier les ingérences dans le droit au respect de la vie privée. L'on vérifie en particulier à cet égard si la loi offre "*des garanties contre les atteintes arbitraires de la puissance publique au droit au respect de la vie privée, à savoir en délimitant le* ***pouvoir d'appréciation*** *des autorités concernées avec une netteté suffisante, d'une part, et en prévoyant un* ***contrôle juridictionnel effectif****, d'autre part*[57]." L'exigence d'un contrôle juridique (effectif) a également été évoquée par le Parlement

---

[54] Voir rubrique B.6.2. de l'arrêt n° 151/2006 du 18 octobre 2006 *En cause : les recours en annulation de la loi du 3 mai 2005 modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, et de la loi du 3 mai 2005 modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité, introduits par l'ASBL Ligue des droits de l'homme*.

[55] Avis 37.748 et 37.749 du 23 novembre 2004 sur des avant-projets de loi "modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité" (37.748/AV) et "modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité" (37.749/AV), points 11 à 18 inclus, publiés à l'adresse suivante : http://www.dekamer.be/FLWB/PDF/51/1598/51K1598001.pdf.

[56] *CEDH, 26 mars 1987, Leander c. Suède, § 51.*

[57] Citation de l'arrêt précité de la Cour constitutionnelle, qui se réfère aussi notamment à "Cour européenne des Droits de l'Homme, 4 mai 2000, *Rotaru c.* Roumanie, § 55 ; 6 juin 2006, *Segerstedt-Wiberg c.* Suède, § 76 ; 4 juillet 2006, *Lupsa c.* Roumanie, § 34."

européen[58]. Dans les analyses du Groupe 29 et du Conseil d'État[59], il est stipulé que l'Accord PNR 2007 offre insuffisamment de garanties contre la mise en œuvre discrétionnaire au niveau du mécanisme d'évaluation[60] et les critères ou les normes (imprécis) pour une utilisation acceptable des données. Le mécanisme d'évaluation commune ne prévoit pas une implication suffisante d'autorités indépendantes de protection des données (parmi lesquelles donc également la Commission)[61]. Il subsiste encore des discussions sur la question de savoir quelles autorités de protection des données pourraient participer à une évaluation de l'Accord PNR 2007. Il ressort également de l'avis du Conseil d'État[62] que l'échange de données PNR européennes dans des cas d'urgence ne se fait pas tant sur la base de critères préétablis, mais plutôt sur la base de jugements "ad hoc" des autorités concernées. Il est enfin frappant de constater que les autorités américaines (DHS) se sont réservé le droit d'interpréter de manière unilatérale un certain nombre de dispositions de l'Accord PNR 2007[63].

2. Transparence au niveau de la finalité : manque de définition, de limitation d'utilisation et tendance de confusion de la finalité

Une des règles de base en matière de protection des données est que la finalité du traitement doit être formulée clairement. Cette exigence découle tant de l'article 4, § 1, 2° de la LVP et de l'article 22 de la Constitution que de l'article 8 de la CEDH et de l'article 5 b. de la Convention 108[64].

La finalité du traitement de données PNR est décrit à l'article I des déclarations comme le fait "*de prévenir et de combattre le terrorisme et les délits qui y sont liés ; (2) de prévenir et de combattre d'autres délits graves de nature transnationale, y compris la criminalité organisée ; et (3) d'empêcher que des personnes se soustraient aux mandats et aux mesures de détention provisoire émis à leur encontre concernant les infractions décrites ci-dessus. 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. Le DHS informera l'UE de l'adoption de toute législation américaine qui affecte matériellement les déclarations faites dans la présente lettre.*"

---

[58] Résolution "PNR/SWIFT" du Parlement européen sur SWIFT, l'Accord PNR et le dialogue transatlantique sur ces questions, P6_TA(2007)0039, JO C 287 E/349 du 29 novembre 2007, considérant D de l'en-tête.

[59] Avis n° 45.582/4 du 2 février 2009, Sénat, 4-1432/1 – 2008/2009, 42.

[60] WP 138, page 16, alinéa 2.

[61] WP 138, page 2.

[62] Page 42, Sénat, 4-1432/1.

