



10019/04/FR
GT 87

**Avis 2/2004 sur le niveau de protection adéquat des données à caractère personnel
contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des
douanes et de la protection des frontières des États-Unis (US CBP)**

Adopté le 29 janvier 2004

Le présent groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et l'article 14 de la directive 97/66/CE.

Le secrétariat est assuré par la Commission européenne, DG Marché intérieur, Direction E (Services, Droit d'auteur, Propriété Industrielle et Protection des Données), Rue de la Loi 200, Bureau C100-6/136, B-1049 Bruxelles, Belgique.

Adresse Internet: www.europa.eu.int/comm/privacy

Avis 2/2004 sur la protection appropriée des données personnelles «PNR» des passagers aériens destinées à être transférées au *Bureau of Customs and Border Protection* (US CPB)

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995¹,

vu l'article 29 et l'article 30, paragraphe 1, point a), et paragraphe 3, de ladite directive,

vu ses règles de procédure, et notamment leurs articles 12 et 14,

a adopté le présent avis:

INTRODUCTION

Dans la foulée des événements du 11 septembre 2001, les États-Unis ont adopté un ensemble de lois et de règlements imposant aux compagnies aériennes opérant des vols à destination de leur territoire de transférer aux autorités américaines des données personnelles sur les passagers et les membres d'équipage des vols à destination ou en provenance de ce pays. En particulier, les autorités ont imposé aux compagnies aériennes l'obligation de fournir au bureau américain des douanes et de la protection des frontières (CPB) un accès électronique aux données des passagers figurant dans les fichiers «PNR» pour les vols à destination, en provenance et via les États-Unis. Les compagnies aériennes qui rejettent ces demandes sont susceptibles d'être sanctionnées par de lourdes amendes et même par la perte de leurs droits d'atterrissage, et leurs passagers subiraient des retards à leur arrivée aux États-Unis.

Le groupe de travail a émis un premier avis en octobre 2002 et un deuxième le 13 juin 2003. Ce dernier prenait en considération la déclaration d'engagement des États-Unis du 22 mai 2003 («*Undertakings of the United States Bureau of Customs and Border Protection et the United States Transportation Security Administration*») reflétant le dernier stade du dialogue relatif aux engagements de la partie américaine sur les conditions de traitement des données passagers PNR.

Dans son avis du 13 juin, le groupe de travail a attiré l'attention sur plusieurs questions de protection des données résultant du transfert des données passagers PNR aux autorités américaines. Les principaux points en suspens concernent la finalité des transferts, le principe de proportionnalité en ce qui concerne les données personnelles à transférer ainsi que le moment des transferts et la durée de conservation des données, le traitement des données sensibles, l'importance d'adopter une méthode de transfert «push», le contrôle strict des transferts ultérieurs vers d'autres administrations ou autorités

¹ Journal officiel n° L 281 du 23.11.1995, p. 31, disponible à l'adresse suivante:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

étrangères, les garanties et les droits des personnes concernées, le mécanisme d'application et de règlement des litiges ainsi que le niveau des engagements.

Plus récemment, le groupe de travail a reçu la communication de la Commission au Conseil et au Parlement intitulée «Transfert des données des dossiers passagers (Passenger Name Record - PNR): une démarche globale de l'Union européenne»² et une version actualisée de la déclaration d'engagement américaine datée du 12 janvier 2004 (annexe I).

Conformément à son avis 4/2003, le groupe de travail estime qu'il convient d'émettre un nouvel avis à la lumière des derniers développements concernant le transfert de données passagers PNR, en tenant compte en particulier des résultats des négociations entre la Commission européenne et les autorités américaines.

1. ACTION CONTRE LE TERRORISME ET PROTECTION DES LIBERTES ET DES DROITS FONDAMENTAUX

Comme cela est déjà indiqué dans les avis 6/2002 et 4/2003, les transferts de données à des autorités américaines suscitent des préoccupations publiques, ont des répercussions profondes et sensibles au plan politique et institutionnel et revêtent une dimension internationale.

La lutte contre le terrorisme est un élément à la fois utile et nécessaire dans les sociétés démocratiques. Dans ce combat contre le terrorisme, il convient de protéger les libertés individuelles et des droits fondamentaux, y compris le respect de la vie privée et la protection des données.

Ces droits sont notamment protégés par la directive 95/46/CE ainsi que par l'article 8 de la convention européenne des droits de l'homme et sont ancrés dans les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. La protection des données est en outre reconnue et renforcée par le projet de constitution européenne discuté par la Convention sur l'avenir de l'Europe.

