I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives

(2008/C 110/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1],

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [2], et notamment son article 41,

vu la demande d'avis formulée par la Commission conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, reçue le 13 novembre 2007,

A ADOPTÉ L'AVIS SUIVANT

I. INTRODUCTION

Consultation du CEPD

1. La Commission a soumis le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives (ci-après dénommée «la proposition») au CEPD pour avis, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001.

2. La proposition porte sur le traitement des données PNR au sein de l'UE et est étroitement liée à d'autres mécanismes de collecte et d'utilisation des données relatives aux passagers, en particulier l'accord intervenu entre l'UE et les États-Unis en juillet 2007. Ces mécanismes intéressent vivement le CEPD, qui a déjà eu l'occasion de formuler des observations préliminaires sur le questionnaire de la Commission relatif au système PNR prévu par l'UE, soumis en décembre 2006 aux parties intéressées [3]. Le CEPD se félicite de ce que la Commission le consulte. Il estime qu'il convient de mentionner le présent avis dans le préambule de la décision du Conseil.

Contexte de la proposition

3. Cette proposition vise à harmoniser les dispositions des États membres en ce qui concerne l'obligation qu'ont les transporteurs aériens assurant des vols au départ ou à destination d'un ou plusieurs États membres, de transmettre aux autorités compétentes les données PNR afin de prévenir et de combattre les infractions terroristes et la criminalité organisée.

4. L'UE a arrêté des modalités de transfert des données PNR, pour des finalités comparables, avec les États-Unis, d'une part, et le Canada, d'autre part. Un premier accord conclu avec les États-Unis en mai 2004 a été remplacé par un

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.

[3] Notamment les États membres, les autorités de protection des données et les associations de transporteurs aériens. Ce questionnaire avait été établi en vue de l'élaboration d'une analyse d'impact de la présente proposition par la Commission européenne.

nouvel accord en juillet 2007 ([1]). Un accord similaire a été conclu avec le Canada en juillet 2005 ([2]). En outre, il est prévu que des négociations soient engagées entre l'UE et l'Australie en vue d'un accord concernant l'échange de données PNR, et la Corée du Sud exige également des données PNR pour les vols à destination de son territoire, sans toutefois qu'il y ait de projet de négociations au niveau européen à ce stade.

5. Au sein de l'UE, cette proposition vient compléter la directive 2004/82/CE ([3]) du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (données API), afin de lutter contre l'immigration clandestine et d'améliorer les contrôles aux frontières. Cette directive aurait dû être transposée dans la législation nationale des États membres au plus tard le 5 septembre 2006. Cependant, tous les États membres ne l'ont pas encore mise en œuvre.

6. Contrairement aux données API (informations préalables sur les passagers), censées permettre l'identification des personnes, les données PNR visées dans la proposition contribueraient à procéder à une évaluation des risques présentés par certaines personnes, à recueillir des informations et à établir des liens entre des personnes connues et d'autres qui ne le sont pas.

7. Les principaux éléments de la proposition sont les suivants:

   — elle prévoit que les transporteurs aériens mettent les données PNR à la disposition des autorités compétentes des États membres afin de prévenir et de combattre les infractions terroristes et la criminalité organisée,

   — elle prévoit qu'en principe chaque État membre désigne une unité de renseignements passagers chargée de collecter les données PNR auprès des transporteurs aériens (ou des intermédiaires désignés) et de procéder à une évaluation des risques présentés par les passagers,

   — les informations ainsi analysées seront transmises aux autorités compétentes de chaque État membre. Ces informations seront échangées avec d'autres États membres au cas par cas et aux fins indiquées plus haut,

   — les transmissions vers des pays tiers doivent répondre à des conditions supplémentaires,

   — les données seront conservées pendant treize ans, dont huit dans une base de données passive,

   — le traitement des données sera régi par la (le projet de) décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (ci-après dénommée «la décision-cadre relative à la protection des données») ([4]),

   — un comité composé de représentants des États membres assistera la Commission pour les questions liées à l'adoption de protocoles et au cryptage, ainsi que pour les critères et les pratiques à appliquer à l'évaluation des risques,

   — la décision fera l'objet d'un réexamen trois ans au plus tard après son entrée en vigueur.

Éléments fondamentaux de l'avis du CEPD

8. La proposition sur laquelle le CEPD est consulté constitue une étape supplémentaire vers une collecte systématique des données concernant des personnes qui, en principe, ne sont soupçonnées d'aucune infraction. Comme il a été mentionné plus haut, on peut observer cette évolution aussi bien au niveau international qu'au niveau européen.

9. Le CEPD note que le Groupe de l'article 29 et le Groupe «Police et justice» ont également présenté un avis conjoint sur la proposition ([5]). Le CEPD se rallie à cet avis. Le présent avis met l'accent sur un certain nombre de points supplémentaires, qu'il développe.

10. Le présent avis du CEPD étudiera tous les aspects pertinents de la proposition, en se concentrant toutefois sur quatre questions principales.

   — La première de ces questions concerne la légitimité des mesures prévues. L'objectif, la nécessité et la proportionnalité de la proposition seront examinés au regard des critères énoncés à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

   — Le présent avis examinera également la question du droit applicable au traitement envisagé. Il convient notamment d'accorder une attention toute particulière au champ d'application de la décision-cadre relative à la protection des données en relation avec l'application de la législation en matière de protection des données existant dans le cadre du premier pilier. Le CEPD se penchera également sur les conséquences du régime de protection des données applicable sur l'exercice par la personne concernée de ses droits.

([1]) 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) (JO L 204 du 4.8.2007, p. 18).

([2]) Accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers (JO L 82 du 21.3.2006, p. 15).

([3]) Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO L 261 du 6.8.2004, p. 24).

([4]) Pour cette proposition, le dernier projet en date peut être consulté sur le registre public des documents du Conseil, sous la cote 16397/07.

([5]) Avis conjoint 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, présentée par la Commission le 6 novembre 2007, adopté par le Groupe de l'article 29 le 5 décembre 2007 et par le Groupe «Police et Justice» le 18 décembre 2007, WP 145, WPPJ 01/07.

— Ensuite, le présent avis portera sur la qualité des destinataires des données au niveau national. En particulier, la qualité des unités de renseignements passagers, des intermédiaires et des autorités compétentes désignées pour procéder à l'évaluation des risques et à l'analyse des données relatives aux passagers suscite certaines inquiétudes, la proposition n'apportant aucune précision à cet égard.

— La quatrième question a trait aux conditions régissant la communication des données à des pays tiers. Il n'apparaît pas clairement quelles conditions ces transmissions devront respecter lorsque différentes règles sont applicables: les conditions prévues par la présente proposition, celles fixées par la décision-cadre relative à la protection des données ou celles définies par les accords internationaux existants (avec les États-Unis et le Canada).

11. D'autres points importants seront recensés dans une dernière partie, notamment les mesures positives en termes de protection des données, mais également d'autres inquiétudes suscitées par la proposition.

II. LÉGITIMITÉ DES MESURES PROPOSÉES

12. Pour analyser la légitimité des mesures proposées conformément aux principes fondamentaux de la protection des données, et en particulier l'article 8 de la Charte des droits fondamentaux de l'Union européenne et les articles 5 à 8 de la Convention n° 108 ([1]) du Conseil de l'Europe, il est nécessaire de cerner précisément la finalité poursuivie par le traitement de données à caractère personnel prévu et d'en évaluer tant la nécessité que la proportionnalité. Il y a lieu de s'assurer qu'il n'existe aucun autre moyen, plus respectueux de la vie privée, d'atteindre le but visé.

Cerner la finalité poursuivie

13. Le libellé de la proposition et l'analyse d'impact indiquent qu'il ne s'agit pas seulement d'identifier des terroristes connus ou des criminels notoires impliqués dans la criminalité organisée, en comparant leur nom avec ceux qui figurent sur les listes gérées par les services répressifs. L'objectif est de recueillir des renseignements sur le terrorisme ou la criminalité organisée, et plus précisément de «procéder à des évaluations de risques des personnes pour obtenir des informations et établir des liens entre des personnes connues et des personnes inconnues» ([2]). Ainsi, l'objectif cité à l'article 3, paragraphe 5, de la proposition est tout d'abord d'«identifier les personnes qui sont *ou qui pourraient être* impliquées dans une infraction terroriste ou dans un crime organisé, *ainsi que leurs associés*».

14. C'est le motif invoqué pour expliquer que les données API ne suffisent pas pour atteindre le but allégué. En effet, comme il a déjà été mentionné, alors que les données API sont censées permettre l'identification des personnes, les données PNR n'ont pas cet objectif, mais leurs détails permettraient de procéder à une évaluation des risques présentés par les personnes, de recueillir des informations et d'établir des liens entre des personnes connues et d'autres qui ne le sont pas.

15. Il n'est donc pas seulement question d'appréhender des personnes *connues*, mais également de localiser des personnes qui *pourraient* répondre aux critères fixés par la proposition.

Afin d'identifier ces personnes, l'analyse de risque et la détection de modèles forment le cœur du projet. Le considérant 9 de la proposition indique explicitement qu'il importe de conserver les données «pour une période assez longue afin de permettre l'élaboration d'indicateurs de risques et l'esquisse de modèles de déplacement et de comportement».

16. L'objectif poursuivi comporte donc deux niveaux, le premier étant l'objectif général de lutte contre le terrorisme et la criminalité organisée, le deuxième englobant, quant à lui, les moyens et les mesures propres à la réalisation de cet objectif. Alors que l'objectif de lutte contre le terrorisme et la criminalité organisée semble suffisamment clair et légitime, les moyens mis en œuvre pour le réaliser sont plus discutables.

Établir des modèles et évaluer les risques

17. La proposition ne précise pas les modalités de l'élaboration des modèles ni celles de l'évaluation des risques. L'analyse d'impact indique que les données PNR seront utilisées de la manière suivante: il s'agit de «comparer les données PNR à un ensemble de caractéristiques et de traits de comportements afin de réaliser une évaluation des risques. Lorsqu'un passager correspond à une certaine catégorie de risques, il pourrait être identifié comme passager à haut risque» ([3]).

18. Les suspects pourraient aussi bien être sélectionnés sur la base d'éléments concrets figurant dans les données PNR les concernant (par exemple un contact avec une agence de voyage suspecte ou encore une référence de carte de crédit volée), que sur la base de «modèles» ou d'un profil abstrait. Différents types de profil pourraient en effet être établis à partir de schémas de déplacements, pour des «passagers normaux» ou des «passagers suspects». Ces profils permettraient d'approfondir les recherches concernant les passagers ne relevant pas de la catégorie «passagers normaux», d'autant plus si leur profil est associé à d'autres éléments suspects, tels une carte de crédit volée.

19. Bien qu'on ne puisse pas partir du principe que les passagers seront ciblés en fonction de leur religion ou de toute autre donnée sensible, il apparaît néanmoins qu'ils pourraient faire l'objet d'une enquête fondée sur un ensemble d'informations *concrètes* et d'informations *abstraites, notamment* des schémas types et des profils abstraits.

([1]) Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

([2]) Exposé des motifs de la proposition, point 1.

([3]) Analyse d'impact, chapitre 2.1, «Description du problème».

20. On peut se demander si ce type d'enquête peut être considéré comme du profilage. Celui-ci peut être défini comme une «une méthode informatisée ayant recours à des procédés de data mining (fouille de données) sur des entrepôts de données (data warehouse) permettant ou devant permettre de classer avec une certaine probabilité et donc avec un certain taux d'erreur induit un individu dans une catégorie particulière afin de prendre des décisions individuelles à son égard» ([1]).

21. Le CEPD n'ignore pas que la définition du profilage fait encore l'objet de discussions. Qu'il soit officiellement établi, ou non, que la proposition vise à «profiler» les passagers, il ne s'agit pas ici de débattre de définitions. Ce qui est en jeu, c'est l'incidence sur les personnes concernées.

22. La préoccupation majeure du CEPD est liée au fait que des décisions concernant des personnes seront prises à partir de modèles et de critères établis en faisant appel aux données relatives à l'ensemble des passagers. Il est donc possible que des décisions concernant une personne soient prises (au moins en partie) sur la base de modèles établis à partir des données relatives à *d'autres* personnes. Par conséquent, c'est en faisant référence à un contexte abstrait que seront prises des décisions qui pourraient avoir des répercussions importantes pour les personnes concernées. Or, il est extrêmement difficile, pour des particuliers, de se défendre contre de telles décisions.

23. En outre, il est prévu que l'évaluation des risques se fasse en l'absence de normes uniformes pour l'identification des suspects. Le CEPD remet sérieusement en question la sécurité juridique de l'ensemble du processus de filtrage, les critères auxquels seront soumis tous les passagers étant mal définis.

24. Il rappelle la jurisprudence de la Cour européenne des droits de l'homme, selon laquelle la législation nationale doit être suffisamment précise pour indiquer aux citoyens dans quelles circonstances et à quelles conditions les autorités publiques sont habilitées à archiver et à utiliser des informations concernant leur vie privée. La personne concernée devrait avoir accès à ces informations, et celles-ci devraient être prévisibles quant à leurs répercussions. En règle générale, «prévisible» signifie «formulées avec une précision suffisante pour permettre à toute personne — bénéficiant éventuellement d'une assistance appropriée — d'adapter son comportement» ([2]).

25. Pour conclure, c'est en particulier ce type de risques qui conduit à examiner attentivement la proposition en question. Alors que l'objectif général de lutte contre le terrorisme et la criminalité organisée est en soi clair et légitime, l'objet du traitement qu'il est prévu de mettre en œuvre ne semble pas suffisamment délimité et justifié. C'est pourquoi le CEPD engage vivement le législateur européen à se pencher sur ce problème, avant l'adoption de la décision-cadre.

Nécessité

26. Il est évident, comme indiqué plus haut, que les mesures envisagées portent atteinte à la vie privée. En revanche, leur utilité est loin d'être démontrée.

27. L'analyse d'impact relative à la proposition met l'accent sur la meilleure manière d'établir un système PNR propre à l'UE, plutôt que sur la nécessité d'un tel système. Dans cette analyse ([3]), il est fait référence aux systèmes PNR existant dans d'autres pays, tels que les États-Unis et le Royaume-Uni. On peut toutefois déplorer l'absence de faits et de chiffres précis concernant ces systèmes. Il est question de «nombreuses arrestations», dans le cadre de «diverses infractions», grâce au système Semaphore mis en place par le Royaume-Uni, sans précision quant à un éventuel lien avec le terrorisme ou la criminalité organisée. Aucun détail n'est donné en ce qui concerne le programme américain, hormis le fait que l'UE a pu «apprécier la valeur de ces données PNR et […] en réaliser le potentiel à des fins répressives».

28. Non seulement *la proposition* ne contient pas d'informations précises sur les résultats concrets de tels systèmes PNR, mais, en outre, les rapports publiés par d'*autres services*, tel que le GAO aux États-Unis (Direction de l'audit du Congrès américain), ne confirment pas, à ce stade, l'efficacité de ces mesures ([4]).

([1]) (Traduction du Conseil) Cette définition est tirée d'une étude récente du Conseil de l'Europe sur le profilage: *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, Novembre 2007 (non encore publié). Voir également la définition qu'en donne Lee Bygrave: «D'une manière générale, le profilage est un processus qui consiste à déduire une série de caractéristiques (le plus souvent comportementales) au sujet d'une personne ou d'une entité donnée, puis de traiter cette personne/entité (ou d'autres personnes/entités) en fonction de ces caractéristiques. En tant que tel, le processus de profilage comporte deux étapes principales: i) la réalisation du profil — processus de déduction d'un profil; ii) l'application du profil — processus de traitement des personnes/entités en fonction du profil déterminé» (Traduction du Conseil). L. A. BYGRAVE, «Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling», *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24, http://www.austlii.edu.au/au/journals/PLPR/2000/40.html

([2]) Rotaru contre Roumanie, n° 28341/95, points 50, 52 et 55 (Traduction du Conseil).
Voir également Amann contre Suisse, n° 27798/95, points 50 *et s.*

([3]) Chapitre 2.1, «Description du problème».

([4]) Voir, par exemple, le rapport adressé en mai 2007 par la Direction de l'audit du Congrès américain aux membres du Congrès qui avaient demandé une étude à ce sujet: «Aviation security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain», http://www.gao.gov/new.items/d07346.pdf

29. Le CEPD est d'avis que les techniques consistant à évaluer les risques présentés par les personnes en recourant à des instruments de «data mining» et des modèles de comportement doivent faire l'objet d'une analyse plus approfondie, et qu'il convient d'en établir clairement l'utilité dans le cadre de la lutte contre le terrorisme, et ce, avant qu'elles soient utilisées à une aussi grande échelle.

Proportionnalité

30. Afin de mesurer l'équilibre entre l'ingérence dans la vie privée d'une personne et la nécessité d'une mesure ([1]), il y a lieu de prendre en considération les éléments suivants:

— les mesures s'appliquent à tous les passagers, qu'ils fassent ou non l'objet d'une enquête des services répressifs; il s'agit d'investigations proactives, effectuées à une échelle sans précédent,

— les décisions relatives aux personnes peuvent se fonder sur des profils abstraits, et comportent donc une marge d'erreur non négligeable,

— la nature des mesures à prendre à l'encontre de la personne concernée relève de la répression: les conséquences en termes d'exclusion ou de contrainte sont dès lors plus lourdes en termes d'ingérence dans la vie privée que dans un contexte différent, par exemple l'escroquerie à la carte de crédit.