[63] Ainsi, "*l'interprétation par les États-Unis de la notion de « cas d'urgence » pourra être examinée lors d'un examen périodique conformément à l'article 4 de l'Accord.*" (page 20 de l'Exposé des motifs). Voir également l'interprétation en vertu de l'article III *in fine* des déclarations relatives au délai de conservation réduit pour les données sensibles.

[64] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, approuvée par la loi du 17 juin 1991, M.B., 30 décembre 1993.

Le manque de définition et de limitation claires des finalités d'utilisation des divers traitements PNR a été critiqué par le Groupe 29[65] et par le Parlement européen[66].
L'Accord PNR 2007 ne comporte pas de définition des notions de "terrorisme" et "autres délits graves"[67]. Cet accord ne se limite clairement pas au traitement d'informations dans le contexte d'enquêtes judiciaires en cours (article III). Il s'agit manifestement aussi d'informations utilisées par diverses autorités de répression. L'on vise ainsi le traitement tant des informations d'identification que des données de profil.

Les limites de l'éventuelle utilisation permise (par exemple l'enrichissement de données) entre différents services judiciaires, administrations et services de renseignement ne sont pas définies précisément à l'article IX.

D'après le Comité économique et social européen, les prestataires de SIR violent systématiquement les règles en matière de protection des données d'un code de conduite existant s'ils utilisent les données qu'ils gèrent pour d'autres finalités que la réalisation de réservations. C'est le cas en vertu de l'Accord PNR 2007 lorsque des transporteurs aériens, des systèmes SIR, … sont obligés de communiquer des données PNR au DHS. La tendance de confusion de finalité entre le "core business" et la répression a été décrite de manière frappante par le CEPD[68] : "*Jusqu'à présent, l'on constatait une séparation claire entre les activités répressives et celles du secteur privé, les missions répressives étant effectuées par des services ad hoc, en particulier les forces de police, et le secteur privé étant sollicité au cas par cas pour communiquer des données à caractère personnel à ces services répressifs. On assiste aujourd'hui à une tendance visant à obliger les acteurs privés à coopérer systématiquement à des fins répressives* ".

Les éléments précités sont clairement problématiques à la lumière du principe de finalité.

---

[65] WP 138, page 8, alinéa 3.

[66] Voir pages 32 et suivantes des débats, 20 octobre 2008, publié à l'adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+CRE+20081020+SIT+DOC+PDF+V0//FR&language=FR. Le MEP déclare notamment ce qui suit à cet égard *"à lire les petits caractères de l'accord PNR UE-Australie – et cela vaut aussi pour l'accord PNR UE-US –, il s'agit non seulement de lutter contre le terrorisme et la criminalité, mais aussi de l'immigration, des risques pour la santé publique, d'objectifs administratifs, de douane, d'immigration, de surveillance et de responsabilité de l'administration publique. Cela n'a rien à voir avec la lutte contre le terrorisme*."

[67] Contrairement au projet de décision-cadre du Conseil.

[68] Voir à cet égard l'avis du CEPD du 20 décembre 2007 *sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives*, JO C 110, 1er mai 2008.

3. Principe de proportionnalité

3.1 Accroissement au lieu de *statu quo* du nombre de données enregistrées et susceptibles d'être communiquées

En vertu de l'article 4, § 1, 3° de la LVP, les données à caractère personnel doivent être "*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement*".

L'évolution du dossier PNR démontre toutefois que les transporteurs aériens se sont vus contraints, sous l'influence des diverses règles PNR, de collecter des données à caractère personnel qui ne sont normalement pas nécessaires à l'exploitation des systèmes de réservation classiques, mais qui servent plutôt au profilage de passagers. On peut ainsi affirmer de manière générale que de nombreuses données API ne servent aucune finalité commerciale spécifique pour les transporteurs aériens.

L'Exposé des motifs mentionne[69] clairement que par rapport à avant, les données traitées ne sont "*pas plus nombreuses, mais pas moins nombreuses non plus*". L'on insiste principalement sur l'évolution de 34 à 19 catégories de données.

Une telle présentation des choses est incorrecte et trompeuse. Il est déjà apparu au point 2.2. que ce sont précisément davantage de données qui sont traitées, et qu'il est même question à l'article III *in fine* des déclarations d'un mécanisme d'extension à l'initiative du DHS[70].