Aussi les libertés et les droits fondamentaux relatifs aux principes régissant la protection des données à caractère personnel dans l'Union européenne ne doivent-ils être restreints que dans les cas où cela est nécessaire au sein d'une société démocratique ou pour les besoins de la protection des intérêts publics tels qu'ils sont définis exhaustivement dans les instruments susmentionnés.

Compte tenu du volume et de la sensibilité des données concernées ainsi que du nombre d'individus touchés (10 à 11 millions de passagers par an), la demande de communication à une autorité publique de données personnelles collectées à des fins commerciales et figurant dans les bases de données des compagnies aériennes proposant des vols à destination des États-Unis ou transitant par les États-Unis, ainsi que dans les systèmes de réservation connexes, en lui fournissant un accès à ces systèmes, est sans précédent dans l'histoire des relations entre les États-Unis et l'Europe et constitue une exception au principe fondamental de spécification de la finalité en matière de protection des données.

² COM(2003)826 final

Il y a donc lieu de faire preuve de prudence tout en tenant compte également des possibilités d'extraction de données auxquelles cette évolution ouvre la voie, en particulier pour les résidents européens, ainsi que du risque qui en découle en matière de surveillance généralisée et de contrôle par un pays tiers.

De plus, des flux similaires de données des compagnies aériennes ont déjà été demandés et/ou proposés par plusieurs autres pays tiers, ce qui soulève la question de l'égalité de traitement des pays tiers et met en évidence la nécessité d'adopter une approche globale pour l'utilisation des données des transports aériens à des fins de sécurité dans un contexte multilatéral.

Il n'est pas certain que la lutte contre le terrorisme et le maintien de la sécurité intérieure seront plus efficaces en mettant partiellement entre parenthèses les principes de proportionnalité et de minimisation des données, alors que le respect de ces principes constitue une garantie essentielle pour la protection des droits des citoyens et convient davantage aux besoins du développement commercial.

À cet égard, le groupe de travail note que la question du transfert de données passagers PNR se pose également à d'autres pays, ce qui exige une approche globale et uniforme à l'échelle mondiale, c'est-à-dire une harmonisation des solutions envisagées pour différents pays.

Le groupe de travail observe par ailleurs que l'expérience récente acquise par certains pays, et notamment l'Australie, montre que l'on peut apporter une réponse proportionnelle et raisonnable aux exigences légitimes de la sécurité intérieure et de la lutte contre le terrorisme en utilisant des systèmes qui sont compatibles avec les principes fondamentaux du respect de la vie privée et de la protection des données à caractère personnel.

2. ACTES LEGISLATIFS A ADOPTER

Le groupe de travail déduit de la communication que la Commission considère que la définition d'une base juridique de qualité pour le transfert de données «PNR» aux autorités américaines doit passer par une décision de la Commission basée sur l'article 25, paragraphe 6, de la directive 95/46/CE en liaison avec un accord international autorisant les compagnies aériennes à traiter les exigences américaines comme des exigences juridiques au sein de l'UE et enjoignant les États-Unis à la réciprocité et au respect des droits des résidents de l'UE («due process»). Pour ce faire, la Commission envisage de passer un «accord bilatéral allégé» avec les États-Unis.

Compte tenu de l'absence de documents pertinents et des compétences des États membres en ce qui concerne la mise en œuvre des articles 6 et 7 de la directive 95/46/CE, le groupe de travail n'est pas en mesure d'adopter un avis sur le contenu ainsi que sur la base et la valeur juridiques éventuelles d'un tel accord.

Le groupe de travail souhaiterait souligner, toutefois, que les décisions de la Commission, prises sur la base de l'article 25, paragraphe 6, de la Directive, font référence, de par leur nature, à la protection appropriée des données personnelles un fois que celles-ci ont été transférées à un pays tiers, et que, jusqu'à présent, elles ont visé les transferts à des organismes du secteur privé situés dans des pays tiers. Il s'agit là de la première fois qu'un transfert est opéré en raison d'une obligation légale issue d'un pays

tiers qui requiert que des sous-traitants opérant à partir de l'Union européenne transfèrent des données à une autorité publique de ce pays tiers, en non-conformité avec les provisions de la Directive.

Afin de garantir une base légale certaine à ces transferts, une formule composée d'une décision sur le caractère adéquat de la protection et d'un accord international est envisagée ; celle-ci devra avoir un certain nombre d'effets juridiques. Le groupe de travail considère que, dans la mesure où l'accord international permet de légitimer une limitation au droit à la vie privée ou une restriction au principe de limitation de la finalité prévu à l'article 6 de la Directive, ledit accord devra en tout état de cause respecter les limites posées par l'article 8 de la Convention européenne des droits de l'Homme et l'article 13 de la Directive.

3. CHAMP D'APPLICATION DU PRINCIPE DE PROTECTION ADEQUATE ET D'UN EVENTUEL ACCORD: LE SYSTEME CAPPS II ET LA TSA

Le groupe de travail a expressément exclu le programme CAPPS II et tout autre système capable de réaliser des opérations de traitement de données à grande échelle du champ d'application de son avis 4/2003.

En fait, ces systèmes présentent des différences qualitatives par rapport au simple transfert de données passagers PNR et soulèvent des questions graves qui doivent être clarifiées et de traitées spécifiquement par le groupe de travail, compte tenu des effets généralisés qu'ils auraient sur les droits fondamentaux des personnes concernées.

Le système CAPPS II soulève notamment un certain nombre de questions spécifiques qui appellent non seulement l'attention particulière du groupe de travail, mais aussi des clauses de sauvegarde plus importantes. Toute décision future sur le système CAPPS II devra être spécifiquement étudiée par le groupe de travail et ne devra pas découler d'une extension automatique du champ d'application de la première décision de la Commission sur le niveau de protection adéquat des transferts de données passagers PNR vers les États-Unis.

Par conséquent, étant donné que le groupe de travail n'a été ni informé ni consulté à propos du cadre juridique définitif du système CAPPS II, tout usage de données à caractère personnel par la TSA dans le cadre du système CAPPS II tel qu'il est proposé et tout essai y afférent doit être exclu au présent comme l'avenir du champ d'application de la décision de la Commission. En d'autres termes, les réflexions émises dans le présent avis reposent sur la supposition selon laquelle la décision de la Commission ne sera pas étendue à l'avenir au système CAPPS II, ni directement, ni indirectement par référence à la législation interne des États-Unis. Dans le cas contraire, il y aurait lieu d'émettre dès à présent des observations beaucoup plus critiques.

De ce fait, le groupe de travail recommande à la Commission de préciser, par une clause spécifique de la décision, que les autorités américaines doivent s'abstenir d'utiliser les données passagers PNR transmises par l'UE non seulement pour mettre en œuvre le système CAPPS II, mais aussi pour l'essayer.

Le groupe de travail est d'avis qu'une telle clause devra également s'appliquer à tout autre usage des données sur les passagers européens transmises par les compagnies aériennes

dans le cadre d'autres programmes tels que les dispositifs «Terrorism Information Awareness» et «US VISIT» ou les programmes de traitement de données biométriques.

4. NIVEAU DES ENGAGEMENTS

Le groupe de travail rappelle que toute décision de la Commission ne devra pas reposer sur de simples « engagements » de la part d'autorités administratives, mais sur des engagements qui sont officiellement publiés au niveau du registre fédéral au moins et ayant force exécutoire aux Etats-Unis. Plus particulièrement, il ne devra pas y avoir de doute quant à l'effet créateur de droits au profit de tierces personnes.

Sur ce point, il est clair que les engagements pris par les Etats-Unis n'auront pas de force exécutoire du côté des Etats-Unis. En outre, le nouveau paragraphe 47 ajouté à la fin des engagements clarifie de manière explicite la force exécutoire des engagements pris par les Etats-Unis, en disposant qu'ils « ne sont pas créateurs de droits ou d'avantages au bénéfice de personnes ou de parties, quelles soient privées ou publiques ».

Le groupe de travail souligne ainsi que le niveau des engagements du côté des Etats-Unis ne peut pas être considéré comme conforme aux exigences posées dans son avis 4/2003 et considère que cette question est une condition essentielle et devra être adressée avant qu'un accord puisse être formalisé.

5. ASPECTS SPECIFIQUES

Compte tenu du contexte global décrit ci-dessus, les demandes américaines telle qu'elles ressortent de la déclaration d'engagement (version mise à jour du 12 janvier 2004) doivent être évaluées à la lumière des avis émis dans ce domaine par le groupe de travail, en particulier l'avis 4/2003 du 13 juin 2003.