31. Le respect du principe de proportionnalité suppose non seulement que la mesure proposée soit efficace, mais aussi que l'objectif poursuivi par la proposition ne puisse être atteint au moyen d'instruments portant moins atteinte à la vie privée. L'efficacité des mesures prévues n'a pas été démontrée. Il convient d'examiner soigneusement l'existence de solutions alternatives avant de mettre en œuvre des mesures supplémentaires et/ou nouvelles pour traiter les informations à caractère personnel. Selon le CEPD, aucune évaluation globale de ce type n'a été effectuée.

32. Il souhaite rappeler l'existence d'autres systèmes à grande échelle visant à contrôler les déplacements de personnes à l'intérieur ou aux frontières de l'UE, qu'ils soient opérationnels ou sur le point d'être mis en œuvre, y compris en particulier le système d'information sur les visas ([2]) et le système d'information Schengen ([3]). Bien que ces instruments n'aient pas pour principal objectif la lutte contre le terrorisme ou la criminalité organisée, les services répressifs y ont, ou y auront, accès dans une certaine mesure dans le cadre plus large de la lutte contre la criminalité ([4]).

33. Un autre exemple concerne les données à caractère personnel contenues dans certaines bases de données de la police nationale — notamment des informations biométriques — qui sont rendues accessibles en vertu du traité de Prüm signé en mai 2005, étendu à l'ensemble des États membres de l'Union européenne ([5]).

34. Tous ces instruments permettent un contrôle global des déplacements de personnes, même si les buts recherchés diffèrent. La manière dont ils peuvent d'ores et déjà contribuer à lutter contre certaines formes de criminalité, y compris le terrorisme, devrait faire l'objet d'une étude approfondie et exhaustive avant que ne soit prise la décision de mettre en œuvre une nouvelle forme de contrôle systématique de toutes les personnes quittant l'UE ou entrant sur son territoire par avion. Le CEPD recommande à la Commission d'effectuer une telle étude, qui constitue une étape nécessaire dans le processus législatif.

Conclusion

35. Au vu de ce qui précède, le CEPD tire au sujet de la légitimité des mesures proposées les conclusions ci-après. Accumuler les bases de données sans disposer d'une vision globale des résultats concrets et des lacunes:

— est contraire à une politique législative rationnelle dans le cadre de laquelle il n'y a pas lieu d'adopter de nouveaux instruments tant que les instruments existants n'ont pas été pleinement mis en œuvre et que leur insuffisance n'a pas été démontrée ([6]),

— pourrait ouvrir la voie à une évolution vers une société de surveillance totale.

36. La lutte contre le terrorisme peut certainement constituer un motif légitime pour appliquer des exceptions aux droits fondamentaux à la vie privée et à la protection des données. Toutefois, pour être valable, la nécessité de l'ingérence doit s'appuyer sur des éléments clairs et indéniables,

([1]) Selon l'article 9 de la Convention 108, «il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la partie, constitue une mesure nécessaire dans une société démocratique:
1) à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales;
2) à la protection de la personne concernée et des droits et libertés d'autrui.»

([2]) Décision 2004/512/CE du Conseil du 8 juin 2004 portant création du système d'information sur les visas (VIS) (JO L 213 du 15.6.2004, p. 5); Proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, (COM)2005 835 final; Proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, (COM)2005 600 final.

([3]) Voir notamment la décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 205 du 7.8.2007).

([4]) Voir à ce sujet l'avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière [COM (2005) 600 final] (JO C 97 du 25.4.2006, p. 6).

([5]) Voir l'avis du CEPD concernant les décisions de Prüm: avis du 4 avril 2007 sur l'initiative de 15 États membres en vue de l'adoption de la décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière (JO C 169 du 21.7.2007, p. 2) et l'avis du 19 décembre 2007 sur l'initiative de la République fédérale d'Allemagne en vue de l'adoption d'une décision du Conseil concernant la mise en œuvre de la décision 2007/…/JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, disponible à l'adresse suivante:
http://www.edps.europa.eu

([6]) Le CEPD a avancé cet argument à maintes reprises, en dernier lieu dans son avis du 25 juillet 2007 sur la mise en application de la directive sur la protection des données (JO C 255 du 27.10.2007, p. 1).

et la proportionnalité du traitement doit être démontrée. Cette exigence s'impose d'autant plus dans le cas d'une atteinte considérable à la vie privée des personnes concernées, comme celle que prévoit la proposition.

37. On ne peut que constater que la proposition ne contient aucun élément justificatif de ce type et que les tests de nécessité et de proportionnalité ne sont pas rencontrés.

38. Le CEPD insiste sur le caractère essentiel des critères de nécessité et de proportionnalité évoqués plus haut. Ils représentent une condition *sine qua non* à l'entrée en vigueur de la présente proposition. Toutes les autres observations qu'il formule dans le présent avis doivent être considérées à la lumière de cette condition préalable.

III. DROIT APPLICABLE — EXERCICE PAR LA PERSONNE CONCERNÉE DE SES DROITS

Droit applicable

39. L'analyse qui suit se concentrera sur trois points:

— une description des différentes étapes du traitement prévu par la proposition en vue de déterminer le droit qui s'applique à chacune de ces étapes,

— les limites de la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, en ce qui concerne le champ d'application d'une part, et les droits des personnes concernées, d'autre part,

— une analyse plus générale de la mesure dans laquelle un instrument relevant du troisième pilier peut s'appliquer à des acteurs privés traitant des données dans le cadre du premier pilier.

Droit applicable aux différentes étapes du traitement

40. L'article 11 de la proposition stipule que «les États membres veillent à ce que la décision-cadre du Conseil (…) relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale s'applique aux traitements de données à caractère personnel en vertu de la présente décision-cadre».

41. Cependant, malgré cette disposition, il n'apparaît pas clairement dans quelle mesure la décision-cadre relative à la protection des données — un instrument qui relève du troisième pilier du traité sur l'UE — s'appliquera aux données traitées par les transporteurs aériens, recueillies par les unités de renseignements passagers, et utilisées ensuite par d'autres services compétents.

42. La première étape du traitement des données à caractère personnel prévu par la proposition est le traitement effectué par les transporteurs aériens, qui sont tenus de communiquer les données PNR dont ils disposent aux unités nationales de renseignement passagers — en principe, par le biais d'un système d'exportation («push»). Le libellé de la proposition et de l'analyse d'impact ([1]) laisse entendre que des données pourraient également être transmises en masse par les transporteurs aériens à des intermédiaires. Les transporteurs aériens sont essentiellement actifs dans un environnement commercial, et soumis à la législation nationale relative à la protection des données mettant en œuvre la directive 95/46/CE ([2]). Des questions concernant le droit applicable se poseront à partir du moment où les données recueillies sont utilisées à des fins répressives ([3]).

43. Les données seraient ensuite filtrées par un intermédiaire (afin d'être formatées et d'exclure les données PNR qui n'apparaîtraient pas sur la liste des données requises par la proposition) ou envoyées directement aux unités de renseignements passagers. Les intermédiaires pourraient aussi être des acteurs du secteur privé, comme SITA, qui exerce des activités en ce sens dans le cadre de l'accord PNR avec le Canada.

44. En ce qui concerne les unités de renseignements passagers, responsables de l'évaluation des risques pour l'ensemble des données, il n'apparaît pas clairement qui sera chargé du traitement. Les services des douanes et ceux chargés des contrôles aux frontières pourraient y participer, sans que les services répressifs soient nécessairement impliqués.

45. La transmission ultérieure des données filtrées aux autorités «compétentes» fera probablement intervenir les services répressifs. La proposition prévoit que «les autorités compétentes ne comprennent que les autorités chargées de prévenir et de combattre les infractions terroristes et la criminalité organisée».

46. Au fil des étapes du traitement des données, les acteurs concernés et l'objectif poursuivi présentent un lien de plus en plus étroit avec la coopération policière et judiciaire en matière pénale. Cependant, la proposition n'indique pas explicitement à quel moment précis la décision-cadre relative à la protection des données s'applique. Le libellé semblerait même suggérer que celle-ci s'applique au processus dans son ensemble, voire aux transporteurs aériens ([4]). Toutefois, la décision-cadre relative à la protection des données prévoit elle-même certaines restrictions à cet égard.

([1]) Article 6, paragraphe 3, de la proposition et annexe A, de l'analyse d'impact, «Moyens utilisés pour la transmission des données par les transporteurs».

([2]) Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

([3]) Voir à cet égard les conséquences de l'arrêt PNR. Arrêt du 30 mai 2006 dans les affaires jointes Parlement européen contre Conseil (C-317/04) et Commission (C-318/04), Recueil 2006, point 56.

([4]) Article 11 de la proposition. Voir également le considérant 10 du préambule: «La décision-cadre du Conseil (…) relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale devrait être applicable aux traitements de toutes les données à caractère personnel réalisés en vertu de la présente décision-cadre. Les droits des personnes concernées pour ce qui concerne le traitement des données, comme le droit à l'information, le droit d'accès, le droit de rectification, d'effacement et de verrouillage des données, ainsi que les droits à réparation et aux recours juridictionnels, devraient être ceux prévus par ladite décision-cadre».

47. Le CEPD remet en question le fait même que le titre VI du traité sur l'UE puisse servir de base juridique à des obligations légales de routine confiées dans un but répressifs à des acteurs du secteur privé. Par ailleurs, il se demande si le titre VI du traité sur l'UE peut servir de base juridique à des obligations légales imposées à des autorités nationales qui ne relèvent pas, en principe, de la coopération entre services répressifs. Le présent avis examinera ces questions en détail.

Restrictions prévues par la décision-cadre relative à la protection des données

48. Le texte de la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale présente au moins deux restrictions importantes en ce qui concerne son champ d'application.

49. Premièrement, le champ d'application de la décision-cadre relative à la protection des données est bien défini dans la décision-cadre elle-même: celle-ci «ne s'applique qu'aux données collectées ou traitées par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales» ([1]).

50. Deuxièmement, la décision-cadre relative à la protection des données n'est pas supposée s'appliquer aux données traitées purement au niveau national: elle se limite aux données échangées entre États membres et à leur transmission ultérieure à des pays tiers ([2]).

51. Comparée à la directive 95/46/CE, la décision-cadre relative à la protection des données est également en retrait, en particulier en ce qu'elle prévoit une large exception au principe de la limitation de la finalité. S'agissant de ce principe, la proposition limite clairement la finalité du traitement à la lutte contre le terrorisme et la criminalité organisée. La décision-cadre relative à la protection des données permet toutefois quant à elle des traitements à des fins plus larges. Dans ce cas, la *lex specialis* (la proposition) devrait primer sur la *lex generalis* (la décision-cadre relative à la protection des données) ([3]), et ceci devrait être explicitement précisé dans le texte de la proposition.

52. C'est pourquoi le CEPD recommande l'ajout, dans la proposition, de la disposition suivante: «Les données à caractère personnel transmises par les transporteurs aériens conformément à la décision-cadre ne peuvent être traitées qu'à des fins de lutte contre le terrorisme et la criminalité organisée. Les exceptions au principe de limitation de la finalité prévues par la décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ne s'appliquent pas».

53. En conclusion, le CEPD constate de graves lacunes en matière de sécurité juridique quant au régime de protection des données applicable aux différents acteurs intervenant dans le projet, et en particulier aux transporteurs aériens et aux autres acteurs relevant du premier pilier, qu'il s'agisse des règles fixées par la proposition, par la décision-cadre relative à la protection des données ou par la législation nationale mettant en œuvre la directive 95/46/CE. Le législateur devrait préciser exactement à quelle étape du traitement ces différentes règles s'appliqueront.

Conditions d'application des règles des premier et troisième piliers

54. Le CEPD remet en question le fait même qu'un instrument relevant du troisième pilier crée des obligations légales de routine à des fins répressives, pour des acteurs du secteur privé ou public qui ne relèvent pas, en principe, de la coopération entre services répressifs.

55. On pourrait comparer cette situation à deux autres cas où le secteur privé est intervenu dans la conservation ou la transmission de données à des fins répressives:

— *l'affaire des données PNR transmises aux autorités américaines, prévoyant une transmission systématique des données PNR par les transporteurs aériens aux services répressifs*. La Cour de justice a estimé, dans cette affaire, que la Communauté n'était pas compétente pour conclure l'accord PNR. Elle a notamment justifié son arrêt par le fait que le transfert de données PNR au bureau des douanes et de la protection des frontières des États-Unis «constitu[ait] des opérations de traitement concernant la sécurité publique et [les] activités de l'État en matière pénale» ([4]). L'opération de traitement visée ici était un transfert *systématique* vers le bureau des douanes et de la protection des frontières des États-Unis, ce qui distingue cette affaire de la suivante:

— *la conservation générale des données par les opérateurs de services de communications électroniques*. Pour ce qui est de la compétence communautaire pour fixer une telle période de conservation, la situation est différente de celle dans l'affaire PNR-États-Unis, étant donné que la directive 2006/24/CE ([5]) prévoit une obligation de conservation des données qui restent sous le contrôle des opérateurs. Aucune transmission systématique des données aux services répressifs n'est envisagée. On peut conclure que, tant que les données restent sous le contrôle des fournisseurs de service, ceux-ci sont également responsables, vis-à-vis des personnes concernées, du respect des obligations en matière de protection des données à caractère personnel.

([1]) Considérant 5 *bis*, de la décision-cadre relative à la protection des données. (version du 11 décembre 2007).
([2]) Article 1er.
([3]) En ce qui concerne ce point, il convient d'examiner attentivement le libellé de l'article 27 *ter* du dernier projet de décision-cadre relative à la protection des données dans le troisième pilier.
([4]) Arrêt de la Cour de justice du 30 mai 2006 dans les affaires jointes Parlement européen contre Conseil (C-317/04) et contre Commission (C-318/04), Recueil 2006, point 56.
([5]) 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 L 105 du 13.4.2006, p. 54).

56. La proposition examinée ici, relative à un système PNR de l'UE, prévoit que les transporteurs aériens sont tenus de rendre systématiquement accessibles les données PNR concernant tous les passagers. Cependant, ces données ne sont pas transmises directement en masse aux services répressifs: elles peuvent être envoyées à un intermédiaire et sont analysées par un tiers, dont le statut demeure flou, avant que des informations sélectionnées soient transmises aux autorités compétentes.

57. L'essentiel du traitement a lieu dans un cadre juridique peu clair, présentant des liens étroits tant avec le premier qu'avec le troisième pilier. Comme nous le verrons plus en détail au point IV, la qualité des acteurs chargés du traitement des données n'est pas précisément définie. Les transporteurs aériens ne sont, de toute évidence, pas des services répressifs, et les intermédiaires peuvent être des acteurs du secteur privé. Même en ce qui concerne les unités de renseignements passagers qui seraient des autorités publiques, il convient de souligner que les autorités publiques n'ont pas toutes la qualité et les compétences requises pour effectuer régulièrement des missions répressives.

58. 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 secteurs 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, ce qui soulève la question du cadre qui, en matière de protection des données (premier ou troisième pilier), s'applique aux conditions d'une telle coopération: les règles devraient-elles se fonder sur la qualité du contrôleur des données (secteur privé) ou sur la finalité poursuivie (services répressifs)?

59. Le CEPD a déjà rappelé le risque de vide juridique entre les activités relevant du premier pilier et celles qui relèvent du troisième pilier ([1]). Il n'est en effet pas évident que les activités effectuées par des entreprises privées, ayant un quelconque rapport avec l'application du droit pénal, relèvent du champ d'action du législateur de l'Union européenne en vertu des articles 30, 31 et 34 du traité UE.

60. Si le cadre général (premier pilier) ne s'appliquait pas, les fournisseurs de services seraient tenus d'opérer de difficiles distinctions au sein même de leurs bases de données. En vertu des dispositions actuelles, il est évident que le responsable du traitement se doit de respecter, vis-à-vis des personnes concernées, les mêmes règles en matière de protection des données quelles que soient les finalités qui justifient la conservation des données. Il convient par conséquent d'éviter d'en arriver à ce que, selon la finalité poursuivie, le traitement par des prestataires de services soit régi par des cadres différents en matière de protection des données.

([1]) Voir l'avis 2007/C 255/01 du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données (JO C 255 du 27.10.2007, p. 1). Voir également le rapport annuel 2006, p. 47.

Exercice de leurs droits par les personnes concernées

61. Les différents régimes juridiques susceptibles de s'appliquer au niveau national auraient des conséquences importantes principalement sur l'exercice de ses droits par la personne concernée.

62. Il est indiqué dans le préambule de la proposition que «le droit à l'information, le droit d'accès, le droit de rectification, d'effacement et de verrouillage des données, ainsi que les droits à réparation et aux recours juridictionnels, devraient être ceux prévus par la décision-cadre relative à la protection des données». Toutefois, cette affirmation ne répond pas à la question de savoir qui est le responsable du traitement chargé de donner suite aux demandes des personnes concernées.

63. Certes, les transporteurs aériens pourraient communiquer des informations sur le traitement, mais la question est plus complexe en ce qui concerne l'accès aux données ou leur rectification. Ces droits sont en effet limités dans le cadre de la décision-cadre relative à la protection des données. Comme indiqué ci-dessus, il est peu probable qu'un prestataire de services tel qu'un transporteur aérien puisse être tenu d'accorder des droits différenciés d'accès et de rectification en ce qui concerne les données qu'il détient, en fonction de la finalité (commerciale ou répressive) poursuivie. On pourrait avancer que ces droits doivent être exercés en s'adressant aux unités de renseignements passagers ou aux autorités compétentes autrement désignées. La proposition ne donne cependant aucune autre indication à cet égard et, comme déjà indiqué, il n'apparaît pas non plus clairement que ces autorités (tout du moins les unités de renseignements passagers) seront des services répressifs disposant normalement de procédures d'accès spécifiques (éventuellement indirectes).

64. La personne concernée risque également de devoir faire face à différents destinataires des données dans la mesure où les unités de renseignements passagers sont concernées: les données sont en effet communiquées à l'unité de renseignements passagers du pays de départ/d'arrivée des vols, mais aussi, éventuellement, aux unités de renseignements passagers d'autres États membres au cas par cas. Par ailleurs, plusieurs États membres peuvent mettre en place ou désigner une unité de renseignements passagers unique et commune. La personne concernée pourrait dans ce cas devoir exercer ses droits en s'adressant à une autorité d'un autre État membre. À nouveau, on ne voit pas clairement si les règles nationales en matière de protection des données s'appliqueront (celles-ci sont censées être harmonisées au sein de l'UE) ou si une législation répressive particulière devra être prise en compte (étant donné l'absence d'harmonisation totale dans le cadre du troisième pilier au niveau national).

65. La question est la même en ce qui concerne l'accès aux données traitées par des intermédiaires, dont le statut n'est pas clair, et qui pourraient aussi être communs à des transporteurs aériens de différents pays de l'UE.

66. Le CEPD regrette l'incertitude qui demeure concernant l'exercice de ses droits fondamentaux par la personne concernée. Il souligne que cette situation est principalement due au fait que des acteurs dont la mission principale n'est pas la répression se voient confier des responsabilités dans ce domaine.

Conclusion

67. Le CEPD estime que la proposition devrait préciser quel régime juridique est applicable à quelle étape du traitement et à quel acteur ou à quelle autorité la personne concernée doit s'adresser pour exercer son droit d'accès ou de rectification. Le CEPD rappelle que, conformément à l'article 30, paragraphe 1, point b), du traité UE, les dispositions relatives à la protection des données devraient être appropriées et couvrir l'éventail complet des opérations de traitement prévues par la proposition. La simple mention de la décision-cadre relative à la protection des données ne suffit pas, compte tenu du champ d'application limité de ladite décision-cadre et de la restriction des droits qu'elle prévoit. En ce qui concerne les services répressifs, les dispositions de la décision-cadre relative à la protection des données devraient au moins s'appliquer à l'ensemble du traitement prévu dans la proposition, afin de garantir la cohérence de l'application des principes de protection des données.

IV. QUALITÉ DES DESTINATAIRES

68. Le CEPD note que la proposition ne donne aucune précision quant à la qualité des destinataires des données à caractère personnel collectées par les transporteurs aériens, qu'il s'agisse des intermédiaires, des unités de renseignements passagers ou des autorités compétentes. Il convient de souligner que la qualité du destinataire est directement liée au type de garanties en matière de protection des données qui s'appliquent audit destinataire. La différence entre les garanties prévues en particulier par les dispositions du premier et du troisième pilier a déjà été mentionnée. Il est essentiel que le régime applicable soit clair pour tous les acteurs concernés, y compris les gouvernements nationaux, les services répressifs, les autorités chargées de la protection des données ainsi que les responsables du traitement des données et les personnes concernées.

Intermédiaires

69. La proposition ne donne aucune indication concernant la qualité des intermédiaires ([1]). Le rôle de ces derniers en tant que responsables du traitement ou sous-traitants n'est pas précisé non plus. L'expérience montre qu'une entité du secteur privé, qu'il s'agisse d'un système informatisé de réservation ou d'une autre entité, pourrait très bien se voir confier la mission de recueillir directement les données PNR auprès des transporteurs aériens pour ensuite les transmettre aux unités de renseignements passagers. C'est en effet la manière dont les données sont traitées dans le cadre de l'accord PNR conclu avec le Canada. SITA ([2]) est la société chargée du traitement des informations. Le rôle de l'intermédiaire est déterminant, étant donné qu'il pourrait être chargé du filtrage/du reformatage des données qui sont transmises en masse par les transporteurs aériens ([3]). Même si les intermédiaires sont tenus de supprimer les informations traitées une fois qu'elles ont été transmises aux unités de renseignements passagers, le traitement en lui-même est très sensible: l'intervention des intermédiaires se traduit notamment par la création d'une base de données supplémentaire comprenant une quantité massive de données, incluant même, selon la proposition, des données sensibles (les intermédiaires étant alors tenus de les effacer). Pour ces raisons, le CEPD recommande qu'aucun intermédiaire ne soit associé au traitement des données relatives aux passagers, sauf si leur qualité et leurs missions sont strictement précisées.

Unités de renseignements passagers

70. Les unités de renseignements passagers jouent un rôle déterminant dans l'identification des personnes qui sont ou qui pourraient être impliquées dans une infraction terroriste ou dans un crime organisé, ainsi que leurs associés. Selon la proposition, elles seront chargées de créer des indicateurs de risque et de fournir des renseignements au sujet des modèles de déplacement ([4]). Lorsque l'évaluation des risques est fondée sur des modèles types de déplacement et non sur des éléments de preuve concrets liés à un cas particulier, l'analyse peut être considérée comme constituant une enquête proactive. Le CEPD souligne que ce type de traitement est en principe strictement réglementé par la législation des États membres (sinon interdit), et qu'il incombe à des autorités publiques particulières, dont le fonctionnement fait également l'objet d'une réglementation stricte.

71. Les unités de renseignements passagers se voient par conséquent confier des traitements d'informations très sensibles, sans que la proposition ne donne aucune précision sur leur qualité et les conditions dans lesquelles elles exerceraient cette compétence. Même s'il est probable que cette mission sera effectuée par un organisme gouvernemental, éventuellement les services des douanes ou ceux chargés des contrôles aux frontières, la proposition n'empêche pas expressément les États membres de la confier aux services de renseignement, voire à tout type de sous-traitant. Le CEPD souligne que la transparence et les garanties qui s'appliquent aux services de renseignement ne sont pas toujours identiques à celles applicables aux services répressifs traditionnels. Il est essentiel de fournir des précisions sur la qualité des unités de renseignements passagers, étant donné que cela aura des conséquences directes sur le cadre juridique applicable et les conditions en matière de contrôle. Le CEPD estime que la proposition doit inclure une disposition supplémentaire précisant les spécificités des unités de renseignements passagers.

([1]) Article 6 de la proposition.

([2]) La SITA a été créée en 1949 par onze transporteurs aériens. Des solutions à valeur ajoutée sont fournies au secteur du transport aérien par l'intermédiaire de la société commerciale SITA INC (Information, Networking Computing) et des services de réseaux par l'intermédiaire de SITA SC sur une base coopérative.

([3]) Annexe A de l'analyse d'impact, «Moyens utilisés pour la transmission des données par les transporteurs».

([4]) Article 3 de la proposition.

Autorités compétentes

72. Il ressort de l'article 4 de la proposition que toute autorité chargée de prévenir ou de combattre les infractions terroristes et la criminalité organisée peut recevoir les données. Si la finalité est clairement définie, la qualité de l'autorité n'est pas précisée. La proposition ne prévoit aucune limitation des destinataires aux services répressifs.

Comme indiqué précédemment en ce qui concerne les unités de renseignements passagers, il est essentiel que les informations sensibles concernées soient traitées dans un environnement assorti d'un cadre juridique clair, ce qui est plus souvent le cas, par exemple, pour les services répressifs que pour les services de renseignement. Étant donné les éléments relatifs au «data mining» et aux recherches proactives qui figurent dans la proposition, on ne peut exclure que ces services de renseignement soient associés au traitement des données, sans exclusion de tout autre type d'autorités.

Conclusion

73. À titre d'observation générale, le CEPD note que la mise en œuvre d'un système PNR de l'UE est rendue encore plus complexe par la diversité des compétences des services répressifs en fonction de la législation nationale des États membres, incluant ou non le renseignement, la fiscalité, l'immigration ou les missions de police. C'est toutefois une raison supplémentaire pour recommander que la proposition soit beaucoup plus précise en ce qui concerne la qualité des acteurs mentionnés et les garanties visant à contrôler l'exécution de leurs missions. Il conviendrait d'intégrer des dispositions supplémentaires à la proposition pour définir précisément les compétences et les obligations légales des intermédiaires, des unités de renseignements passagers et des autres autorités compétentes.

V. CONDITIONS DE COMMUNICATION À DES PAYS TIERS

74. La proposition prévoit certaines garanties en ce qui concerne la communication des données PNR à des pays tiers ([1]). Elle prévoit en particulier expressément l'application de la décision-cadre relative à la protection des données aux transferts de données, elle définit une limitation précise de la finalité et elle indique que l'accord de l'État membre est nécessaire en cas de transfert ultérieur. Le transfert devrait également se faire dans le respect de la législation nationale de l'État membre concerné et de tout accord international applicable.

75. De nombreuses questions subsistent cependant, en particulier en ce qui concerne la qualité de l'accord, les conditions d'application de la décision-cadre relative à la protection des données et la question de la «réciprocité» dans le transfert de données à des pays tiers.