La Commission déplore qu'il soit question d'une telle extension, et que l'Exposé des motifs de l'article III donne une présentation incorrecte des choses à ce sujet.

3.2. Insistance accrue sur le profilage, y compris les données à caractère personnel sensibles et les données non limitées aux voyageurs effectifs

---

[69] Voir le commentaire de l'article III à la page 12 de l'Exposé des motifs : *"— les types de données PNR : dix-neuf catégories de données sont concernées, en d'autres termes quinze de moins par rapport à la version initiale et à l'accord provisoire. Il s'agit en premier lieu d'une opération de rationalisation du fait que les trente-quatre catégories de départ contenaient des informations faisant double emploi (par exemple « travel agent » et « travel agency » faisaient l'objet de rubriques séparées ; par ailleurs, une dizaine de données sont maintenant regroupées sous « frequent flyer »). En fait, les données demandées ne sont pas plus nombreuses, mais pas moins nombreuses non plus."*

[70] Voir la disposition "*Si cela est nécessaire dans un cas exceptionnel où la vie de la personne concernée ou d'autres personnes pourrait être mise en danger ou subir une atteinte grave, les fonctionnaires du DHS peuvent demander et utiliser des informations figurant dans les données PNR de l'UE autres que celles énumérées ci-dessus, y compris des données sensibles.*"

La nature des données traitées en vertu de l'Accord PNR 2007 dépasse ce qui est strictement nécessaire pour identifier des passagers ou pour assurer le service commercial (voir ci-avant). L'accent est aussi clairement mis sur les informations relatives au profil au lieu de l'identification des passagers. Un certain nombre de données API[71] ne peuvent être déduites d'un examen de tickets d'avion ou de documents de voyage traditionnels en vertu de compétences normales en matière de contrôle frontalier, bien que le DHS a précisément mentionné à l'article III des déclarations que la majorité des données pouvaient être déduites de ces documents[72]. Par ailleurs, dans les données API, il n'y a pas que des données de passagers/voyageurs qui sont traitées (voir ci-avant). Des données sensibles[73] au sens des articles 6 et 7 de la LVP sont également traitées.

Tant le Congrès américain que le Parlement européen[74] ont déjà exprimé leur préoccupation quant à cette tendance croissante de profilage et de "data mining".

3.3. Délai de conservation de données fortement accru et conséquences y afférentes

De manière plus générale, on doit constater qu'au cours de ces dernières années, il est de plus en plus question d'un glissement de paradigme lorsque l'obligation de minimalisation de données[75] doit être appliquée pour la lutte contre la criminalité. L'accent mis sur une conservation de données plus longue s'avère être le plus extrême en vertu de l'Accord PNR 2007, surtout si on le compare avec les délais de conservation en vertu de la Directive 2006/24/CE sur la conservation et la troisième directive sur le blanchiment[76]. On peut bien entendu argumenter que pour la lutte contre des formes graves de criminalité, un délai de conservation plus long est nécessaire en comparaison avec des délais de conservation pour d'autres traitements privés ou des traitements en vue de lutter contre des délits moins graves, et que les enquêtes judiciaires en cours doivent être préservées. La Commission remarque quand même qu'il est question d'éléments qui indiquent une augmentation

---

[71] Par exemple : adresse de facturation, autres noms dans le PNR, informations sur le voyageur fréquent, adresse e-mail, informations sur le profil (OSI/SSI/SSR), identité de la personne qui a demandé des informations (qui n'est pas nécessairement le voyageur).

[72] Sénat, 4-1432/1, page 29 *in fine*.

[73] Par exemple : préférences personnelles dont on peut déduire la religion (par exemple, demande d'un repas casher). Dans les données PNR de voyageurs d'affaires, des codes sont également souvent repris pour mentionner l'appartenance syndicale ou pour indiquer quel département ou client paie le voyage.

[74] Résolution "PNR/SWIFT" du Parlement européen (voir supra), point 4.

[75] Le traitement de données à caractère personnel doit se limiter en principe aux données à caractère personnel qui sont "*adéquates, pertinentes et non excessives*" (article 4, § 1, 3° de la LVP). En outre, les données à caractère personnel ne peuvent être conservées pour une durée excédant celle nécessaire, "*sous une forme permettant l'identification des personnes concernées*" (article 4, § 1, 5° de la LVP).