A. NATURE TRANSITOIRE DU NIVEAU DE PROTECTION ADEQUAT

Une durée de trois ans et demi a été suggérée pour l'ensemble des mesures, y compris la déclaration d'engagement, le constat de protection adéquate et l'accord international correspondant.

Le groupe de travail accueille favorablement l'introduction d'une clause de caducité dans l'accord et espère que les trois ans et demi proposés dans son avis 4/2003 seront pris en considération.

B. LIMITATION DE FINALITE

Le DHS (ministère américain de la sécurité intérieure) utilisera les données passagers PNR pour les besoins de la CBP, le but étant de prévenir et de combattre:

- 1) le terrorisme et les crimes liés au terrorisme;
- 2) d'autres crimes graves, y compris les crimes organisés qui, par nature, revêtent un caractère transnational;

- 3) la fuite d'individus faisant l'objet d'un mandat d'arrêt ou placé en détention pour l'un des crimes visés ci-dessus.

Le groupe de travail note que l'on a donné une description plus ciblée et plus précise de la finalité de l'usage des données «PNR». Toutefois, la catégorie 2 demeure vague, notamment en ce qui concerne le champ d'application des «autres crimes graves» visés dans la déclaration américaine. De plus, la finalité des mesures reste beaucoup plus vaste que la lutte contre les actes de terrorisme sur laquelle le groupe de travail juge qu'il faut mettre l'accent (avis 4/2003).

C. LISTE DES DONNEES A TRANSFERER

Le CPB propose désormais que les transferts de données passagers PNR incluent une liste de 34 éléments informatifs, ce que la Commission a approuvé. Cette liste résulte de l'exclusion de quatre champs de données (identification des billets gratuits, nombre de bagages, nombre de bagages pour chaque segment, surclassements volontaires/involontaires) de la liste des 38 éléments «PNR» figurant à l'annexe B de la déclaration d'engagements du 22 mai 2003³.

Le groupe de travail observe que les progrès réalisés en ce qui concerne la liste des données à transmettre sont très minces. En effet, la liste américaine révisée contient toujours les 20 éléments dont le groupe de travail juge le transfert disproportionné et problématique dans son avis 4/2003.

Il convient en outre de noter que les autorités américaines n'ont fait passer le nombre d'éléments à transmettre de 38 à 34 qu'en supprimant quatre éléments qui avaient été acceptés par le groupe de travail dans son avis du 13 juin. Pour ce qui est des 20 éléments qui continuent d'être demandés par les autorités américaines même s'ils n'ont pas été acceptés par le groupe de travail, aucune indication ou explication n'a été fournie pour justifier la nécessité de leur traitement ou leur caractère proportionnel et non excessif dans la lutte d'une société démocratique contre le terrorisme.

Le groupe de travail rappelle la liste des 19 éléments acceptés dans son avis du 13 juin 2003, tout ajout à cette liste étant soumis à une vérification stricte des principes de proportionnalité et de minimisation de données.

D. DONNEES SENSIBLES

Le dialogue a notamment permis de faire en sorte que certaines données «PNR» ne seront pas utilisées, mais supprimées par les autorités américaines, sachant à cet égard que l'article 8, paragraphe 1, de la directive renvoie aux «données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle».

³ Même si l'annexe B de la déclaration d'engagement du 22 mai 2003 énumère 39 éléments, seuls 38 peuvent réellement figurer dans un PNR, puisque l'ancien domaine OSI («Other service information») ne devrait être utilisé que si un code SSR («Special Service request») n'est pas disponible, conformément au service de réservation IATA – Manuel, 20^{ème} édition, effectif le 1^{er} juin 2003-31 mai 2003, point 10.3, p. 127.

La liste des codes et des champs de données à supprimer n'est pas encore disponible. Le groupe de travail tient néanmoins à souligner que si certains codes doivent clairement être supprimés (par exemple ceux qui ont trait aux préférences alimentaires, à l'état de santé ou aux convictions religieuses, tels que «tarif pèlerin», «missionnaire» ou «clergé»), d'autres codes nécessitent un examen approfondi, en particulier les champs «libres» de type «remarques générales» qui sont susceptibles de contenir des données sensibles. Dans leur déclaration d'engagement (version du 12 janvier), les autorités américaines font savoir que ces éléments seraient supprimés par l'utilisation d'une liste de mots «déclencheurs». Une telle approche ne garantit pas la suppression de l'ensemble des données sensibles figurant dans ces champs. Aussi la seule solution sûre consisterait à exclure ces champs du transfert, conformément à l'avis 4/2003.

À cet égard, le groupe de travail rappelle son avis du 13 juin 2003 selon lequel le transfert de données sensibles doit être exclu. Il n'est donc pas envisageable de ne procéder à des suppressions qu'après avoir transmis des données sensibles aux autorités américaines. Le groupe de travail invite la Commission à trouver les solutions techniques appropriées (tels que des filtres) afin d'éviter toute transmission de données sensibles aux autorités américaines.

E. UTILISATION DES DONNEES TIREES DES DOSSIERS PASSAGERS PNR

Dans une formule ajoutée à la déclaration, les autorités américaines décrivent les limitations qui existent en ce qui concerne leur accès aux données «tirées» de fichiers «PNR» lesquelles sont susceptibles de révéler certains aspects de la vie d'un passager et risquent d'interférer gravement avec le droit de la personne concernée à une vie privée et familiale, conformément à l'article 8 de la convention européenne des droits de l'homme. La nouvelle formulation est la suivante:

«Les informations personnelles supplémentaires qui seront recherchées par suite directe de l'examen de données passagers PNR seront obtenues auprès de sources non gouvernementales, uniquement par des voies légales et pour des impératifs légitimes de lutte contre le terrorisme ou d'application de la loi. Par exemple, si un numéro de carte de crédit figure dans un PNR, des informations sur les opérations liées au compte bancaire concerné pourront être recherchées dans le cadre d'une procédure légale, tel qu'un ordre de communication («*subpoena*») émis par un grand jury, une ordonnance de tribunal ou tout autre moyen légal. En outre, l'accès aux fichiers liés à des adresses électroniques mentionnées dans un PNR obéira aux exigences de la loi des États-Unis en matière de *subpoenas*, d'ordonnances des tribunaux, de mandats et d'autres procédures légales, en fonction du type d'information recherché».

Ces éclaircissements sont les bienvenus. Toutefois, ils ne répondent pas entièrement aux préoccupations du groupe de travail. En particulier, les finalités pour lesquelles les données passagers PNR peuvent être utilisées ne doivent pas inclure d'autres «impératifs [...] d'application de la loi» non spécifiés. De plus, l'accès aux messageries électroniques et à d'autres informations personnelles tirées d'un fichier «PNR» ne doit s'inscrire que dans le cadre des exigences de procédure visées dans les instruments internationaux de coopération judiciaire et policière. En outre, il doit être clair qu'en cas d'abus, un individu peut intenter un recours devant une autorité indépendante.

F. PERIODE DE CONSERVATION DES DONNEES

Le CBP conservera les données passagers PNR aux fins convenues par le CBP pendant trois ans et demi. Les données qui sont consultées manuellement pendant cette période seront conservées dans un fichier de données effacées pendant huit années supplémentaires.

Le groupe de travail note qu'il s'agit là d'une amélioration par rapport aux 7 ans initialement proposés dans la déclaration du 22 mai. Une durée de 3 ans et demi reste cependant beaucoup plus longue que la période de «quelques semaines voire quelques mois» telle que la préconise le groupe de travail dans son avis 4/2003. Le groupe de travail doute que le stockage généralisé de l'ensemble des données «PNR» sur des périodes aussi longues puisse être jugé «proportionnel et nécessaire dans une société démocratique».

De plus, la conservation supplémentaire des données pendant huit ans, prévue au simple cas où celles-ci seraient consultées, est disproportionnée dans la mesure où il n'y a pas de lien avec une enquête concrète ou un mandat concernant la personne dont les données sont consultées et qu'il est ainsi possible de dépasser *de facto* la limite de trois ans et demi.

On notera à cet égard qu'il est possible d'envisager des solutions qui sont plus respectueuses des principes de protection des données, mais qui restent efficaces dans la lutte contre la criminalité. L'Australie par exemple a élaboré un système dans le cadre duquel les douanes de ce pays ne conservent ou ne stockent de données sur un passager que si ce dernier a commis un acte illégal ou si les données sont nécessaires pour les besoins d'une enquête concernant un délit présumé.

G. METHODE DE TRANSFERT

En ce qui concerne la méthode de transfert, la groupe de travail rappelle son avis 4/2003 dans lequel in considère que le seul mécanisme de transfert dont la mise en œuvre ne crée pas de problèmes majeurs est celui du «push» (par lequel les données sont sélectionnées et transférées par les compagnies aériennes aux administrations américaines) plutôt que celui du «pull» (par lequel les autorités américaines ont un accès en ligne direct aux bases de données des compagnies aériennes et des systèmes de réservation).

Même si les autorités américaines n'émettent plus d'objection depuis quelques mois sur le système «push», le groupe de travail est particulièrement inquiet par le fait que les mécanismes techniques permettant d'appliquer un tel système géré directement par les compagnies aériennes européennes n'aient pas encore été mis en place. Le groupe de travail considère que des mesures concrètes devraient être adoptées d'ici avril 2004 au plus tard et encourage vivement la Commission à prendre sans attendre les mesures nécessaires pour atteindre cet objectif. En outre, le groupe de travail souligne que le niveau de protection assuré par les Etats-Unis ne pourra pas être considéré comme adéquat sans l'instauration d'un système « push ».

H. MOMENT DU TRANSFERT

Dans son avis 4/2003, le groupe de travail estime que les services de l'US CBP devraient recevoir les données relatives à un vol spécifique au plus tôt 48 heures avant le décollage. Après cela, les données ne devraient être mises à jour qu'une seule fois.

Sur ce point, la dernière version de la déclaration est strictement fidèle à la version précédente, qui prévoit un transfert des données 72 heures avant le décollage et un maximum de trois mises à jour.

Le groupe de travail déplore qu'aucune amélioration n'ait été obtenue sur ce point pendant les négociations.

I. TRANSFERT DE DONNEES PASSAGERS PNR VERS D'AUTRES AUTORITES ADMINISTRATIVES OU ETRANGERES

Dans son avis 4/2003, le groupe de travail demande que les autres organes publics habilités à recevoir les données soient identifiés avec précision, ajoutant que tout transfert ultérieur direct ou indirect devra être subordonné à l'acceptation d'engagements spécifiques au moins aussi favorables que ceux qui sont fournis à la Commission par les autorités américaines en ce qui concerne la protection des données transférées. En outre, le nombre d'autorités susceptibles de recevoir des données devra être restreint.

Le groupe de travail note qu'aucune liste globale des autorités auxquelles les données sont susceptibles d'être transférées n'a encore été établie. En outre, le groupe de travail reste préoccupé par les dispositions permettant au CBP de divulguer des données conformément aux «autres exigences prévues par la loi», en particulier si ces dispositions sont envisagées à la lumière des lois et des protocoles d'accord obligeant les États-Unis à partager leurs données avec d'autres pays.

En particulier, le mécanisme visé aux points 29 et 35 de la déclaration diffère sensiblement du principe de limitation de la finalité tel qu'affirmé par le groupe de travail (à savoir la lutte contre le terrorisme et les crimes liés au terrorisme) et même des finalités plus larges telles que définies aux points 1 et 3 de la déclaration.

J. GARANTIES – DROITS DES PERSONNES CONCERNEES

1) INFORMATIONS CLAIRES SUR LES PERSONNES CONCERNEES

Aux termes de l'avis 4/2003, et conformément à l'article 10 de la Directive, une information claire et précise devra être fournie aux personnes concernées sur l'identité du responsable du traitement, la finalité du traitement et toute autre information, telle que l'existence d'un droit d'accès et de rectification et les voies de recours effectives qui leur sont ouvertes.

Le groupe de travail note que le CBP fournira des informations aux voyageurs. À cet égard, le groupe de travail observe qu'il sera possible de finaliser rapidement une note d'information type une fois que le cadre juridique aura été fixé de manière plus précise, compte tenu également du projet soumis au groupe de travail. Il y a toutefois lieu de considérer qu'une note d'information globale peut servir de complément, mais en aucun cas de substituer aux exigences juridiques qui doivent être remplies pour que les transferts de données passagers PNR vers les États-Unis soient légaux.

2) ACCES

Dans son avis 4/2003, le groupe de travail souligne la nécessité de garanties réellement applicables, pour ce qui est des règles générales relatives à la liberté d'information (FOIA) afin d'assurer que ces dernières ne seront pas utilisées par des tiers pour accéder à des données passagers PNR détenues par l'administration américaine. Dans ces circonstances, il est important d'empêcher une possible discrimination entre citoyens et d'assurer que le droit d'accès des personnes concernées est mis en œuvre de manière générale et non ambiguë.

En ce qui concerne l'accès des tierces parties, le groupe de travail accueille favorablement les éclaircissements fournis par le CBP dans le document «Exemptions under the Freedom of Information Act (FOIA) Applicable to Passenger Name Record (PNR) Data».

Néanmoins, pour ce qui est de l'accès des passagers à leurs propres données, le groupe de travail continue d'avoir des craintes quant à la façon dont certaines exemptions pourraient être utilisées pour faire opposition aux droits d'une personne concernée, permettant ainsi à l'administration de lui refuser l'accès à ses données.

En outre, le groupe de travail souligne que le droit d'accès des personnes concernées n'a pas été explicitement étendu, alors que cela est préconisé dans l'avis 4/2003, aux nouvelles données susceptibles d'être générées par le traitement des données transmises depuis l'Europe (profil de risque, listes d'exclusion, etc.).

3) RECTIFICATION

Dans son avis 4/2003, le groupe de travail insiste sur l'importance de fournir aux personnes concernées un mécanisme efficace pour obtenir la rectification de leurs données. Le groupe de travail note que le champ d'application de la loi américaine sur la vie privée («US Privacy Act») est limité aux résidents américains. Aussi la question de la non discrimination des résidents européens par rapport aux citoyens américains n'est-elle toujours pas résolue et il convient de déterminer si le mécanisme de rectification exposé dans la déclaration peut être considéré comme un outil efficace et juridiquement contraignant en ce qui concerne le droit de rectification que le FOIA accorde aux citoyens américains et aux résidents étrangers.

4) RECOURS

Le «DHS Privacy Office» est convenu d'examiner rapidement les plaintes qui lui seront adressées par les autorités chargées de la protection des données dans les États membres pour le compte d'un résident de l'UE estimant que le DHS, y compris son «Privacy Office», n'a pas traité sa plainte à sa satisfaction.

Le groupe de travail accueille favorablement cette évolution. Il est important qu'une personne puisse obtenir une aide qualifiée dans certains cas; toutefois, la question relative à l'indépendance réelle du «Chief Privacy Officer», telle qu'elle est soulevée dans l'avis 4/2003 du groupe, n'a pas encore été résolue. Les membres du groupe de travail considèrent que les dispositions internes qu'ils ont prises en ce qui concerne les fonctions de «panel» visés dans la FAQ 5 de l'accord sur la sphère de sécurité peuvent être utiles dans ce contexte. Ils étudieront les corrections qu'il conviendra éventuellement d'y apporter en vue d'une application dans le contexte des «PNR».

Le groupe de travail déplore en revanche que les passagers n'aient pas la garantie de pouvoir s'adresser dans tous les cas à un mécanisme de recours véritablement indépendant en cas de litige avec le DHS. En outre, il apparaît maintenant que la déclaration ne se traduira peut-être pas par des effets juridiques contraignants ou des obligations dont la mise en œuvre peut être exigée devant un tribunal (cf. point 9 ci-dessus). Cette lacune reste importante en comparaison des droits dont jouit tout individu dont les données sont traitées dans l'UE, indépendamment de sa nationalité.

K. AUDITS

La nouvelle formulation suivante a été incluse dans la déclaration d'engagement (paragraphe 43):

«Le CBP, conjointement avec le Ministère de la sécurité intérieure, s'engage à participer une fois par an, ou plus souvent si cela est convenu entre les parties, à une révision conjointe avec la Commission assistée au besoin d'experts des États membres de l'UE⁴ concernant la mise en œuvre des présents engagements afin de contribuer au bon fonctionnement des modalités détaillées dans la présente déclaration. Cette révision commune peut porter sur les résultats du rapport annuel adressé au Congrès par le haut responsable de la vie privée auprès du Ministère de la sécurité intérieure (conformément au paragraphe 42 de la présente déclaration) et, dans la mesure autorisée par ce haut responsable, sur toute enquête réalisée au cours de la période sous-revue ou sur tout constat concernant, en particulier, la sécurité des données, le partage des PNR avec les autorités désignées et l'accès du personnel au PNR dans les bases de données concernées, ainsi que le traitement des plaintes. Dans la mesure où le haut responsable l'autorise, la révision commune peut porter aussi sur la mise en œuvre des présents engagements, de même que sur tout aspect susceptible d'améliorer les modalités d'utilisation des données passagers PNR aux fins visées au paragraphe 3 de la présente déclaration d'engagement.»

Il s'agit là d'une autre évolution favorable et le groupe de travail attend de ces révisions qu'elles soient menées avec l'ouverture et la transparence nécessaires pour en assurer l'efficacité. En tout état de cause, les membres du groupe de travail s'engagent à participer le cas échéant à toute révision de ce type et à observer les règles de confidentialité convenues par les deux parties. Le groupe de travail se réserve évidemment le droit de réétudier cette question, s'il le juge nécessaire, quel que soit le calendrier des révisions.

L. CROISEMENT DE FICHIERS

Les événements récents montrent qu'un nouvel élément doit être pris en considération en plus de ceux qui ont été mentionnés ci-dessus. Les données passagers PNR collectées par le CBP sont comparées aux États-Unis à des listes de personnes recherchées. Ces opérations de croisement de fichiers sont à l'origine de l'annulation à la dernière minute

⁴ Chaque partie devra, au préalable, informer l'autre de la composition de sa délégation, qui pourra regrouper des responsables des autorités compétentes en matière de protection des données ou de la vie privée, des autorités douanières et d'autres autorités policières ou en charge de la sécurité des frontières et des transports aériens. Les autorités participantes seront tenues au secret des délibérations et recevront les autorisations nécessaires. Cette exigence de confidentialité ne fera cependant pas obstacle à ce que chaque partie rende compte comme il se doit des résultats de la révision commune aux autorités nationales compétentes, y compris le Congrès des États-Unis et le Parlement européen. Les deux parties arrêteront d'un commun accord les modalités détaillées de la révision.

de plusieurs vols en provenance de l'UE. Les informations fournies ultérieurement au public montrent que ces annulations étaient dues à des erreurs ou à des cas de confusion d'identité ou d'homonymie avec des personnes suspectées de terrorisme.

Ces circonstances s'inscrivent dans le cadre de la qualité des données et du principe de protection des données. Le groupe de travail considère que d'autres initiatives doivent être prises pour éviter d'exposer les passagers, les membres d'équipage et les compagnies aériennes à ce type de problèmes.

CONCLUSION

Le groupe de travail rappelle que l'objectif global, conformément à ce qu'il indique dans son avis 4/2003, est l'établissement d'un cadre légal clair pour que tout transfert de données des compagnies aériennes vers les États-Unis soit compatible avec les principes de protection des données personnelles. Le groupe de travail a pris bonne note des progrès réalisés dans le dialogue États-Unis/Union européenne en ce qui concerne les données passagers PNR, notamment la dernière déclaration du 12 janvier 2004 récemment présentée par l'administration américaine et se réjouit des améliorations qu'elle comporte par rapport à la version précédente.

De l'avis du groupe de travail toutefois, les progrès limités qui ont été enregistrés ne permettent pas de juger qu'un niveau adéquat de protection des données est atteint. Le groupe de travail estime que toute solution devra respecter au moins les principes suivants de protection des données:

– **qualité des données:**

- le transfert de données doit uniquement avoir pour finalité la lutte contre les actes de terrorisme et certains crimes en rapport avec le terrorisme (à définir);
- la liste des données à transférer doit être proportionnelle et ne pas être excessive;
- les croisements de données par rapport à celles d'individus suspects doivent respecter des normes de qualité élevée assurant une certitude de résultat;
- les périodes de conservation des données doivent être courtes et proportionnelles;
- les données des passagers ne doivent pas être utilisées pour mettre en œuvre et/ou tester le système CAPPS II ou des systèmes similaires;

– les **données sensibles** ne doivent pas être transmises;

– **droits des personnes concernées:**

- il convient de transmettre des informations claires, actuelles et compréhensibles aux passagers;
- un droit d'accès et de rectification doit être accordé sans discrimination;
- il y a lieu de prévoir des dispositions satisfaisantes garantissant aux passagers le droit de s'adresser à un organe de recours véritablement indépendant;

- **niveau d'engagement des autorités américaines:**
 - les engagements pris par la partie américaine doivent avoir un caractère juridique pleinement contraignant pour les États-Unis;
 - il y a lieu de clarifier le champ d'application, la base juridique et la valeur d'un éventuel «accord international allégé»;
- les **transferts ultérieurs** de données passagers PNR à d'autres gouvernements ou organes étrangers doivent être strictement limités;
- **méthode de transfert:** il convient de mettre en place une méthode de transfert «push», par laquelle les données sont sélectionnées et transférées par les compagnies aériennes aux administrations américaines.

Fait à Bruxelles, le 29 janvier 2004

Par le groupe de travail

Le Président

Stefano RODOTA