([1]) Article 8 de la proposition.

Qualité de l'accord

76. L'État membre d'origine doit donner son accord explicite à la transmission ultérieure de données d'un pays tiers à un autre pays tiers. La proposition ne précise pas dans quelles conditions cet accord sera donné ni par qui, ni si les autorités nationales chargées de la protection des données devraient être associées à la décision. Le CEPD estime que la manière dont l'accord sera donné devrait au moins être conforme à la législation nationale concernant les conditions de transfert de données à caractère personnel aux pays tiers.

77. En outre, l'accord d'un État membre ne devrait pas prévaloir sur le principe selon lequel un niveau adéquat de protection doit être assuré par le pays destinataire pour le traitement prévu. Il conviendrait que toutes ces conditions soient réunies, comme dans la décision-cadre relative à la protection des données (article 14). Le CEPD propose par conséquent d'ajouter au paragraphe 1 de l'article 8 un point c) qui serait libellé comme suit: «et c) l'État tiers assure un niveau adéquat de protection pour le traitement prévu.» Le CEPD rappelle à cet égard que des mécanismes garantissant l'application de normes communes et la prise de décisions coordonnées en ce qui concerne le caractère adéquat du niveau de protection doivent être mis en place ([2]).

Application de la décision-cadre relative à la protection des données

78. La proposition se réfère aux conditions et garanties prévues par la décision-cadre relative à la protection des données, tout en précisant expressément certaines conditions, en particulier, l'accord susmentionné de l'État membre concerné et une limitation de la finalité à la prévention et la lutte contre les infractions terroristes et la criminalité organisée.

79. La décision-cadre relative à la protection des données prévoit elle-même des conditions applicables à la transmission de données à caractère personnel à des pays tiers, à savoir la limitation de la finalité, la qualité des destinataires, l'accord de l'État membre et le principe d'adéquation. Toutefois, elle prévoit également des dérogations à ces conditions de transmission: des intérêts légitimes qui prévalent, en particulier des intérêts publics importants, peuvent être une base suffisante pour le transfert même si les conditions énumérées ci-dessus ne sont pas remplies.

80. Comme il a déjà été indiqué au point III du présent avis, le CEPD estime qu'il doit être clairement indiqué dans le texte de la proposition que les garanties plus précises prévues par la proposition priment sur les conditions générales — et les exceptions — de la décision-cadre relative à la protection des données, lorsque celle-ci s'applique.

([2]) Avis du CEPD du 26 juin 2007 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, points 27 à 30 (JO C 139 du 23.6.2007, p. 1).

Réciprocité

81. La proposition traite de la question des éventuelles «demandes à titre de réciprocité» de pays qui peuvent demander à l'UE des données PNR concernant des vols à partir de l'UE vers leur territoire. Dans les cas où l'UE demande des données provenant des bases de données de transporteurs aériens de ces pays tiers parce qu'ils opèrent un vol à destination ou à partir de l'UE, ces pays tiers pourraient demander les mêmes informations aux transporteurs établis dans l'UE, y compris des données concernant des citoyens de l'UE. Même si la Commission considère cette éventualité comme «très peu probable», celle-ci est prévue. La proposition fait référence à cet égard au fait que les accords conclus avec les États-Unis et avec le Canada prévoient cette réciprocité «qui peut être appliquée automatiquement» ([1]). Le CEPD s'interroge sur l'impact d'une telle réciprocité automatique et sur l'application de garanties à ces transmissions, et notamment la prise en compte de l'existence d'un niveau adéquat de protection dans le pays concerné.

82. Il convient de faire une distinction entre les pays tiers qui ont déjà conclu un accord avec l'UE et ceux qui ne disposent pas d'un tel accord.

Pays n'ayant pas conclu d'accord avec l'UE

83. Le CEPD note que la réciprocité pourrait conduire à communiquer des données à caractère personnel à des pays dans lesquels aucune garantie ne peut être donnée en termes de normes démocratiques et de niveau adéquat de protection des données.

84. L'analyse d'impact fournit d'autres éléments en ce qui concerne les conditions de transmission des données à des pays tiers: l'avantage du système PNR de l'UE où les données sont filtrées par les unités de renseignements passagers y est souligné. Seules des données sélectionnées concernant des personnes soupçonnées (et non des données en masse) seraient transmises aux autorités compétentes des États membres et sans doute aussi à des pays tiers ([2]). Le CEPD recommande de préciser ce point dans le texte de la proposition. Une simple déclaration dans l'analyse d'impact n'assure pas la protection nécessaire.

85. La sélection des données contribuerait certes à réduire les incidences sur la vie privée des passagers, mais il faut rappeler que les principes de protection des données vont bien au-delà de la limitation des données et comprennent des principes tels que la nécessité, la transparence et l'exercice par la personne concernée de ses droits, autant de principes qui doivent tous être pris en compte lorsque l'on détermine si un pays tiers offre un niveau adéquat de protection.

Pays ayant conclu un accord bilatéral avec l'UE

86. L'analyse d'impact indique que ce traitement permettra à l'UE de mettre l'accent sur certains principeset d'assurer la cohérence dans le cadre de ces accords bilatéraux avec des pays tiers. Il donne aussi la possibilité de demander un traitement réciproque aux pays tiers avec lesquels l'UE a un accord, ce qui n'est pas possible à l'heure actuelle ([3]).

87. Ces remarques amènent à poser la question de l'incidence de la proposition sur les accords existants conclus avec le Canada et les États-Unis. Les conditions d'accès aux données prévues par ces accords sont en effet plus souples, ces données ne faisant pas l'objet d'une sélection similaire à celle envisagée en l'espèce avant d'être transmises à ces pays tiers.

88. L'analyse d'impact indique que, au cas où l'UE a conclu un accord international avec un pays tiers concernant l'échange et/ou la transmission de données PNR à ce pays tiers, il convient de tenir dûment compte de cet accord. Les transporteurs devraient envoyer les données PNR aux unités de renseignements passagers conformément à la pratique habituelle dans le cadre des dispositions en vigueur. L'unité de renseignements passagers qui reçoit ces données les transmet à l'autorité compétente du pays tiers avec lequel l'accord a été conclu ([4]).

89. Alors que la proposition semble prévoir *uniquement* la transmission de données *sélectionnées* à toute autorité compétente, au sein de l'UE ou en dehors de son territoire, l'analyse d'impact, le préambule de la proposition (considérant 21) et l'article 11 lui-même, quant à eux, rappellent qu'il convient de prendre dûment en considération les accords existants. On pourrait en conclure que le filtrage ne peut être une mesure valable que pour les accords à conclure à l'avenir. Il pourrait être prévu, dans cette perspective, que l'accès en masse reste la règle pour l'accès, par exemple, des autorités américaines aux données PNR, conformément aux dispositions de l'accord entre l'UE et les États-Unis, mais qu'en parallèle et au cas par cas, des données particulières définies par les unités de renseignements passagers, comprenant des données relatives aux vols à destination des États-Unis sans s'y limiter, pourraient être transmises aux États-Unis.

90. Le CEPD regrette le manque de clarté sur ce point déterminant de la proposition. Il estime qu'il est de la plus haute importance que les conditions de la transmission des données PNR à des pays tiers soient cohérentes et soumises à un niveau harmonisé de protection. En outre, pour des raisons de sécurité juridique, des précisions relatives aux garanties applicables à la transmission de données devraient figurer dans la proposition elle-même, et pas seulement dans l'analyse d'impact comme c'est le cas à l'heure actuelle.

([1]) Exposé des motifs de la proposition, point 2.
([2]) Analyse d'impact, point 5.2., «Protection de la vie privée».
([3]) Analyse d'impact, point 5.2., «Relations avec des pays tiers».
([4]) Annexe A de l'analyse d'impact, «Organismes recevant des données des unités de renseignements passagers».

VI. AUTRES POINTS IMPORTANTS

Traitement automatisé

91. Le CEPD note que la proposition prévoit expressément que les unités de renseignements passagers et les autorités compétentes des États membres s'abstiennent de toute action répressive sur la seule base du traitement automatisé des données PNR ou en raison de la race ou de l'origine ethnique de la personne, de ses convictions religieuses ou philosophiques, de ses opinions politiques ou de son orientation sexuelle ([1]).

92. Cette précision est la bienvenue car elle limite les risques de mesures arbitraires à l'encontre des personnes concernées. Le CEPD note cependant que sa portée est limitée à *l'action répressive* des unités de renseignements passagers ou des autorités compétentes. Dans son libellé actuel, le texte n'exclut pas le filtrage automatisé des personnes selon des profils types et n'empêche pas non plus la constitution automatisée de listes de suspects et l'instauration de mesures telles qu'une surveillance accrue, tant que ces mesures ne sont pas considérées comme des actions répressives.

93. Le CEPD considère que la notion d'*action répressive* est trop vague et que, par principe, *aucune décision* ne devrait être prise à l'égard de personnes sur la *seule* base du traitement automatisé des données les concernant ([2]). Le CEPD recommande de modifier le texte en conséquence.

Qualité des données

94. L'article 5, paragraphe 2, de la proposition fournit une précision importante puisqu'il explique que les transporteurs aériens ne sont aucunement tenus de collecter ou de conserver des données autres que celles recueillies initialement à des fins commerciales.

95. Plusieurs aspects du traitement de ces données méritent néanmoins de plus amples commentaires:

— les données qui doivent être mises à disposition, énumérées à l'annexe 1 de la proposition, sont très nombreuses, et leur liste est similaire à celle des données mises à la disposition des autorités américaines en vertu de l'accord entre l'UE et les États-Unis. Les autorités chargées de la protection des données, et en particulier le Groupe de l'article 29, ont déjà émis à plusieurs reprises des doutes concernant la qualité de certaines des données demandées ([3]).

— il semble ressortir du libellé de l'analyse d'impact ([4]) et de l'article 6, paragraphe 3, de la proposition que les données pourraient aussi être transmises en masse aux intermédiaires par les transporteurs aériens. Dans un premier temps, les données transmises à un tiers ne seraient même pas limitées conformément à la liste des données PNR figurant à l'annexe 1 de la proposition.

— en ce qui concerne le traitement des données sensibles, même s'il est possible de filtrer ces données au stade des intermédiaires, la question demeure de savoir si la transmission du champ libre par les transporteurs aériens est strictement nécessaire.

Le CEPD soutient les arguments avancés à cet égard dans l'avis du Groupe de l'article 29.

Moyens utilisés pour la transmission des données PNR

96. Les transporteurs aériens établis en dehors de l'UE sont invités à utiliser un système d'exportation («*push*») pour transmettre les données aux unités de renseignements passagers ou aux intermédiaires dans la mesure où ils possèdent l'infrastructure technique nécessaire à cet effet. Si ce n'est pas le cas, ils devront autoriser l'extraction des données par un système d'importation («*pull*»).

97. Permettre l'utilisation de différentes méthodes de communication des données en fonction des transporteurs aériens concernés ne fera qu'augmenter les difficultés relatives au contrôle de la conformité de la transmission des données PNR avec les règles de protection des données, et risque également d'entraîner une distorsion de concurrence entre les transporteurs aériens de l'UE et les autres.

98. Le CEPD rappelle que le système d'exportation («*push*») qui permet aux transporteurs aériens de garder le contrôle de la qualité des données transmises et des conditions de transmission, est la seule méthode acceptable en termes de proportionnalité du traitement. En outre, il doit s'agir d'une véritable exportation, c'est-à-dire que les données ne devraient pas être envoyées en masse à un intermédiaire, mais devraient être filtrées dès la toute première étape du traitement. Il n'est pas acceptable que des données non nécessaires — et des données ne figurant pas à l'annexe 1 de la proposition — soient envoyées à un tiers, même si ces données sont immédiatement effacées par ce tiers.

Conservation des données

99. L'article 9 de la proposition prévoit une période de conservation des données PNR de cinq ans, et une période supplémentaire de huit années durant laquelle les données doivent être conservées dans une base de données passive, qui sera accessible dans des conditions limitées.

([1]) Considérant 20 et article 3, paragraphes 3 et 5, de la proposition.

([2]) Voir à cet égard l'article 15, paragraphe 1, de la directive 95/46/CE. La directive interdit les décisions automatisées dans les cas où elles affecteraient la personne concernée. Eu égard au contexte de la proposition, les décisions prises dans un cadre répressif sont en tout état de cause susceptibles d'affecter de manière significative les personnes concernées. Le fait d'être soumis à de contrôles complémentaires peut affecter la personne concernée, en particulier si ces actions sont répétées.

([3]) Voir en particulier l'avis 5/2007 du 17 août 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, WP 138.

([4]) Annexe A de l'analyse d'impact, «Moyens utilisés pour la transmission des données par les transporteurs».

100. Le CEPD émet des doutes quant à la différence établie entre les deux types de base de données: rien ne garantit que la base de données passive constitue un véritable système d'archivage, avec des méthodes distinctes de conservation et d'extraction des données. En effet, la plupart des conditions fixées pour accéder à la base de données passive sont des exigences de sécurité qui pourraient tout aussi bien s'appliquer à la base de données utilisée pour conserver les données pendant cinq ans.

101. La durée totale de conservation — treize ans — est en tout état de cause excessive. Elle est justifiée dans l'analyse d'impact par la nécessité d'élaborer des indicateurs de risques et d'établir des modèles de déplacement et de comportement ([1]), dont l'efficacité reste à démontrer. S'il est évident que les données peuvent être conservées aussi longtemps que nécessaire dans un cas particulier et dans la mesure où une enquête est en cours, rien ne permet de justifier la conservation pendant treize ans des données concernant tous les passagers lorsqu'aucun soupçon ne pèse sur eux.

102. Le CEPD note en outre que les réponses des États membres au questionnaire de la Commission, selon lesquelles la durée moyenne de conservation requise serait de trois ans et demi, ne plaident pas en faveur de cette période de conservation ([2]).

103. Par ailleurs, la période de treize ans est comparable à la période de conservation de quinze ans qui est prévue par l'accord le plus récent conclu avec les États-Unis. Le CEPD a toujours considéré que cette longue période de conservation n'avait été adoptée qu'en raison de la forte pression exercée par le gouvernement américain pour disposer d'une période beaucoup plus longue que trois ans et demi, et non parce qu'elle avait été à un quelconque moment défendue par le Conseil ou la Commission. Il n'y a aucune raison de transposer un tel compromis — justifié uniquement par la nécessité de faire aboutir les négociations — dans un instrument juridique adopté par l'UE seule.

Rôle du comité des États membres

104. Le comité des États membres institué en vertu de l'article 14 de la proposition sera compétent pour les questions de sécurité, notamment les protocoles et le cryptage des données PNR, mais aussi pour formuler des recommandations concernant les critères généraux communs, les méthodes et les pratiques à appliquer à l'évaluation des risques.

105. Hormis ces indications, la proposition ne comprend aucun élément ni critère en ce qui concerne les conditions concrètes régissant le processus d'évaluation des risques ou le cadre dans lequel il s'inscrira. L'analyse d'impact indique que les critères retenus dépendront en dernier recours des renseignements détenus par chaque État membre, qui sont en constante évolution. L'évaluation des risques doit être effectuée en l'absence de normes uniformes en matière d'identification des suspects. On peut dès lors se demander dans quelle mesure le comité des États membres sera en mesure de jouer un rôle à cet égard.

Sécurité

106. La proposition détaille une série de mesures de sécurité ([3]) qui doivent être prises par les unités de renseignements passagers, les intermédiaires et d'autres autorités compétentes afin d'assurer la protection des données. Étant donné l'importance de la base de données et le caractère sensible du traitement, le CEPD estime que, outre les mesures envisagées, l'entité chargée du traitement des données devrait également être tenue de notifier officiellement toute violation de la sécurité.

107. Le CEPD a connaissance du projet visant à établir une telle procédure de notification dans le secteur des communications électroniques au niveau européen. Il conseille d'inclure une telle garantie dans la proposition examinée et se réfère à cet égard au système de notification en cas de violation de la sécurité mis en place aux États-Unis pour les administrations ([4]). Des incidents de sécurité peuvent en effet se produire dans tout domaine d'activité dans le secteur privé ou public, comme l'a prouvé la récente perte par l'administration britannique de la totalité d'une base de données à caractère personnel ([5]). Des bases de données à grande échelle comme celle envisagée dans la proposition seraient prioritaires pour bénéficier d'un tel système d'alerte.

Clause de réexamen et de caducité

108. Le CEPD note qu'un réexamen doit avoir lieu dans un délai de trois ans suivant l'entrée en vigueur de la décision-cadre, sur la base d'un rapport élaboré par la Commission. Il reconnaît que ce réexamen, réalisé sur la base des informations communiquées par les États membres, accordera une attention particulière aux garanties en matière de protection des données, et portera notamment sur la mise en oeuvre du système d'exportation («*push*»), la conservation des données et la qualité de l'évaluation des risques. Pour être exhaustif, ce réexamen devrait comprendre les résultats d'une analyse de données statistiques produites sur la base du traitement des données PNR. Ces statistiques devraient, outre les éléments mentionnés à l'article 18 de la proposition, comprendre des renseignements statistiques sur l'identification de personnes à haut risque tels que les critères utilisés pour cette identification et les résultats concrets de toute action répressive en découlant.