[76] Directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 *relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme*, JO, 25 novembre 2005.

manifeste lors de l'établissement d'obligations de conservation de données et/ou un éventuel manque de politique européenne uniforme et équilibrée au travers des différents instruments juridiques.

L'Accord PNR 2007 prévoit un délai de conservation de données de 15 ans (7 ans dans une "base de données active" et 8 ans dans un "mode veille")[77]. Certes, une exception est prévue pour le traitement de données sensibles. En vertu de l'article III des déclarations, les données à caractère personnel sensibles sont effacées par le DHS soit immédiatement, soit dans les 30 jours[78]. Ces 30 jours ne sont toutefois appliqués que "*après que les fins pour lesquelles les données ont été consultées ont été atteintes et si leur conservation n'est pas exigée par la loi.*"

La Commission fait remarquer qu'il est question, dans l'Exposé des motifs, d'un délai de conservation de 7 jours[79] (au lieu de 7 ans). Il s'agit clairement d'une erreur qui doit être corrigée.

Toutefois, le délai de base est le double de celui de l'accord précédent (pour la base de données active). Ce délai est au moins trois fois supérieur par rapport aux autres instruments juridiques européens qui ont été adoptés ces dernières années en vue de la lutte contre le terrorisme et/ou la criminalité grave. Voir la troisième directive blanchiment[80] qui prévoit un délai de conservation de 5 ans, et la directive sur la conservation de données[81] qui prévoit un délai de conservation de données de télécommunications pour "*une durée minimale de six mois et maximale de deux ans à compter de la date de la communication*". On ne sait pas clairement pourquoi les données de passagers (et d'autres personnes) nécessitent un délai de conservation bien plus long que les données de télécommunications et les données relatives à des transactions financières (suspectes) ainsi que les données de clients et bénéficiaires de produits financiers et d'assurances.

Si des données sont stockées massivement, le risque de profilage des personnes concernées augmente, tout comme le risque de détournement de finalité ("function creep"), c'est-à-dire le détournement potentiel de l'utilisation de données pour d'autres infractions pour lesquelles il n'y

---

[77] Article VII des déclarations.

[78] "*Si cela est nécessaire dans un cas exceptionnel où la vie de la personne concernée ou d'autres personnes pourrait être mise en danger ou subir une atteinte grave* ".

[79] Page 14 de l'Exposé des motifs concernant l'article VII.

[80] Article 30 de la Directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 *relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme*, JO, 25 novembre 2005. Après consultation du contrôleur financier belge, il apparaît que ce délai soit interprété comme un délai maximal.

[81] Article 6 de la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 *sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*, JO, 13 avril 2006.

avait pas initialement d'accord (politique) d'échange de données. L'article II des déclarations comporte certes une limite d'utilisation des données, associée à un certain nombre de finalités générales[82]. Il convient bien entendu de veiller de manière stricte à l'application correcte de ce principe. Vu l'évolution dans d'autres dossiers (mise en œuvre de la directive précitée sur la conservation de données), il subsiste toutefois encore la préoccupation quant à la demande d'utiliser également les données obtenues pour le traitement de litiges civils comme des litiges relatifs à la relation de travail entre employé et employeur, aux divorces, etc.

3.4. Manque de mise en œuvre d'un mécanisme "pull"

Tant le Groupe 29 que le CEPD[83] ont toujours défendu, dans l'affaire PNR et plus récemment dans le programme TFTP de l'UST (département américain du Trésor), la nécessité (d'une forme proportionnelle de) système "push" au lieu de "pull" dans les relations à l'égard des autorités et compagnies aériennes américaines et européennes.

Jusqu'à présent, aucun mécanisme push fonctionnel et proportionnel n'a toutefois encore été fourni. Les États-Unis peuvent donc encore extraire des données à caractère personnel, de sorte qu'il s'agit en réalité d'un système "pull" disproportionné concernant les données des systèmes SIR des transporteurs aériens. Les accords à cet égard dans la convention n° 2 de l'Accord PNR 2007 restent donc lettre morte.

3.5. Destinataires des données

L'interprétation courante de l'article 22 de la Constitution par le Conseil d'État[84] requiert que l'identité des destinataires/utilisateurs des données soit définie par le législateur.

