Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière

(2011/C 181/02)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 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 la demande d'avis formulée conformément à l'article 28, paragraphe 2, du règlement (CE) nº 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],

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

I.1. *Consultation du CEPD*

1. Le 2 février 2011, la Commission a adopté une proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (ci-après «la proposition») [3]. La proposition a été envoyée au CEPD pour consultation le même jour.

2. Le CEPD se félicite d'avoir été consulté par la Commission. Déjà avant l'adoption de la proposition, le CEPD avait eu la possibilité de présenter des observations informelles. Certaines de ces observations ont été prises en considération dans la proposition et le CEPD relève que dans l'ensemble, les garanties de protection des données ont été renforcées dans la proposition. Cependant, un certain nombre de points restent préoccupants, notamment en ce qui concerne l'ampleur et les finalités de la collecte des données à caractère personnel.

I.2. *La proposition dans son contexte*

3. Des discussions sur un possible système PNR à l'échelle de l'Union sont engagées depuis 2007, date à laquelle la Commission a adopté une proposition de décision-cadre du Conseil sur cette question [4]. Le principal objectif d'un système PNR au niveau de l'Union est la mise en place d'un système obligeant les transporteurs aériens assurant des vols internationaux entre l'UE et des pays tiers à transmettre aux autorités compétentes les données PNR de tous les passagers, afin de prévenir et de détecter les infractions terroristes et les formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière. Les données seraient centralisées et analysées par des unités de renseignements passagers et le résultat de l'analyse serait transmis aux autorités nationales compétentes de chaque État membre.

4. Depuis 2007, le CEPD suit de près les développements liés à un possible système PNR au niveau de l'Union, parallèlement aux développements concernant les systèmes PNR de pays tiers. Le 20 décembre 2007, le CEPD a adopté un avis sur cette proposition de la Commission [5]. À de nombreuses autres occasions, des observations concordantes ont été formulées, non seulement par le CEPD mais également par le groupe de travail «Article 29» [6], sur la question de la conformité du traitement des données PNR à des fins répressives avec les principes de nécessité et de proportionnalité ainsi qu'avec d'autres garanties essentielles en matière de protection des données.

5. Le principal aspect régulièrement soulevé par le CEPD porte sur la justification de la nécessité d'un système PNR européen qui viendrait s'ajouter à un certain nombre d'autres instruments autorisant le traitement de données à caractère personnel à des fins répressives.

6. Le CEPD reconnaît que des améliorations visibles sur le plan de la protection des données ont été apportées à la proposition actuelle, par rapport à la version sur laquelle il a déjà rendu un avis. Ces améliorations portent notamment sur le champ d'application de la proposition, la définition du rôle des différentes parties prenantes (unités de renseignements passagers), l'exclusion du traitement de données sensibles, l'adoption d'une méthode «push» sans période de transition [7] et la limitation de la période de conservation des données.

---

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM(2011) 32 final.
[4] COM(2007) 654 final.
[5] Avis du CEPD du 20 décembre 2007 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, JO C 110 du 1.5.2008, p. 1.
[6] — Avis du 19 octobre 2010 sur la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, disponible à l'adresse http://www.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC/OC2010
— Les avis du groupe de travail «Article 29» peuvent être consultés en cliquant sur le lien suivant: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers
[7] Ce qui signifie que les données PNR sont activement transmises par les compagnies aériennes, et non extraites (méthode «pull») par les autorités publiques en accédant directement à la base de données des compagnies aériennes.

7. Le CEPD se félicite également des éléments supplémentaires inclus dans l'analyse d'impact sur la justification d'un système PNR au niveau de l'Union. Cependant, alors qu'il existe une volonté claire d'expliquer la nécessité du système, le CEPD ne trouve toujours dans ces nouvelles justifications aucun motif probant pour développer le système, notamment en ce qui concerne «l'information préalable» à grande échelle de tous les passagers. La nécessité et la proportionnalité seront analysées ci-dessous au chapitre II. Le chapitre III portera sur des aspects plus spécifiques de la proposition.

II. **NÉCESSITÉ ET PROPORTIONNALITÉ DE LA PROPOSITION**

II.1. *Observations préliminaires sur la nécessité et la proportionnalité*

8. La démonstration de la nécessité et de la proportionnalité du traitement de données est un préalable indispensable au développement du système PNR. Dans le passé, le CEPD a déjà insisté, notamment dans le contexte de la révision possible de la directive 2006/24/CE (ci-après la «directive relative à la conservation des données»), sur le fait que la nécessité de traiter ou de stocker d'énormes quantités de données doit s'appuyer sur une démonstration claire de la relation entre *l'utilisation* et le *résultat*, et permettre l'évaluation *sine qua non* de la possibilité d'obtenir des résultats comparables avec d'autres moyens, plus respectueux de la vie privée ([1]).

9. En vue de justifier le système, la proposition, et notamment son analyse d'impact, comprennent une documentation complète et des arguments juridiques afin d'établir, d'une part, que le système est nécessaire et, d'autre part, qu'il est conforme aux exigences en matière de protection des données. Elle va même encore plus loin en énonçant qu'elle apporte de la valeur ajoutée sur le plan de l'harmonisation des normes en matière de protection des données.

10. Après avoir analysé ces éléments, le CEPD considère que la proposition dans sa version actuelle ne satisfait *pas* aux exigences de nécessité et de proportionnalité imposées par l'article 8 de la Charte des droits fondamentaux de l'Union, l'article 8 de la CEDH et l'article 16 TFUE. Le raisonnement qui sous-tend cette observation est développé dans les paragraphes suivants.

II.2. *Documents et statistiques communiqués par la Commission*

11. Le CEPD constate que l'analyse d'impact comprend d'abondantes explications et statistiques visant à justifier la proposition. Ces éléments ne sont cependant pas convaincants. À titre d'exemple, la description de la menace du terrorisme et des formes graves de criminalité dans l'analyse d'impact ainsi que dans l'exposé des motifs de la proposition ([2]) cite le nombre de 14 000 infractions pénales par tranche de 100 000 habitants dans les États membres en 2007. Si ce chiffre peut paraître impressionnant, il concerne en fait des types de criminalité non différenciés et ne peut en aucune façon contribuer à justifier une proposition qui ne cible et ne combat qu'un type limité de criminalité grave et transnationale et de terrorisme. Prenons un autre exemple: le fait de citer un rapport sur les «problèmes» de drogue sans lier les statistiques au type de trafic de stupéfiants concerné par la proposition ne constitue pas selon le CEPD une référence valable. Il en est de même pour les indications des conséquences de la criminalité, qui citent la «valeur du patrimoine volé» et l'impact physique et émotionnel sur les victimes, alors qu'il ne s'agit pas de données directement liées à l'objet de la proposition.

12. Un dernier exemple: l'analyse d'impact indique que la Belgique a «signalé que 95 % de toutes les saisies de drogues en 2009 étaient exclusivement ou essentiellement consécutives au traitement des données PNR». Il convient cependant de souligner que la Belgique n'a pas (encore) mis en place de projet PNR systématique, comparable à celui que prévoit la proposition. Les données PNR pourraient donc être utiles dans des cas bien précis, ce que le CEPD ne conteste pas. C'est plutôt la collecte à grande échelle aux fins d'une évaluation systématique de tous les passagers qui soulève de sérieuses préoccupations en matière de protection des données.

13. Le CEPD considère que les documents de référence ne sont pas suffisamment pertinents et précis pour démontrer la nécessité de l'instrument.

II.3. *Conditions pour limiter un droit fondamental*

14. Si le document établit le lien entre les mesures de traitement des données et la Charte, la CEDH et l'article 16 TFUE, il mentionne directement les limitations possibles de ces droits et adhère à la conclusion selon laquelle «les mesures proposées étant destinées à lutter contre le terrorisme et d'autres infractions graves, contenues dans un acte législatif, elles respecteraient manifestement de telles exigences à condition qu'elles soient nécessaires dans une société démocratique et sous réserve du respect du principe de proportionnalité» ([3]). Cependant, une démonstration claire de la nécessité des mesures et de l'absence d'autres solutions moins intrusives fait défaut.

15. En ce sens, le fait que des finalités supplémentaires telles que l'application de la loi en matière d'immigration, la «no-flight list» et la sécurité sanitaire ont été envisagées et n'ont finalement pas été incluses pour des raisons de proportionnalité ne signifie pas que la «limitation» du traitement des données PNR aux infractions terroristes et autres formes graves de criminalité soit de fait proportionnée car moins invasive. L'option consistant à limiter le système à la lutte contre le terrorisme, sans inclure d'infractions supplémentaires, comme envisagé dans de précédents systèmes PNR, et notamment dans le précédent système PNR australien,

([1]) Voir «Le moment de vérité pour la directive sur la conservation des données», discours de Peter Hustinx prononcé à la conférence «Taking on the Data Retention Directive», Bruxelles, le 3 décembre 2010, disponible à l'adresse http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_FR.pdf

([2]) Analyse d'impact, chapitre 2.1.1, et exposé des motifs, chapitre 1, premier paragraphe.

([3]) Analyse d'impact, chapitre 3.2, deuxième paragraphe.

n'a pas non plus été envisagée. Le CEPD souligne que dans ce système antérieur, sur lequel le groupe de travail «Article 29» a adopté un avis positif en 2004, les finalités étaient limitées à «[l'identification] des passagers susceptibles de représenter une menace de terrorisme ou d'activité criminelle connexe» ([1]). Le système australien ne prévoyait pas non plus de conserver les données PNR à l'exception de celles concernant certains passagers, identifiés comme présentant une menace spécifique ([2]).

16. En outre, en ce qui concerne la prévisibilité de la surveillance pour les personnes concernées, on peut douter que la proposition de la Commission satisfasse aux exigences d'une base juridique solide conformément au droit de l'Union: l'«évaluation» des passagers («évaluation des risques» dans la version précédente) sera réalisée sur la base de critères non transparents et en constante évolution. Comme cela est explicitement mentionné dans le texte, le principal objet du système n'est pas le traditionnel contrôle aux frontières, mais plutôt le renseignement en matière criminelle ([3]) et l'arrestation de personnes qui ne sont pas des suspects, avant qu'une infraction ait été commise. Le développement d'un tel système à l'échelle européenne, impliquant la collecte des données de tous les passagers et la prise de décisions sur la base de critères d'évaluation inconnus et qui évoluent, suscite de sérieuses préoccupations en matière de transparence et de proportionnalité.

17. Selon le CEPD, la seule finalité qui serait conforme aux exigences de transparence et de proportionnalité serait l'utilisation des données PNR au cas par cas, comme indiqué à l'article 4, paragraphe 2, point c), mais uniquement quand survient une menace réelle et sérieuse appuyée par des indicateurs concrets.

II.4. *Le risque de détournement d'usage*

18. L'article 4, paragraphe 2, point b), dispose que les unités de renseignements passagers peuvent procéder à l'évaluation du risque que représentent les passagers et, ce faisant, confronter les données PNR aux «bases de données pertinentes». Cette disposition n'indique pas quelles sont les bases de données pertinentes. La mesure n'est donc pas prévisible, alors qu'il s'agit d'une condition prévue dans la Charte et la CEDH. Cette disposition soulève également la question de sa compatibilité avec le principe de limitation de la finalité: selon le CEPD, elle devrait par exemple être exclue pour une base de données telle qu'Eurodac qui a été développée pour des finalités différentes ([4]). En outre, elle ne devrait être envisagée qu'en cas de besoin spécifique, dans une situation particulière où il existe une suspicion préexistante concernant une personne après qu'une infraction a été commise. Par exemple, la confrontation systématique de la base de données du système d'information sur les visas ([5]) avec les données PNR serait excessive et disproportionnée.

II.5. *La valeur ajoutée de la proposition sur le plan de la protection des données*

19. L'idée selon laquelle la proposition améliorerait la protection des données en offrant des conditions égales en ce qui concerne les droits des personnes est critiquable. Le CEPD reconnaît le fait que, si la nécessité et la proportionnalité du système étaient établies, des normes uniformes à travers l'Union, y compris en matière de protection des données, amélioreraient la sécurité juridique. Cependant, le libellé actuel de la proposition, au considérant 28, mentionne que «la présente directive ne porte pas atteinte à la possibilité offerte aux États membres de prévoir, en vertu de leur législation nationale, un système de collecte et de traitement des données PNR à des fins autres que celles visées dans la présente directive, ou de collecter, auprès de transporteurs autres que ceux que la directive mentionne, des données relatives à des vols intérieurs (…)».

20. L'harmonisation apportée par la proposition est donc limitée. Elle peut concerner les droits des personnes concernées, mais non la limitation des finalités, et on peut supposer que selon ce libellé, les systèmes PNR déjà utilisés pour lutter par exemple contre l'immigration illégale pourraient poursuivre cette lutte conformément à la directive.

21. Cela signifie, d'une part, que des différences subsisteraient entre les États membres ayant déjà développé un système PNR, et, d'autre part, que la grande majorité des États membres qui ne collectent pas systématiquement de données PNR (21 sur 27 États membres) y seront contraints. Le CEPD estime que sous cet angle, toute valeur ajoutée sur le plan de la protection des données est très contestable.

([1]) Avis 1/2004 du 16 janvier 2004 sur le niveau de protection assuré en Australie à la transmission de données des dossiers passagers par les compagnies aériennes, WP85.

([2]) L'avis du groupe de travail «article 29» explique également que «[e]n ce qui concerne la conservation des données PNR, il n'existe pas d'obligation juridique en ce sens pour les douanes. La législation n'interdit pas non plus aux douanes de stocker ces données. Les données PNR des passagers considérés comme présentant un risque peu élevé par le logiciel d'analyse automatisée de profil (95 % à 97 % du total) ne sont pas stockées et aucune trace de ces informations n'est conservée. La politique générale appliquée par les douanes consiste donc à ne pas garder ces données. Dans le cas des 0,05 % à 0,1 % de passagers signalés aux douanes pour une évaluation complémentaire, les données PNR des compagnies aériennes sont temporairement conservées — mais pas stockées — en attendant l'issue de l'évaluation à la frontière. Après celle-ci, les données PNR sont effacées du PC du fonctionnaire de la PAU concerné et ne sont pas introduites dans des bases de données australiennes».

([3]) Exposé des motifs, chapitre 1. Contexte de la proposition, cohérence avec les autres politiques et objectifs de l'Union.

([4]) L'objet d'Eurodac «est de contribuer à déterminer l'État membre qui, en vertu de la convention de Dublin, est responsable de l'examen d'une demande d'asile présentée dans un État membre et de faciliter à d'autres égards l'application de la convention de Dublin dans les conditions prévues dans le présent règlement», en vertu de l'article premier, paragraphe 1, du règlement (CE) nº 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, JO L 316 du 15.12.2000, p 1.

([5]) «Le VIS a pour objet d'améliorer la mise en œuvre de la politique commune en matière de visas, la coopération consulaire et la consultation des autorités consulaires centrales chargées des visas en facilitant l'échange de données entre les États membres sur les demandes de visas et les décisions y relatives», en vertu de l'article 2 du règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), JO L 218 du 13.8.2008, p. 60.

22. Les conséquences du considérant 28 constituent au contraire une grave violation du principe de limitation de la finalité. Selon le CEPD, la proposition devrait explicitement prévoir que les données PNR ne peuvent pas être utilisées pour d'autres finalités.

23. Le CEPD parvient à une conclusion similaire à celle tirée de l'évaluation de la directive sur la conservation des données: dans les deux contextes, l'absence d'harmonisation réelle va de pair avec l'absence de sécurité juridique. En outre, la collecte et le traitement supplémentaires de données à caractère personnel deviennent obligatoires pour l'ensemble des États membres, alors que la nécessité réelle du système n'a pas été démontrée.

II.6. *Lien avec la communication sur la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice*

24. Le CEPD constate également que les développements du système PNR sont liés à l'évaluation générale en cours de l'ensemble des instruments de l'UE dans le domaine de la gestion de l'échange d'informations, lancée par la Commission en janvier 2010 et développée dans la récente communication sur la présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice ([1]). Notamment, un lien est clairement établi avec le débat actuel sur la stratégie européenne relative à la gestion de l'information. Le CEPD considère à cet égard que les résultats des travaux actuels sur le modèle européen d'échange d'informations, dont la publication est prévue pour 2012, devraient être pris en considération dans l'évaluation de la nécessité d'un système PNR à l'échelle de l'Union.

25. Dans ce contexte, et eu égard aux faiblesses de la proposition et notamment de son analyse d'impact, le CEPD estime qu'une analyse d'impact de la protection des données et de la vie privée est nécessaire dans des cas comme celui-ci, où le contenu de la proposition concerne les droits fondamentaux à la vie privée et à la protection des données. Une analyse d'impact générale ne suffit pas.

III. OBSERVATIONS PARTICULIERES

III.1. *Champ d'application*

26. Les infractions terroristes, les infractions graves et les infractions transnationales graves sont définies à l'article 2, points g), h) et i) de la proposition. Le CEPD se félicite du fait que les définitions — et leur champ d'application— aient été affinées et qu'une distinction ait été établie entre les infractions graves et les infractions transnationales graves. Cette distinction est appréciée, surtout parce qu'elle implique un traitement différent des données à caractère personnel, excluant une évaluation au regard de critères préétablis lorsqu'il s'agit d'infractions graves qui ne sont pas transnationales.

27. La définition d'infractions graves reste cependant trop large selon le CEPD. La proposition le reconnaît et indique que les États membres ont toujours la possibilité d'exclure les *infractions mineures* relevant de la définition d'infractions graves ([2]) mais pour lesquelles le traitement de données PNR ne serait pas conforme au principe de proportionnalité. Ce libellé laisse entendre que la définition prévue dans la proposition pourrait aussi bien inclure des infractions mineures, dont le traitement serait disproportionné. Ce que les infractions mineures devraient couvrir n'est pas clairement défini. Au lieu de laisser aux États membres la possibilité de limiter le champ d'application, le CEPD considère que la proposition devrait explicitement énumérer les infractions qui devraient être incluses dans son champ d'application, et celles qui devraient être exclues étant donné qu'elles devraient être considérées comme mineures et ne satisfont pas au critère de la proportionnalité.

28. Il en est de même pour la possibilité laissée à l'article 5, paragraphe 5, de traiter des données liées à tout type d'infraction détectée lors d'actions répressives, ainsi que la possibilité mentionnée au considérant (28) d'étendre le champ d'application à d'autres fins que celles visées dans la proposition, ou à d'autres transporteurs.

29. Le CEPD est également préoccupé par la possibilité visée à l'article 17 d'inclure les vols internes dans le champ d'application de la directive, compte tenu de l'expérience acquise par les États membres qui recueillent déjà des données PNR relatives à des vols internes. Un tel élargissement du champ d'application du système PNR menacerait de manière encore plus importante les droits fondamentaux des personnes et ne devrait pas être envisagé avant d'effectuer une analyse correcte comprenant une analyse d'impact détaillée.

30. Pour conclure, le fait de laisser le champ d'application ouvert et de donner aux États membres la possibilité d'étendre les finalités est contraire à l'exigence selon laquelle les données ne peuvent être collectées que pour des finalités spécifiées et explicites.

III.2. *Unités de renseignements passagers*

31. Le rôle des unités de renseignements passagers et les garanties qui entourent le traitement des données PNR soulèvent des questions spécifiques, notamment compte tenu du fait que les unités de renseignements passagers reçoivent les données de tous les passagers qui leur sont communiquées par les transporteurs aériens et qu'elles sont dotées — en vertu du texte de la proposition — de compétences larges pour traiter ces données. Ce rôle comprend l'évaluation du comportement de passagers qui ne sont suspectés d'aucune infraction et la possibilité de recouper des données PNR avec des bases de données indéterminées ([3]). Le CEPD constate que la proposition prévoit des conditions «d'accès restrictif», mais considère que ces conditions ne suffisent pas à elles seules, étant donné l'ampleur des compétences des unités de renseignements passagers.

32. En premier lieu, la nature de l'autorité désignée en tant qu'unité de renseignements passagers et sa composition ne sont pas clairement établies. La proposition mentionne la possibilité que des membres du personnel puissent être «détachés par les autorités publiques compétentes», mais

([1]) COM(2010) 385 final.

([2]) Comme indiqué dans les décisions-cadres 2008/841/JAI et 2002/584/JAI du Conseil.

([3]) Voir également l'avis du CEPD du 20 décembre 2007 concernant les unités de renseignements passagers.

n'offre aucune garantie concernant la compétence et l'intégrité du personnel de l'unité de renseignements passagers. Le CEPD recommande d'inclure de telles garanties dans le texte de la directive, lesquelles doivent tenir compte du caractère sensible du traitement qui doit être réalisé par les unités de renseignements passagers.

33. En deuxième lieu, la proposition mentionne la possibilité de désigner une unité de renseignements passagers pour plusieurs États membres. Cela ouvre la voie à des risques d'utilisation abusive et de transmission de données en dehors des conditions de la proposition. Le CEPD reconnaît que certains États, notamment les plus petits, peuvent trouver des avantages à allier leurs forces, mais recommande tout de même d'assortir cette possibilité de conditions. Celles-ci devraient tenir compte de la coopération avec les autorités compétentes et de la surveillance, notamment en ce qui concerne l'autorité de protection des données chargée de la supervision et l'exercice des droits de la personne concernée, étant donné que plusieurs autorités peuvent être compétentes pour superviser une unité de renseignements passagers.

34. Il existe un risque de détournement d'usage lié aux éléments susmentionnés, notamment compte tenu de la qualité du personnel compétent pour analyser les données et du «partage» d'une unité de renseignements passagers entre plusieurs États membres.

35. En troisième lieu, le CEPD émet des doutes quant aux garanties prévues contre les abus. Les obligations d'enregistrement sont appréciées mais insuffisantes. L'autocontrôle devrait être complété par un contrôle externe plus structuré. Le CEPD suggère que des audits soient organisés systématiquement, tous les quatre ans. Un ensemble complet de règles de sécurité devrait être élaboré et imposé horizontalement à toutes les unités de renseignements passagers.

III.3. *Échange de données entre États membres*

36. L'article 7 de la proposition envisage plusieurs scénarios autorisant l'échange de données entre unités de renseignements passagers — ceci étant la situation normale — ou entre les autorités compétentes d'un État membre et des unités de renseignements passagers dans des circonstances exceptionnelles. Les conditions sont également plus strictes selon qu'un accès est demandé à la base de données visée à l'article 9, paragraphe 1, dans laquelle les données sont conservées les 30 premiers jours, ou à la base de données mentionnée à l'article 9, paragraphe 2, dans laquelle les données sont conservées pendant cinq ans.

37. Les conditions d'accès sont définies de manière plus stricte lorsque la demande d'accès va au-delà de la procédure normale. Le CEPD relève cependant que le libellé utilisé prête à confusion: l'article 7, paragraphe 2, est applicable dans un «cas précis de prévention ou de détection d'infractions terroristes ou d'infractions graves ou d'enquêtes ou de poursuites en la matière»; l'article 7, paragraphe 3, mentionne «des circonstances exceptionnelles, afin de réagir à une menace spécifique ou dans le cadre d'une enquête ou de poursuites spécifiques concernant des infractions terroristes ou des infractions graves», tandis que l'article 7, paragraphe 4, concerne «une menace immédiate et grave à la sécurité publique», et que l'article 7, paragraphe 5, mentionne une «menace spécifique et réelle ayant trait à des infractions terroristes ou à des infractions graves». Les conditions d'accès par différentes parties prenantes aux bases de données varient en fonction de ces critères. Cependant, la différence entre une menace spécifique, une menace immédiate et grave et une menace spécifique et réelle n'est pas clairement établie. Le CEPD souligne la nécessité de préciser davantage les conditions dans lesquelles les transferts de données seront autorisés.

III.4. *Droit applicable*

38. La proposition mentionne, comme base juridique générale des principes de protection de données, la décision-cadre 2008/977/JAI du Conseil, et étend son champ d'application au traitement de données au niveau national.

39. Le CEPD a déjà souligné en 2007 [1] les lacunes de la décision-cadre en ce qui concerne les droits des personnes concernées. Parmi les éléments qui font défaut dans la décision-cadre, citons par exemple des conditions régissant l'information de la personne concernée en cas de demande d'accès aux données la concernant: les informations devraient être communiquées sous une forme intelligible, la finalité du traitement devrait être indiquée, et les garanties devraient être renforcées en cas de recours à l'autorité chargée de la protection des données dans l'éventualité où un accès direct est refusé.

40. La référence à la décision-cadre a également des conséquences en ce qui concerne l'identification de l'autorité chargée de la protection des données, compétente pour contrôler l'application de la future directive, étant donné qu'il ne s'agit pas nécessairement de la même APD que celle qui est compétente pour les questions concernant (l'ancien) premier pilier. Le CEPD estime qu'il est insatisfaisant d'invoquer uniquement la décision-cadre dans le contexte de l'après-Lisbonne, alors que l'un des principaux objectifs est d'adapter le cadre juridique pour garantir un niveau de protection élevé et harmonisé entre les (anciens) piliers. Il considère que des dispositions supplémentaires doivent être intégrées dans la proposition afin de compléter la référence à la décision-cadre du Conseil, dans laquelle des lacunes ont été décelées, notamment en ce qui concerne les conditions d'accès aux données à caractère personnel.

41. Ces préoccupations valent également pour les dispositions concernant les transferts de données à des pays tiers. La proposition mentionne l'article 13, paragraphe 3, point ii), de la décision-cadre, qui prévoit de larges exceptions aux garanties de protection des données: elle déroge notamment à la condition de caractère adéquat lorsque «des intérêts légitimes prévalent, en particulier des intérêts publics importants». Cette exception est formulée en des termes très vagues et pourrait s'appliquer potentiellement à de nombreux cas de traitement de données PNR, en cas d'interprétation large. Le CEPD estime que la proposition devrait explicitement empêcher l'application des exceptions de la décision-cadre dans le contexte du traitement des données PNR, et maintenir la condition d'une analyse stricte du caractère adéquat.

[1] Troisième avis du Contrôleur européen de la protection des données du 27 avril 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, JO C 139 du 23.6.2007, p. 1.

III.5. *Conservation des données*

42. La proposition prévoit une période de 30 jours de conservation, ainsi qu'une période supplémentaire de cinq ans dans les archives. Cette durée de conservation des données a été considérablement diminuée par rapport aux versions précédentes du document, dans lesquelles les périodes de conservation allaient jusqu'à cinq ans et huit ans.

43. Le CEPD approuve la réduction de la première période de conservation à 30 jours. Il conteste cependant la période de conservation supplémentaire de cinq ans: selon lui, la la nécessité de conserver ultérieurement ces données sous une forme permettant toujours d'identifier les personnes concernées n'apparait pas clairement.

44. Il relève également un problème de terminologie dans le texte, qui a d'importantes conséquences juridiques: l'article 9, paragraphe 2, indique que les données PNR seront «masquées», et qu'elles seront donc «anonymisées». Cependant, le texte mentionne plus bas qu'il est toujours possible d'accéder à «l'intégralité des données PNR». Si cela est possible, cela signifie que les données PNR n'ont jamais été totalement anonymisées: tout en étant masquées, elles demeurent identifiables. Le cadre de protection des données reste par conséquent pleinement applicable, ce qui soulève la question fondamentale de la nécessité et de la proportionnalité quant à la conservation de données identifiables de tous les passagers pour une durée de cinq ans.

45. Le CEPD recommande que la proposition soit reformulée, en conservant le principe d'anonymisation réelle, sans qu'il soit possible de revenir à des données identifiables, ce qui signifie qu'aucune enquête rétroactive ne devrait être autorisée. Ces données pourraient toujours — et uniquement — être utilisées afin de servir des intérêts de renseignements généraux basés sur l'identification de types de terrorisme et d'infractions connexes dans les flux migratoires. Cette condition devrait être différenciée de la conservation de données sous une forme identifiable — sous réserve de certaines garanties — dans des cas ayant donné lieu à des suspicions concrètes.

III.6. *Liste de données PNR*

46. Le CEPD se réjouit du fait que les données sensibles ne soient pas incluses dans la liste des données à traiter. Il souligne cependant que la proposition prévoit toujours la possibilité que ces données soient envoyées à l'unité de renseignements passagers, qui a ensuite l'obligation de les effacer (article 4, paragraphe 1, et article 11). Ce libellé ne permet pas de savoir au juste si les unités de renseignements passagers ont toujours une obligation d'effacer les données sensibles envoyées par les compagnies aériennes, ou si elles doivent effacer ces données uniquement dans le cas exceptionnel où les compagnies aériennes les auraient envoyées par erreur. Le CEPD recommande que le texte soit modifié afin d'établir clairement qu'aucune donnée sensible ne devrait être envoyée par les compagnies aériennes, à la source même du traitement de données.

47. Hormis les données sensibles, la liste de données qui peuvent faire l'objet de transferts reflète dans une large mesure la liste PNR des États-Unis, qualifiée de trop large dans plusieurs avis du groupe de travail «Article 29» [1]. Le CEPD considère que cette liste devrait être limitée conformément à l'avis du groupe de travail, et que tout ajout devrait être dûment justifié. C'est notamment le cas du champ «remarques générales», qui devrait être exclu de la liste.

III.7. *Décisions individuelles automatisées*

48. Selon l'article 4, paragraphe 2, points a) et b), l'évaluation du risque représenté par les passagers au regard de critères préétablis ou de bases de données pertinentes peut comprendre un traitement automatisé mais qui doit être contrôlé individuellement par des moyens non automatisés.

49. Le CEPD se félicite des clarifications apportées dans cette nouvelle version du texte. Le caractère ambigu du précédent champ d'application de la disposition, concernant des décisions automatisées produisant «un effet juridique *négatif* sur une personne ou *l'affectant* considérablement (…)» a été remplacé par une formulation plus explicite. Il est désormais clair que toute correspondance positive sera examinée individuellement.

50. Il est également clairement établi dans la nouvelle version qu'en aucun cas une évaluation ne peut être fondée sur la race ou l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, son état de santé ou sa vie sexuelle. En d'autres termes, le CEPD comprend d'après ce nouveau libellé qu'aucune décision ne peut être prise, même en partie, sur la base de données sensibles. Cette disposition cadre avec celle prévoyant qu'aucune donnée sensible ne peut être traitée par des unités de renseignements passagers et devrait également être considérée comme bienvenue.

III.8. *Réexamen et données statistiques*

51. Le CEPD considère qu'il est de la plus haute importance qu'une évaluation complète de la mise en œuvre de la directive soit réalisée, comme prévu à l'article 17. Il estime que le réexamen devrait non seulement permettre d'évaluer le respect général des normes de protection des données, mais plus fondamentalement et spécifiquement d'évaluer si les systèmes PNR constituent une mesure nécessaire. Les données statistiques mentionnées à l'article 18 jouent un rôle important à cet égard. Le CEPD considère que ces informations devraient inclure le nombre d'actions répressives, comme le prévoit le projet, mais également le nombre de condamnations effectives qui en ont résulté ou non. Ces données sont indispensables pour que le résultat de l'évaluation soit concluant.