([1]) Annexe A de l'analyse d'impact, «Période de conservation des données».
([2]) Annexe B de l'analyse d'impact.
([3]) Article 12 de la proposition.
([4]) Voir en particulier les travaux de l'«Identity Theft Task Force» américaine (Task force sur le vol d'identité), http://www.idtheft.gov/
([5]) Voir le lien vers le site internet de la British HM Revenue and Customs (administration fiscale et douanière du Royaume-Uni), http://www.hmrc.gov.uk/childbenefit/update-faqs.htm Voir aussi l'adresse http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

109. Le CEPD a déjà insisté dans le présent avis sur l'absence d'éléments concrets établissant la nécessité du système proposé. Il estime cependant que, si la décision-cadre devait entrer en vigueur, elle devrait au moins être complétée par une clause de caducité. À la fin d'une période de trois ans, cette décision-cadre devrait être abrogée au cas où aucun élément ne viendrait justifier son maintien en vigueur.

Incidence sur d'autres instruments juridiques

110. Dans ses dispositions finales, la proposition fixe une condition à la poursuite de l'application des accords ou des arrangements bilatéraux ou multilatéraux en vigueur. Ces instruments ne peuvent s'appliquer que dans la mesure où ils sont compatibles avec la réalisation des objectifs de la proposition de décision-cadre.

111. Le CEPD s'interroge quant au champ d'application de cette disposition. Comme déjà indiqué au point V, dans la partie consacrée à la réciprocité, on ne voit pas bien quelle sera l'incidence de cette disposition sur le contenu des accords conclus avec des pays tiers, tels que l'accord avec les États-Unis. Par ailleurs, on ne voit pas bien non plus si cette disposition pourrait avoir une incidence sur les conditions d'application des instruments ayant un champ d'application plus large comme la Convention n° 108 du Conseil de l'Europe. Bien que cela semble improbable au vu des différences en termes de contextes institutionnels et d'acteurs concernés, tout risque de mauvaise interprétation devrait être évité et il devrait être précisé dans la proposition que celle-ci n'a pas d'incidence sur les instruments ayant un champ d'application plus large, notamment ceux ayant pour objet la protection des droits fondamentaux.

VII. **CONCLUSION**

112. Le CEPD souligne l'impact considérable de la proposition examinée en termes de protection des données. Il a concentré son analyse sur quatre questions essentielles que soulève la proposition, et il insiste sur le fait que les questions soulevées doivent être traitées de manière exhaustive. Dans son libellé actuel, la proposition n'est pas conforme aux droits fondamentaux, notamment à l'article 8 de la Charte des droits fondamentaux de l'Union, et ne devrait pas être adoptée.

113. Si les observations faites ci-dessus, en particulier concernant le critère de légitimité, devaient être suivies d'effet, certaines propositions rédactionnelles ont été faites dans le présent avis qui devraient être prises en compte par le législateur. Il est fait référence en particulier aux points 67, 73, 77, 80, 90, 93, 106, 109 et 111 du présent avis.

Légitimité des mesures proposées

114. Alors que l'objectif général de lutte contre le terrorisme et la criminalité organisée est en soi clair et légitime, l'objet central du traitement qu'il est prévu de mettre en œuvre ne semble pas suffisamment délimité et justifié.

115. Le CEPD est d'avis que les techniques consistant à évaluer les risques présentés par les personnes en recourant à des instruments de «data mining» et des modèles de comportement doivent faire l'objet d'une analyse plus approfondie, et qu'il convient d'en établir clairement l'utilité dans le cadre de la lutte contre le terrorisme, et ce, avant qu'elles soient utilisées à une échelle aussi grande.

116. Accumuler les bases de données sans disposer d'une vision globale des résultats concrets et des lacunes:

— est contraire à une politique législative rationnelle dans le cadre de laquelle il n'y a pas lieu d'adopter de nouveaux instruments tant que les instruments existants n'ont pas été pleinement mis en œuvre et que leur insuffisance n'a pas été démontrée,

— pourrait ouvrir la voie à une évolution vers une société de surveillance totale.

117. La lutte contre le terrorisme peut certainement constituer un motif légitime pour appliquer des exceptions aux droits fondamentaux à la vie privée et à la protection des données. Toutefois, pour être valable, la nécessité de l'ingérence doit s'appuyer sur des éléments clairs et indéniables, et la proportionnalité du traitement doit être démontrée. Cette exigence s'impose d'autant plus dans le cas d'une atteinte considérable à la vie privée des personnes concernées, comme celle que prévoit la proposition.

118. On ne peut que constater que la proposition ne contient aucun élément justificatif de ce type et que les tests de nécessité et de proportionnalité ne sont pas rencontrés.

119. Le CEPD insiste sur le caractère essentiel des critères de nécessité et de proportionnalité évoqués plus haut. Ils représentent une condition sine qua non à l'entrée en vigueur de la présente proposition.

Cadre juridique applicable

120. Le CEPD constate de graves lacunes en matière de sécurité juridique quant au régime de protection des données applicable aux différents acteurs intervenant dans le projet, et en particulier aux transporteurs aériens et aux autres acteurs relevant du premier pilier, qu'il s'agisse des règles fixées par la proposition, par la décision-cadre relative à la protection des données ou par la législation nationale mettant en œuvre la directive 95/46/CE. Le législateur devrait préciser exactement à quelle étape du traitement ces différentes règles s'appliqueront.

121. La tendance actuelle visant à contraindre des acteurs privés à coopérer systématiquement à des objectifs répressifs soulève la question du cadre qui, en matière de protection des données (premier ou troisième pilier), s'applique aux conditions d'une telle coopération: la question de savoir si les règles doivent se fonder sur la qualité du contrôleur des données (secteur privé) ou sur la finalité poursuivie (services répressifs) reste posée.

122. Le CEPD a déjà rappelé le risque de vide juridique entre les activités relevant du premier pilier et celles qui relèvent du troisième pilier ([1]). Il est difficile de déterminer si les activités effectuées par des entreprises privées, dans une perspective d'application du droit pénal, relèvent du champ d'action du législateur de l'Union européenne en vertu des articles 30, 31 et 34 du traité UE.

123. Il convient par conséquent d'éviter d'en arriver à ce que, selon la finalité poursuivie, le traitement de données par des prestataires de services soit régi par des cadres différents en matière de protection des données, en particulier eu égard aux difficultés que cela entraînerait en termes d'exercice de leurs droits par les personnes concernées.

Qualité des destinataires

124. La proposition ne donne aucune précision quant à la qualité des destinataires des données à caractère personnel collectées par les transporteurs aériens, qu'il s'agisse des intermédiaires, des unités de renseignements passagers ou des autorités compétentes.

125. La qualité du destinataire, qui pourrait dans certains cas être un acteur du secteur privé, est directement liée au type de garanties en matière de protection des données qui s'appliquent audit destinataire. Il est essentiel que le régime applicable soit clair pour tous les acteurs concernés, y compris le législateur, les autorités chargées de la protection des données, ainsi que les responsables du traitement des données et les personnes concernées.

Transfert de données à des pays tiers

126. Le CEPD souligne qu'il est nécessaire de veiller à ce qu'un niveau adéquat de protection soit assuré dans le pays destinataire. Il s'interroge également sur l'importance du principe de «réciprocité» visé dans la proposition et sur son application à des pays déjà liés par un accord avec l'UE, comme le Canada ou les États-Unis. Il estime qu'il est de la plus haute importance que les conditions de la transmission des données à des pays tiers soient cohérentes et soumises à un niveau harmonisé de protection.

Autres points importants

127. Le CEPD attire également l'attention du législateur sur certains aspects particuliers de la proposition qui doivent être précisés, ou qui doivent prendre davantage en compte les principes de protection des données. Il s'agit notamment des aspects suivants:

— il convient de limiter les conditions dans lesquelles des décisions automatisées peuvent être prises,

— la qualité des données traitées devrait être réduite,

— la méthode de transmission de données devrait uniquement se fonder sur le système d'exportation («*push*»),

— la période de conservation des données est jugée excessive et injustifiée,

— le rôle du comité des États membres pourrait être davantage précisé en ce qui concerne ses recommandations sur l'«évaluation des risques»,

— les mesures de sécurité devraient comprendre une procédure de «notification en cas de violation de la sécurité»,

— le réexamen de la décision devrait comprendre une clause de caducité,

— il devrait être précisé dans la proposition qu'elle n'a pas d'incidence sur les instruments ayant un champ d'application plus large et ayant notamment pour objet la protection des droits fondamentaux.

Remarques finales

128. Le CEPD note que la proposition examinée a été présentée à un moment où le cadre institutionnel de l'Union européenne est sur le point de connaître un changement fondamental. Les conséquences du traité de Lisbonne en termes de prise de décision seront décisives, en particulier en ce qui concerne le rôle du Parlement.

129. Étant donné l'incidence sans précédent de la proposition en termes de droits fondamentaux, le CEPD recommande de ne pas l'adopter dans le cadre du traité actuel mais de veiller à ce qu'elle soit adoptée selon la procédure de codécision prévue par le nouveau traité. Cela renforcerait les bases juridiques sur lesquelles les mesures déterminantes proposées seraient prises.

([1]) Voir l'avis 2007/C 255/01 du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données (JO C 255 du 27.10.2007, p. 1). Voir également le rapport annuel 2006, p. 47.