La limitation initiale (sur papier) du premier accord PNR selon laquelle les données PNR ne peuvent être consultées que par les services douaniers est clairement abandonnée. En outre, les utilisateurs potentiels (aux États-Unis ou ailleurs) des données s'avèrent être décrits de manière très générale à

---

[82] "*uniquement aux autres autorités gouvernementales américaines chargées du maintien de l'ordre, de la sécurité publique ou de la lutte contre le terrorisme, pour servir dans le cadre des affaires relatives à la lutte contre le terrorisme, à la criminalité transnationale et à la sécurité publique (y compris lorsqu'il s'agit de menaces, de vols aériens, de personnes ou de lignes aériennes suscitant des préoccupations) qu'elles examinent ou analysent, conformément à la loi et en application des engagements écrits et de la législation américaine sur l'échange d'informations entre les autorités gouvernementales des États-Unis.*"

[83] Voir le § 98 de l'avis du CEPD *sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives*, JO, 1er mai 2008.

[84] Voir notamment l'avis 27.289/4 du 27 février 1998, l'avis 29.125 du 14 avril 1999, page 7 de l'avis 34.270/1 du 23 janvier 2003, l'avis 37.765 du 4 novembre 2004, l'avis 27.289 du 25 février 1998 et l'avis 45.070 du 27 août 2008.

l'article II des déclarations, comme les "*autres autorités gouvernementales*" et "*autres autorités gouvernementales de pays tiers*". Cette description comporte aussi bien les autorités policières que judiciaires ainsi que les services qui assurent la sécurité publique. Il aurait été recommandé et plus clair de disposer d'une liste exhaustive des services publics pertinents.

4. Primauté *de facto* des décisions administratives américaines lors de l'application desdites "watch lists" et "no fly lists" – pas d'accès au juge

Il apparaît entre-temps que l'exécution de l'Accord PNR 2007 implique l'application de listes noires américaines aux ressortissants européens. Bien que le Groupe 29 ait déjà demandé des précisions à ce sujet en 2003[85], il devient de plus en plus manifeste que l'administration américaine peut déterminer arbitrairement qui peut prendre l'avion et qui peut se déplacer, vu la décision administrative de placer des personnes sur une "watch list" ou une "no fly list". Quelques incidents se sont déjà produits à cet égard, lesquels ont été rapportés dans les médias belges[86]. Par ailleurs, les États-Unis obligent les transporteurs aériens à vérifier l'identité des passagers sur la base de ces listes noires et grises. La promesse de mettre fin à cette obligation dans le chef du secteur privé n'est pas encore retirée.

Le droit d'accès (rapide et simple) à une instance judiciaire européenne indépendante ou à un contrôleur indépendant[87] au sujet des listes noires précitées n'est pas prévu ou réglé explicitement dans l'Accord PNR 2007. Cette pratique doit être jugée à la lumière de la récente affaire Kadi et Barakaat devant la Cour de Justice[88] concernant les listes de terroristes. Le respect des droits humains est, d'après la Cour, une exigence de légitimité de mesures communautaires. Les obligations imposées par un accord international ne peuvent donc pas porter préjudice aux principes constitutionnels du Traité C.E., qui doivent être contrôlés par la Cour dans le cadre de l'ensemble du système de moyens juridiques que le Traité a créés. En l'occurrence, la Cour a jugé que les droits de la défense, en particulier le droit d'être entendu et le droit à un contrôle judiciaire effectif, n'avaient pas été respectés.

---

[85] WP 78, point 6 (page 7).

[86] Les incidents concernaient entre autres un journaliste colombien et un Belge ayant un profil politique actif. Il n'y avait aucune indication selon laquelle une des deux personnes était mentionnée sur une liste officielle de terroristes. Il s'agissait de vols qui ne devaient pas atterrir aux États-Unis, mais qui ne faisaient que pénétrer l'espace aérien des États-Unis (Paris-Mexico, vol d'Air France). Voir DESPIC-POPOVIC, H., Journaliste fiché, avion dérouté, La Libre, 25 avril 2009. Voir également les communiqués de presse de début septembre 2009 concernant le vol du 19 août 2009 sur le vol AF438. Il y avait à bord un Belge qui figurait sur la "*no fly list*" des services de sécurité américains. Dans le plan de vol de l'AF438, il n'était nulle part question d'un atterrissage sur le sol américain.