III.9. *Relation avec d'autres instruments*

52. La proposition s'applique sans préjudice d'accords existants avec des pays tiers (article 19). Le CEPD estime que cette disposition devrait mentionner plus explicitement l'objectif d'un cadre global prévoyant des garanties harmonisées de protection des données dans le domaine des données PNR, au sein de l'UE et en dehors de ses frontières, comme

[1] Avis du 23 juin 2003 sur le niveau de protection assuré aux États-Unis pour la transmission de données passagers, WP78. Cet avis ainsi que les avis ultérieurs du groupe de travail sur cette question sont disponibles à l'adresse: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

demandé par le Parlement européen et explicité par la Commission dans sa communication du 21 septembre 2010 relative à «la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers».

53. En ce sens, les accords avec les pays tiers ne devraient pas inclure de dispositions en deçà du seuil de protection des données de la directive. Cette condition revêt une importance particulière au moment où les accords avec les États-Unis, l'Australie et le Canada sont renégociés dans la perspective d'un cadre global et harmonisé.

IV. **CONCLUSION**

54. La mise en place d'un système PNR à l'échelon de l'Union, ainsi que la négociation d'accords PNR avec des pays tiers, est un projet de longue haleine. Le CEPD reconnaît que, par rapport à la proposition de décision-cadre du Conseil de 2007 relative à l'utilisation des données des dossiers passagers, des améliorations visibles ont été apportées au projet de texte. Des garanties de protection des données ont été ajoutées, sur la base des débats et avis de différentes parties prenantes et notamment du groupe de travail «Article 29», du CEPD et du Parlement européen.

55. Le CEPD se félicite de ces améliorations et plus particulièrement des efforts visant à limiter le champ d'application de la proposition et les conditions de traitement des données PNR. Cependant, force est de constater que la condition préalable indispensable à tout développement d'un système PNR — à savoir le respect des principes de nécessité et de proportionnalité — n'est pas satisfaite dans la proposition. Le CEPD rappelle que selon lui, les données PNR pourraient certainement être nécessaires à des fins répressives dans des cas *bien déterminés* et être utilisées de façon conforme aux exigences en matière de protection des données. C'est leur utilisation de façon systématique et sans discernement pour tous les passagers qui soulève des préoccupations particulières.

56. L'analyse d'impact fournit des éléments visant à justifier la nécessité des données PNR pour lutter contre la criminalité, mais la nature de ces informations est trop générale et ne parvient pas à étayer le traitement à grande échelle des données PNR à des fins de renseignement. Selon le CEPD, la seule mesure conforme aux exigences en matière de protection des données serait l'utilisation des données PNR au cas par cas, quand survient une menace sérieuse accompagnée par des indicateurs concrets.

57. Au-delà de cette lacune majeure, les observations du CEPD concernent les aspects suivants:

— le champ d'application devrait être beaucoup plus limité compte tenu du type d'infractions concernées. Le CEPD émet des doutes quant à l'inclusion dans la proposition de formes graves de criminalité n'ayant aucun lien avec le terrorisme. En tout état de cause, les infractions mineures devraient être explicitement circonscrites et écartées. Le CEPD recommande d'exclure la possibilité pour les États membres d'élargir le champ d'application;

— la nature des différentes menaces autorisant l'échange de données entre unités de renseignements passagers ou avec les États membres n'a pas été suffisamment définie;

— les principes de protection des données applicables ne devraient pas uniquement se fonder sur la décision-cadre 2008/977/JAI du Conseil qui comprend des lacunes, notamment au niveau des droits des personnes concernées et des transferts à des pays tiers. Un niveau plus élevé de garanties, basé sur les principes de la directive 95/46/CE, devrait être introduit dans la proposition;

— aucune donnée ne devrait être conservée au-delà de 30 jours sous une forme identifiable, sauf dans les cas nécessitant une enquête plus approfondie;

— la liste des données PNR à traiter devrait être restreinte, conformément aux recommandations formulées préalablement par le groupe de travail «Article 29» et le CEPD. Notamment, le champ «remarques générales» ne devrait pas être inclus;

— l'évaluation de la directive devrait être fondée sur des données exhaustives, incluant le nombre de personnes effectivement condamnées — et pas seulement poursuivies — sur la base du traitement de leurs données.

58. Le CEPD recommande également que les développements relatifs à un système PNR au niveau de l'Union soient évalués dans une perspective plus large, incluant l'évaluation générale actuelle de l'ensemble des instruments européens dans le domaine de la gestion de l'échange de l'information mise en œuvre par la Commission en janvier 2010. En particulier, les résultats des travaux actuels sur le modèle européen d'échange d'informations, dont la publication est prévue pour 2012, devraient être pris en considération lors de l'évaluation de la nécessité d'un système PNR à l'échelle de l'Union.

Fait à Bruxelles, le 25 mars 2011.

Peter HUSTINX

Contrôleur européen de la protection des données