[87] Indépendamment de mécanismes de respect en vertu du droit américain repris à l'article V.

[88] CJE 3 septembre 2008 dans les affaires conjointe s C-402/05 P et C-415/05 P, *Yassin Abdullah Kadi et Al Barakaat International Foundation c. Conseil et Commission,* points 348-394.

5. Responsable du traitement

Depuis 1996, il existe quelques précédents où tant la Commission[89] que la Commission vie privée française[90] ont défendu que pour les systèmes SIR, la responsabilité (commune) est d'application (article 1, § 4 de la LVP). Les agences de voyages, les transporteurs aériens, les entreprises (ayant des systèmes de réservation propres), les systèmes SIR présents dans l'Union européenne comme Amadeus et les autorités locales peuvent par conséquent être tenus (co)responsables des traitements PNR dans la mesure où ils déterminent les finalités et les moyens des traitements. La Commission adhère également au point de vue du Comité économique et social européen selon lequel "*la responsabilité des SIR en matière de contrôle des données doit être reconnue formellement, non seulement pour les données relatives au transport aérien et ferroviaire mais également pour celles concernant les hôtels, voitures, ferrys, contrats d'assurance et autres enregistrées dans leurs systèmes.*"[91] Certes, elle souligne le fait que cette appréciation implique toujours une analyse préalable des faits, et qu'il faudrait donc d'abord démontrer de manière suffisante si et dans quelle mesure ces prestataires de SIR déterminent également la finalité et les moyens du traitement.

6. Possibilités de recours restreintes, contrôle indépendant restreint et évaluation en attente

À cet égard, il est apparu qu'une des questions les plus importantes en suspens est celle des possibilités de recours, qui ne sont pas encore prévues en vertu du droit européen, à l'encontre de décisions administratives "no fly" du DHS. Cela doit être apprécié à la lumière de l'affaire Kadi et Barakaat précitée devant la Cour de Justice et de la critique susmentionnée du Parlement européen[92].

L'évaluation en attente de l'Accord PNR 2007 est également une question en suspens.
Un aspect important de cette évaluation devrait être un examen plus approfondi des résultats effectifs atteints dans le domaine de la lutte contre le terrorisme et de la lutte contre la grande criminalité au moyen des données PNR. À ce sujet, les points de vue les plus divergents ont déjà été

[89] Voir conclusions III.1 de la recommandation n° 01/98 de la Commission concernant le "Système informatisé de réservation" du 14 décembre 1998.

[90] Explication de la Commission vie privée française (CNIL) le 11 septembre 1996, à l'occasion de la 18e conférence internationale sur la protection de la vie privée et des données à caractère personnel.

[91] Voir la recommandation 1.10 de l'avis précité.

[92] Résolution "PNR/SWIFT" du Parlement européen sur SWIFT, l'Accord PNR et le dialogue transatlantique sur ces questions, P6_TA(2007)0039, JO C 287 E/349 du 29 novembre 2007, considérant D de l'en-tête.

formulés. D'après certaines sources, principalement d'origine anglo-saxonnes[93], le traitement de données PNR est nécessaire et ce traitement a déjà permis de trouver des solutions dans quelques cas concrets. D'autres sources semblent le contester. Ainsi, une institution américaine[94] a conclu que le data mining n'était pas approprié pour découvrir des terroristes et un responsable en matière de vie privée d'un transporteur aérien néerlandais a déclaré ce qui suit[95] : *"Quoi qu'il en soit, aucune personne n'a encore jamais été arrêtée jusqu'à présent sur la base de simples données PNR"* [Traduction libre réalisée par le secrétariat de la Commission en l'absence de traduction officielle]. Tant qu'il n'y a pas de données suffisamment objectives et fiables sur la base desquelles les décideurs peuvent prendre une décision sur une base objective, il est approprié de faire preuve de la prudence nécessaire et d'insister pour qu'une évaluation approfondie et indépendante de la nécessité des transferts de données soit effectuée.

La Commission estime qu'une évaluation de l'Accord PNR 2007 s'impose, et que tant le Parlement européen que les autorités indépendantes de protection des données qui existent doivent être associés au maximum au processus d'évaluation. Il en va de même pour les futures renégociations du nouvel accord PNR d'ici (au plus tard) 2014 et ensuite pour l'exécution de cet accord.

PAR CES MOTIFS,

Vu les risques flagrants pour les droits et libertés (notamment) des passagers concernés et le principe de prudence, la Commission estime que dans ce dossier, les principes de contrôle préalable et de contrôle indépendant au sens des articles 20 et 28 de la Directive 95/46/CE (tels qu'exécutés par les articles 17*bis* et 29 de la LVP) doivent pouvoir être entièrement appliqués lors de l'exécution ou de la révision de l'Accord PNR 2007.

La Commission constate que :

- son avis est demandé plus de deux ans après la fin de la négociation de l'Accord PNR 2007 ;

---

[93] Voir notamment les déclarations de M. Michael Chertoff pour le Comité LIBE du Parlement européen du 14 mai 2007, LIBE(2007)0514_1, publiées à l'adresse suivante : http://www.dhs.gov/xnews/speeches/sp_1180627041914.shtm.

[94] Institution CATO ; JONES, J. et HARPER, J., "Effective counterterrorism and the limited Role of Predicative Data Mining", Analysis n° 584, 11 décembre 1996. Cette étude est publiée sur le site www.cato.org et a également été évoquée dans la doctrine néerlandaise (article Kuipers, F., Passagiersgegevens en terrorisme. Toegang tot reserveringsinformatie als wondermiddel om terroristen te weren, International Spectator, juin 2008, page 340).

[95] KUIPERS, F., l.c., page 341.

- lors de l'adoption de l'arrêté du Conseil le 23 juillet 2007, la Belgique a effectué une déclaration officielle selon laquelle elle accepte l'application provisoire de l'accord[96] ;
- l'accord est par conséquent déjà en vigueur depuis plus de deux ans.

La Commission souligne en outre le caractère temporaire de l'Accord PNR 2007, qui a été limité à 7 ans (2007-2014).

La Commission décide par conséquent de ne formuler aucun jugement quant au présent 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 à caractère personnel des passagers (données PNR) par les transporteurs aériens au Ministère américain de la sécurité intérieure.

La Commission souligne qu'il faudra tenir compte du fait qu'en matière de transfert de données PNR, tant au niveau européen qu'avec des pays tiers, des négociations plus approfondies seront encore tenues quant au renouvellement ou à la conclusion de tels accords, et/ou à la modification de l'actuel cadre réglementaire européen.

À la lumière des analyses de l'Accord PNR 2007 et de l'expérience de ces deux dernières années, la Commission souhaite attirer l'attention sur les points suivants qui constituent une part essentielle de la protection de la vie privée et qui ne sont pas suffisamment pris en compte dans le présent accord :

- le manque de clarté au niveau :
  - du manque de limitation dans la définition des finalités d'utilisation ;
  - de la détermination des destinataires de données ;
  - du règlement du mécanisme d'évaluation et de l'accès à une instance judiciaire européenne indépendante ;
- le manque de contrôle indépendant ;
- le manque d'évaluation de l'Accord PNR 2007;
- les différentes violations du principe de proportionnalité, parmi lesquelles le nombre accru de données susceptibles d'être communiquées, les délais de conservation des données fortement allongés et le mécanisme push qui n'est pas mis en œuvre.

---

[96] Voir page 1 de l'Exposé des motifs : *"Elle souligne néanmoins l'importance qu'elle attache à une évaluation efficace et régulière de la mise en œuvre de cet accord, particulièrement en ce qui concerne les engagements américains relatifs à la protection des données privées qui sont décrits dans les Assurances. Elle demande que cet aspect soit inclus dans les modalités du processus de réexamen à déterminer entre l'UE et le DHS et que les États membres soient informés de ces modalités."*

À cet égard, la Commission de la protection de la vie privée se réserve le droit de procéder à d'autres évaluations dans ce dossier, lorsqu'elle l'estimera nécessaire. Elle souhaite que son avis soit demandé au sujet de toute modification réglementaire, évaluation et/ou disposition nationale d'exécution de l'Accord PNR. Elle reste à disposition pour une éventuelle concertation ultérieure.

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere