

## I

(Résolutions, recommandations, orientations et avis)

## AVIS

## CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

### Troisième avis du contrôleur européen de la protection des données 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

(2007/C 139/01)

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 <sup>(1)</sup>,

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 <sup>(2)</sup>, et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

#### I. INTRODUCTION

1. Le 19 décembre 2005 et le 29 novembre 2006, le CEPD a émis deux avis <sup>(3)</sup> sur la proposition, présentée par la Commission, 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. Dans ces avis, le contrôleur a souligné l'importance que revêt la proposition en tant qu'instrument efficace capable de garantir la protection des données à caractère personnel dans le domaine visé par le titre VI du traité UE. Il a en particulier fait part, dans son deuxième avis, de la préoccupation que lui inspire l'évolution des négociations, qui mène à un niveau de protection des données à caractère personnel non seulement inférieur à celui offert par la directive 95/46/CE, mais également incompatible avec celui offert par la convention 108 du Conseil de l'Europe formulée en termes plus généraux <sup>(4)</sup>.
2. En janvier 2007, la présidence allemande a défini un ensemble de points essentiels en vue de réexaminer la proposition afin de lever les réserves existant encore et améliorer la protection des données dans le cadre du troisième pilier <sup>(5)</sup>. Le projet de proposition révisé <sup>(6)</sup> a été présenté au Parlement européen le 13 avril 2007 pour une deuxième consultation.

<sup>(1)</sup> JO L 281 du 23.11.1995, p. 31.

<sup>(2)</sup> JO L 8 du 12.1.2001, p. 1.

<sup>(3)</sup> Le premier avis est paru au JO C 47 du 25.2.2006, p. 27; le deuxième est disponible sur le site web du CEPD ([www.edps.europa.eu](http://www.edps.europa.eu)).

<sup>(4)</sup> 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.

<sup>(5)</sup> Doc. 5435/07 du 18 janvier 2007, disponible à l'adresse suivante: [register.consilium.europa.eu](http://register.consilium.europa.eu)

<sup>(6)</sup> Doc. 7315/07 du 13 mars 2007, disponible à l'adresse suivante: [register.consilium.europa.eu](http://register.consilium.europa.eu)

3. Les modifications considérables apportées à la proposition révisée, ainsi que son importance, justifient un nouvel avis du CEPD. Celui-ci portera essentiellement sur les préoccupations majeures du CEPD et ne reviendra pas sur tous les éléments avancés dans les avis précédents, qui restent valables pour la proposition révisée.

## II. NOUVEL ÉLAN DONNÉ PAR LA PRÉSIDENTE ALLEMANDE

4. Le CEPD se félicite des efforts importants déployés par la présidence allemande dans le cadre des négociations concernant la décision-cadre du Conseil. Il est bien connu que les négociations étaient bloquées au Conseil à cause de différences de point de vue fondamentales entre les États membres sur des questions essentielles. La présidence a donc pris une sage décision en relançant ces négociations sur la base d'un texte nouveau.
5. Le fait que la présidence allemande ait donné un nouvel élan aux négociations est très positif en soi. Toutefois, après un examen approfondi de la dernière version du texte, le CEPD est déçu par le contenu, le texte soumis par la présidence allemande n'étant pas à la hauteur des attentes, et ce pour les raisons suivantes:
  - ce texte diminue le niveau de protection offert au citoyen, plusieurs dispositions essentielles à cet égard, qui figuraient dans la proposition de la Commission, ayant en effet été supprimées,
  - à bien des égards, la proposition révisée offre même un niveau de protection inférieur à celui offert par la convention 108, ce qui la rend non seulement insatisfaisante, mais en outre incompatible avec les obligations internationales des États membres,
  - le texte rend ce dossier encore plus complexe, vu qu'il couvre les données traitées par Europol, Eurojust et le système d'information douanier du troisième pilier, et qu'il ouvre le débat sur le contrôle de ces organes. Le présent avis examinera notamment si une décision-cadre du Conseil est bien l'instrument juridique qui convient pour ces questions,
  - la qualité législative du texte n'est pas satisfaisante. Outre le choix de l'instrument juridique, plusieurs dispositions ne répondent pas aux exigences fixées par les lignes directrices communes relatives à la qualité rédactionnelle de la législation communautaire <sup>(7)</sup>. En particulier, le texte n'est pas formulé d'une manière claire, simple et précise, ce qui empêche le citoyen d'identifier exactement ses droits et ses obligations,
  - le faible niveau de protection offert par la proposition ne saurait répondre aux besoins de la création d'un espace de liberté, de sécurité et de justice à l'intérieur duquel les autorités policières et judiciaires pourraient échanger des informations en matière répressive sans tenir compte des frontières nationales. En effet, la proposition ne prévoyant pas un niveau de protection des données élevé et largement applicable, les échanges d'informations restent soumis aux différentes «règles d'origine» et aux «deux poids, deux mesures» qui nuisent considérablement à la coopération en matière répressive sans toutefois améliorer la protection des données à caractère personnel <sup>(8)</sup>.
6. Le CEPD est conscient qu'il est difficile de recueillir l'unanimité au Conseil. Toutefois, la procédure de prise de décision ne saurait justifier une approche favorisant le plus petit commun dénominateur, qui porterait atteinte aux droits fondamentaux des citoyens de l'UE et entraverait l'efficacité des services répressifs. Dans ce contexte, il serait souhaitable de prendre pleinement en compte l'expertise dans le domaine de la protection des données et d'intégrer comme il se doit les recommandations que le Parlement européen a formulées dans ses résolutions <sup>(9)</sup>.

<sup>(7)</sup> Accord interinstitutionnel du 22 décembre 1998 sur les lignes directrices communes relatives à la qualité rédactionnelle de la législation communautaire (JO C 73 du 17.3.1999, p. 1). Des exemples figurent dans le chapitre V du présent avis.

<sup>(8)</sup> Par exemple, l'article 14 «Transfert aux autorités compétentes de pays tiers ou à des instances internationales»; l'article 12, paragraphe 1, point d), sur le traitement ultérieur des données à caractère personnel; l'article 10 relatif au respect des délais d'effacement et de vérification; et l'article 13 ayant trait au respect des restrictions de traitement nationales.

<sup>(9)</sup> Le Parlement européen a adopté sa première résolution sur la proposition initiale de la Commission le 27 septembre 2006. Une deuxième résolution, concernant la proposition révisée, devrait être adoptée en juin.

## III. CADRE JURIDIQUE ET PRINCIPAUX THÈMES DU PRÉSENT AVIS

7. Une décision-cadre sur la protection des données à caractère personnel dans le cadre du troisième pilier est un élément fondamental de l'élaboration d'un espace de liberté, de sécurité et de justice. L'importance croissante de la coopération policière et judiciaire en matière pénale ainsi que les actions découlant du programme de La Haye <sup>(10)</sup> ont souligné la nécessité de disposer de normes communes de protection des données à caractère personnel dans le cadre du troisième pilier.
8. Malheureusement, comme le CEPD et d'autres acteurs concernés <sup>(11)</sup> l'ont à maintes reprises fait remarquer, les instruments existant actuellement au niveau européen sont insuffisants. La convention 108 du Conseil de l'Europe, qui est contraignante pour les États membres, définit des principes fondamentaux généraux en matière de protection des données, mais, bien qu'il faille l'interpréter à la lumière de la jurisprudence de la Cour européenne des Droits de l'Homme, elle n'offre pas le degré de précision nécessaire, comme le CEPD l'a indiqué à plusieurs reprises <sup>(12)</sup>. La directive 95/46/CE, qui intègre et précise les principes de la convention 108 en ce qui concerne le marché intérieur, a été adoptée dès 1995. Cette directive ne s'applique pas aux actions qui relèvent du troisième pilier. Pour les actions relevant du domaine de la coopération policière et judiciaire, tous les États membres ont souscrit à la recommandation n° R (87) 15 <sup>(13)</sup>, qui, dans une certaine mesure, désigne la convention 108 pour le secteur de la police. Mais il ne s'agit pas d'un instrument contraignant.
9. Dans ce contexte, l'article 30, paragraphe 1, point b), du traité UE dispose que les actions communes dans le domaine de la coopération policière impliquant le traitement d'informations par les services répressifs ont lieu «sous réserve des dispositions appropriées relatives à la protection des données à caractère personnel». Or en l'absence d'une décision-cadre du Conseil présentant un contenu satisfaisant, de telles dispositions n'existent pas.
10. On peut aisément faire le parallèle avec la mise en place du marché intérieur, où un niveau de protection élevé des données à caractère personnel dans l'ensemble de la Communauté a été considéré comme un élément essentiel pour venir à bout des obstacles à la libre circulation des biens, des services, des capitaux et des personnes, et a mené à l'adoption de la directive 95/46/CE. Par analogie, un espace de liberté, de sécurité et de justice où les informations sont censées circuler librement entre les services répressifs, tant au niveau national qu'au niveau de l'UE, requiert une protection élevée et uniforme des données à caractère personnel dans tous les États membres.
11. Ces considérations contrastent avec la situation actuelle, où il n'existe aucun cadre général de ce type et où les dispositions relatives à la protection des données à caractère personnel dans le cadre du troisième pilier sont liées au secteur concerné et inscrites dans divers instruments juridiques <sup>(14)</sup>. Certaines propositions récentes <sup>(15)</sup> confirment et soulignent la dispersion actuelle des dispositions en matière de protection des données dans ce domaine et mettent en danger leur cohérence. En outre, l'absence de cadre général nuit à l'adoption rapide de nombreuses propositions dans le domaine de la coopération policière et judiciaire.
12. Au vu de ce qui précède, le CEPD a fermement soutenu la proposition de la Commission dans ses avis précédents et a formulé des recommandations appropriées en vue d'améliorer cette proposition, qui était nécessaire pour assurer un niveau adéquat de protection du citoyen. Le CEPD a constamment soutenu qu'un cadre général pour la protection des données dans le cadre du troisième pilier devait garantir un niveau de protection des données élevé et cohérent, en s'appuyant sur des principes en matière de protection des données énoncés dans la convention 108 et la directive 95/46/CE, tout en tenant compte, le cas échéant, des particularités propres aux activités répressives.
13. Il importe d'autant plus d'assurer la cohérence de ce cadre général avec les principes de protection des données existant dans le cadre du premier pilier dans un contexte où la participation accrue du secteur privé implique que les données à caractère personnel transitent du premier au troisième pilier (comme

<sup>(10)</sup> Voir également le plan d'action du Conseil et de la Commission mettant en œuvre le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne (JO C 198 du 12.8.2005, p. 1).

<sup>(11)</sup> La Conférence des autorités européennes de protection des données a émis un avis le 24 janvier 2006, disponible sous la cote n° 6329/06 sur [register.consilium.europa.eu](http://register.consilium.europa.eu). Le Comité consultatif du Conseil de l'Europe sur la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) adoptée le 20 mars 2007 un document soulignant ses remarques initiales, disponible à l'adresse: [www.coe.int/dataprotection/](http://www.coe.int/dataprotection/)

<sup>(12)</sup> Voir, plus récemment, le point 60 de l'avis du CEPD du 4 avril 2007 sur l'initiative de quinze États membres en vue d'adopter une décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière.

<sup>(13)</sup> Recommandation n° R (87) 15 du Comité des ministres du Conseil de l'Europe aux États membres relative à l'utilisation de données à caractère personnel dans le domaine policier, adoptée le 17 septembre 1987 et disponible sur: [www.coe.int/dataprotection/](http://www.coe.int/dataprotection/)

<sup>(14)</sup> Tels les instruments juridiques régissant Europol, Eurojust, et le Système d'information douanier dans le cadre du troisième pilier.

<sup>(15)</sup> Telles les initiatives récentes concernant Europol, le traité de Prüm et l'accès des services répressifs à la base de données VIS.

dans le cas des dossiers des passagers aériens) ou vice versa. Il est facile de trouver des exemples pertinents: l'utilisation de listes des personnes interdites d'embarquement à bord d'aéronefs («no fly lists») établies dans un but répressif par des compagnies aériennes pour des finalités relevant du premier pilier (objectifs commerciaux et sécurité à bord des avions), ainsi que le proposition concernant l'accès des services répressifs à la base de données VIS, établie comme instrument d'une politique commune en matière de visas <sup>(16)</sup>. C'est pourquoi le CEPD insiste sur le fait que les principes de protection des données dans le cadre du premier pilier doivent également s'appliquer au troisième pilier. Cependant, les spécificités des activités répressives peuvent justifier la nécessité de dispositions supplémentaires ou exceptionnelles <sup>(17)</sup>.

14. Des garanties en matière de protection des données dans le cadre du troisième pilier, qui soient appropriées, cohérentes et généralement applicables, sont essentielles, non seulement pour assurer le respect du droit fondamental à la protection des données à caractère personnel des personnes physiques, mais aussi pour améliorer l'efficacité de la coopération en matière répressive au sein d'un espace de liberté, de sécurité et de justice.
15. Dans ce contexte, le présent avis évalue dans quelle mesure la proposition révisée actuelle établit des dispositions appropriées concernant la protection des données à caractère personnel, conformément à l'article 30, paragraphe 1, point b), du traité UE. Ce faisant, le CEPD mentionnera certaines recommandations formulées dans ses avis précédents. Le présent avis étudiera également la question de savoir si la proposition révisée respecte les obligations internationales imposées aux États membres par la convention 108 du Conseil de l'Europe et la jurisprudence de la Cour européenne des Droits de l'Homme, ainsi que les principes énoncés dans la recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Le CEPD se penchera par ailleurs sur la question de savoir dans quelle mesure les dispositions prévues par la proposition influenceraient l'efficacité de la coopération policière et judiciaire.

#### IV. PRINCIPALES PRÉOCCUPATIONS

##### IV.1. Applicabilité au traitement national des données à caractère personnel

16. La proposition inclut à présent un considérant précisant que les États membres appliquent au traitement des données au niveau national les dispositions contenues dans la décision-cadre, de manière à ce que les conditions nécessaires à leur transmission puissent être réunies dès la collecte des données (considérant 6 bis). Ce considérant tente de répondre aux préoccupations formulées non seulement par le CEPD dans ses avis précédents, mais aussi par de nombreuses autres parties prenantes. En effet, le Parlement européen, la Conférence des autorités européennes de protection des données, et même le Comité consultatif T-PD du Conseil de l'Europe — composé des représentants des gouvernements européens chargés de la protection des données — ont tous clairement indiqué à diverses reprises que l'applicabilité de la décision-cadre au traitement national des données est une condition essentielle afin, non seulement, d'assurer un niveau de protection suffisant des données à caractère personnel, mais aussi de permettre une collaboration efficace entre les services répressifs <sup>(18)</sup>.
17. Cependant, en tant que tel, ce considérant ne peut imposer une obligation qui n'est pas explicitement énoncée dans les dispositions. Malheureusement, l'article premier — «objectif et champ d'application» — limite explicitement l'applicabilité de la proposition aux données échangées entre États membres ou organes de l'UE, en garantissant «*que les droits et libertés fondamentaux, en particulier la vie privée de la personne concernée, [soient] suffisamment protégés, lorsque des données à caractère personnel sont transmises [...]*».
18. Par conséquent, le projet actuel laisse les États membres libres d'appliquer les principes uniformes en matière de protection des données au traitement national des données à caractère personnel et ne les contraint pas à mettre en œuvre des niveaux identiques de protection des données, tout cela dans un espace de coopération policière et judiciaire où les frontières intérieures doivent être supprimées. À cet égard, le CEPD souligne une fois de plus que la possibilité d'avoir différents niveaux de protection des données dans différents États membres dans le cadre du troisième pilier:
  - serait incompatible avec la création d'un espace de liberté, de sécurité et de justice au sein duquel les citoyens se déplacent librement et avec un rapprochement approprié des législations conformément à l'article 34, paragraphe 2, point b), du traité UE,
  - ne serait pas appropriée pour la protection des données à caractère personnel, au vu de l'article 30, paragraphe 1, point b), du traité UE,

<sup>(16)</sup> Voir 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].

<sup>(17)</sup> Dans le même esprit, voir également l'exposé des motifs de la recommandation n° R (87) 15, paragraphe 37.

<sup>(18)</sup> Voir les documents mentionnés dans la note en bas de page 9.

— serait inefficace et irréaliste pour les services répressifs, dont le travail serait entravé par des distinctions ingérables entre données nationales et données transmises ou accessibles aux fins de leur transmission, qui dans la plupart des cas feront partie d'un même dossier <sup>(19)</sup>.

19. Le CEPD conseille vivement au législateur d'étendre le champ d'application, en obligeant — et non en se contentant d'inviter — les États membres à appliquer la décision-cadre au traitement national des données à caractère personnel. De plus, il n'y a pas d'arguments juridiques étayant le point de vue selon lequel l'application aux données nationales ne serait pas permise en vertu de l'article 34 du traité UE.

#### IV.2. Limitation des autres finalités auxquelles les données à caractère personnel peuvent être traitées

20. Le principe de limitation de la finalité est l'un des principes de base de la protection des données. La convention 108 précise notamment que les données à caractère personnel sont «*enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités*» [article 5, point b)]. Les exceptions à ce principe ne sont autorisées que dans la mesure où elles sont prévues par la loi et constituent une mesure nécessaire dans une société démocratique, entre autres, «*à la répression des infractions pénales*» (article 9). La jurisprudence de la Cour européenne des Droits de l'Homme a clairement établi que de telles exceptions devaient être proportionnées, précises et prévisibles, conformément à l'article 8, paragraphe 2, de la Convention européenne des Droits de l'Homme <sup>(20)</sup>.
21. Dans la proposition actuelle, les dispositions concernant la limitation de la finalité sont énoncées à la fois à l'article 3 et à l'article 12. L'article 3 autorise le traitement ultérieur à des fins compatibles avec celles pour lesquelles les données ont été collectées, et est donc, à cet égard, conforme aux principes de base de la protection des données.
22. Toutefois, l'article 3 est bien trop large et ne couvre pas une limitation appropriée de la finalité en vue de l'enregistrement, également requise par l'article 5, point b), de la convention 108 susmentionnée. La référence générale aux finalités du titre VI du traité UE ne saurait être considérée comme des finalités spécifiques et légitimes. Les finalités de la coopération policière et judiciaire ne sont pas légitimes par nature <sup>(21)</sup>, et elles ne sont certainement pas précisées.
23. L'article 3 ne prévoit aucune exception qui serait admise en vertu de l'article 9 de la convention 108. Cependant, l'article 12 de la proposition définit une série importante, un peu floue, d'exceptions au principe de limitation de la finalité dans le cas de données à caractère personnel transmises ou mises à disposition par un autre État membre. Notamment, la condition selon laquelle des exceptions sont nécessaires n'est pas expressément indiquée dans cet article. De plus, il n'est pas clair quelles sont les «*autres procédures [...] administratives*» aux fins desquelles l'article 12, paragraphe 1, point b), autorise le traitement de données à caractère personnel collectées et transmises pour une finalité différente. En outre, l'article 12, paragraphe 1, point d), autorise le traitement «*pour toute autre finalité*», à la seule condition que l'autorité compétente qui a transmis les données à caractère personnel donne son consentement. À cet égard, il convient de noter que, quelles que soient les circonstances, le consentement de l'autorité qui a transmis les données ne saurait remplacer le consentement de la personne concernée, pas plus qu'il n'apporte le fondement juridique permettant de déroger au principe de limitation de la finalité. Par conséquent, le CEPD souhaiterait souligner qu'une exception aussi large et ouverte ne répond pas aux exigences de base en matière de protection adéquate des données, et contredit même les principes de base de la convention 108. Il recommande dès lors au législateur de reformuler les dispositions concernées.
24. Une dernière remarque concerne l'article 12, paragraphe 2, qui prévoit la possibilité que des décisions du Conseil relevant du troisième pilier prévalent sur le paragraphe 1 dans le cas où des conditions appropriées sont prévues pour le traitement de données à caractère personnel. Le CEPD note que le libellé de ce paragraphe est très général et qu'il ne rend pas compte de la nature de la décision-cadre du Conseil en tant que *lex generalis* pour la coopération policière et judiciaire. Cette *lex generalis* devrait s'appliquer à tous les types de traitement de données à caractère personnel dans ce domaine.
25. Le CEPD est d'avis que les dispositions actuelles concernant le traitement ultérieur des données à caractère personnel influent sur le principe fondamental de limitation de la finalité et qu'elles offrent même un niveau de protection inférieur au niveau existant prévu par la convention 108. Par conséquent, le CEPD recommande au législateur de reformuler les dispositions concernées à la lumière des règles internationales existantes en matière de protection des données et de la jurisprudence établie en la matière.

<sup>(19)</sup> Pour un raisonnement plus détaillé à ce sujet, voir les paragraphes 11 à 13 du deuxième avis du CEPD.

<sup>(20)</sup> L'affaire la plus explicite dans la jurisprudence consolidée dans ce domaine est l'affaire Rotaru contre Roumanie.

<sup>(21)</sup> Il ne suffit pas de partir du point de vue que dans toutes les circonstances et dans tous les cas la police opère dans les limites de ses obligations légales.

#### IV.3. Protection adéquate lors de l'échange de données à caractère personnel avec des pays tiers

26. La convention 108 traite également des transferts de données à caractère personnel à des pays tiers. Le protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données énonce le principe général — assorti de certaines dérogations — selon lequel le transfert de données à caractère personnel n'est autorisé que si cette partie « assure un niveau de protection adéquat pour le transfert considéré ». Le principe de « protection adéquate » a été mis en œuvre et énoncé dans divers instruments juridiques de l'Union européenne relatifs à la protection des données, qui relèvent non seulement du premier pilier, comme la directive 95/46/CE <sup>(22)</sup>, mais également du troisième pilier comme les instruments juridiques portant création d'Europol et d'Eurojust.
27. Le considérant 12 de l'actuelle proposition stipule qu'en cas de transfert de données à caractère personnel vers des pays tiers ou des instances internationales, « ces données devraient, en principe, bénéficier d'un niveau de protection suffisant ». Par ailleurs, l'article 14 autorise que des données à caractère personnel transmises par un autre État membre soient transférées à des États tiers ou des instances internationales dès lors que l'autorité qui a transmis ces données a autorisé leur transfert dans le respect de sa législation nationale. Par conséquent, les dispositions de la proposition n'instaurent aucune nécessité de protection adéquate et ne prévoient aucun critère commun ou mécanisme afin d'évaluer le caractère adéquat du niveau de protection. En d'autres termes, l'évaluation du caractère adéquat du niveau de protection fourni par l'État tiers ou par l'instance internationale est laissée à la discrétion de chaque État membre. Par conséquent, la liste des pays et des instances internationales ayant un niveau de protection adéquat — vers lesquels un transfert est autorisé — variera considérablement d'un État membre à l'autre.
28. Ce cadre juridique ferait également obstacle à la coopération policière et judiciaire. En effet, lorsqu'ils statueront sur une demande de dossier formulée par un État tiers, les services répressifs d'un État membre ne devront pas seulement examiner le niveau de protection du pays en question, mais vérifier également si chacun des autres États membres (jusqu'à 26) ayant participé à l'établissement du dossier a donné ou non son accord, conformément à sa propre évaluation du caractère adéquat du niveau de protection du pays tiers en question.
29. À cet égard, l'article 27 de la proposition consacré au lien avec les conventions avec des États tiers, ajoute à la confusion en indiquant que cette décision-cadre ne préjuge pas des obligations et des engagements des États membres ou de l'Union européenne qui sont inscrits dans des conventions bilatérales et/ou multilatérales avec des États tiers. Selon le CEPD, cette disposition devrait être clairement limitée aux accords existants et stipuler que les accords futurs devront être conformes aux dispositions de la proposition en question.
30. Le CEPD estime que les dispositions actuelles sur le transfert de données à caractère personnel vers des pays tiers et des instances internationales ne permettent pas de protéger les données à caractère personnel et sont impossibles à mettre en œuvre pour les services répressifs. Par conséquent, le CEPD rappelle <sup>(23)</sup> qu'il est nécessaire d'assurer un niveau de protection adéquat lorsque des données à caractère personnel sont transférées à des pays tiers ou à des organisations internationales et qu'il est essentiel de mettre en place 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. Le même avis a été exprimé auparavant par le Parlement européen et par le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) du Conseil de l'Europe.

#### IV.4. Qualité des données

31. L'article 5 de la convention 108 énonce les principes visant à assurer la qualité des données à caractère personnel. D'autres instruments non contraignants, tels que la recommandation n° R (87) 15 et ses trois évaluations effectuées jusqu'à présent, fournissent des détails supplémentaires à ce sujet.
32. Si l'on compare l'actuelle proposition avec les instruments susmentionnés, il apparaît clairement que d'importantes garanties, dont certaines avaient été prévues dans la proposition de la Commission, font défaut dans la version révisée de cette proposition.
- L'article 3 de la proposition ne permet pas de garantir que les données sont obtenues et traitées *loyalement*, ainsi que l'exige l'article 5 de la convention 108.

<sup>(22)</sup> En ce qui concerne ce point, il convient de noter que la Commission a récemment déclaré, dans sa *Communication du 7 mars 2007 relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données* que les dispositions de la directive 95/46/CE, relatives aux transferts de données à caractère personnel aux États tiers sont dans l'ensemble adéquates et ne nécessitent pas de modifications.

<sup>(23)</sup> Voir les préoccupations déjà manifestées dans le premier avis (point IV.8) et dans le second avis (points 22 et 23) du CEPD.

- La proposition ne comprend plus aucune disposition prescrivant — comme l'exige le principe 3.2 de la recommandation n° R (87) 15 — que les différentes catégories de données soient différenciées en fonction de leur *degré d'exactitude* et de fiabilité et que les données fondées sur des faits soient différenciées de celles fondées sur des opinions ou appréciations personnelles <sup>(24)</sup>. Dans la pratique, l'absence d'une telle exigence commune risque de porter atteinte aux données échangées entre les services de police étant donné que ceux-ci ne seront pas en mesure de déterminer s'il convient de considérer ces données comme des «preuves», des «faits», des «renseignements confirmés» ou «des renseignements non confirmés». Ceci risque non seulement de nuire aux opérations de sécurité et à la collecte de renseignements, mais également de rendre l'obtention d'une condamnation plus difficile pour les tribunaux.
  - Il n'y a aucune *distinction entre les différentes catégories de personnes concernées* (criminels, suspects, victimes, témoins, etc.) ni de garanties spécifiques pour les données relatives aux personnes non suspectes, contrairement au principe 2 de la recommandation n° R (87) 15 et à ses rapports d'évaluation <sup>(25)</sup>. Ici encore, ces distinctions ne sont pas seulement nécessaires pour protéger les données à caractère personnel des citoyens, mais également pour permettre aux destinataires de ces données de les utiliser pleinement. Sans ces distinctions, les services de police qui reçoivent les données ne peuvent les utiliser immédiatement, mais doivent d'abord déterminer la qualification de ces données ainsi que la manière dont elles peuvent être utilisées et échangées à diverses fins répressives.
  - La vérification régulière prévue à l'article 6 ne permet pas de *vérifier régulièrement la qualité des données* et n'assure pas l'élimination des données superflues ou inadaptées des dossiers de police, ni leur mise à jour, ainsi que l'exige la recommandation n° R (87) 15 <sup>(26)</sup>. L'importance d'une telle vérification pour la protection des données est évidente, mais il convient une fois de plus de rappeler que ceci est également essentiel au fonctionnement efficace des services de police. Inutiles dans le meilleur des cas, les informations obsolètes et périmées peuvent, dans le pire des cas, détourner des ressources destinées à des priorités actuelles vers des sujets qui ne sont pas et ne devraient pas être au centre des enquêtes.
  - Si des données à caractère personnel — communiquées par un autre État membre — s'avèrent inexactes, il n'existe pas d'obligation ni de mécanisme pour assurer leur *rectification dans l'État membre d'origine*. Une fois de plus, la question de l'exactitude des données est vitale pour le fonctionnement efficace des autorités policières et judiciaires. Si la qualité des données ne peut être garantie, ceci nuira à l'utilité du transfert de données en tant qu'instrument de lutte contre la criminalité transfrontière.
33. Dans ce contexte, le CEPD estime que les dispositions relatives à la qualité des données de la proposition en question ne sont ni appropriées ni complètes — compte tenu notamment de la recommandation n° R (87) 15 à laquelle ont souscrit tous les États membres — et sont inférieures au niveau de protection requis par la convention 108. Il est également utile de rappeler une fois de plus que l'exactitude des données à caractère personnel est utile tant au regard de la répression que pour la protection de l'individu <sup>(27)</sup>.

#### IV.5. Échange de données à caractère personnel avec des autorités non compétentes et des personnes privées

34. Selon le principe 5 (Communication de données) de la recommandation n° R (87) 15, la communication de données à caractère personnel par des services de police à d'autres organes publics ou à des personnes privées ne devrait être permise qu'à des conditions strictes et spécifiques. De telles dispositions, énoncées dans la proposition initiale de la Commission et saluées par le CEPD et le Parlement européen, sont désormais supprimées de la version révisée de la proposition. Le nouveau texte ne prévoit donc aucune garantie spécifique pour les transferts de données à caractère personnel à des personnes privées ou à des autorités autres que des services répressifs.

<sup>(24)</sup> Le point 52 de l'exposé des motifs de la recommandation indique que «[On a estimé] possible d'établir une distinction entre les données corroborées et celles qui ne le sont pas (par exemple, des appréciations relatives à des comportements), entre des faits et des opinions, entre des informations fiables (à différents degrés) et des suppositions, entre des motifs raisonnables de supposer que des informations sont exactes et une croyance sans fondement en leur exactitude.» Voir également la deuxième évaluation de la pertinence de la recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (1998), point 5.1.

<sup>(25)</sup> Voir notamment le point 5.2 de la deuxième évaluation mentionnée ci-dessus, ainsi que les points 24 à 27 de la troisième évaluation de la recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (2002).

<sup>(26)</sup> Voir le principe 7 de la recommandation (Durée de conservation et mise à jour des données) et les points 96 à 98 de l'exposé des motifs.

<sup>(27)</sup> Point 74 de l'exposé des motifs de la recommandation n° R (87) 15.

35. En outre, l'accès des services répressifs aux données à caractère personnel contrôlées par des personnes privées et leur utilisation ultérieure par ces services ne sont autorisés que sur la base de conditions et de limitations bien définies. En particulier, ainsi que le CEPD l'a déjà mentionné dans ses avis antérieurs, l'accès des services répressifs n'est permis qu'au cas par cas, dans des conditions et à des fins spécifiques, et s'effectue sous contrôle judiciaire dans les États membres. De nouveaux éléments, tels que la directive 2006/24/CE <sup>(28)</sup> sur la conservation des données, l'accord PNR avec les États-Unis <sup>(29)</sup> et l'accès des services répressifs aux données détenues par la SWIFT <sup>(30)</sup>, confirment l'importance fondamentale de ces garanties. Il est regrettable que la proposition actuelle ne fournisse aucune garantie spécifique sur l'accès des services répressifs aux données à caractère personnel collectées par des personnes privées et sur leur utilisation ultérieure par ces services.
36. À ce propos, le CEPD constate qu'en ce qui concerne l'échange de données à caractère personnel avec des personnes privées et des autorités non compétentes, la proposition actuelle ne respecte pas les principes de la recommandation n° R (87) 15 et n'aborde pas la question fondamentale de l'accès des services répressifs aux données à caractère personnel contrôlées par des personnes privées et de leur utilisation ultérieure par ces services.

#### IV.6. Autres points importants

37. En dehors des principaux sujets de préoccupation susmentionnés, le CEPD souhaite attirer l'attention du législateur sur les points qui figurent ci-après et qui, pour la plupart, ont été traités de manière plus détaillée dans ses avis antérieurs:
- **Catégories particulières de données.** L'article 7 de la proposition révisée contredit l'interdiction de principe énoncée par l'article 6 de la convention 108. En outre, il ne fait pas référence aux données à caractère personnel liées à des condamnations pénales, lesquelles sont à l'évidence très importantes dans le cadre de la coopération policière et judiciaire et ne fournit aucune garantie spécifique en ce qui concerne les données biométriques et les profils ADN.
  - **Décisions individuelles automatisées.** Le CEPD constate avec satisfaction que l'article 8 intègre cette disposition dans la proposition révisée.
  - **Journalisation et enregistrement d'une trace documentaire.** L'article 11, en vue d'être efficace à des fins de vérification de la licéité du traitement des données, énonce des mécanismes appropriés pour la journalisation et l'enregistrement d'une trace documentaire non seulement de toutes les transmissions de données, mais également de *tous les accès* aux données.
  - **Droit d'être informé.** L'article 16 est incomplet, étant donné qu'il ne fournit aucune information sur l'identité des contrôleurs et des destinataires. En outre, le considérant 13 («[...] il peut être nécessaire d'informer la personne concernée») présente cette information comme une simple possibilité et non comme une obligation fondamentale du contrôleur.
  - **Droit d'accès.** L'article 17 est incomplet, puisque le droit d'accès comprend également des informations sur les *finalités* du traitement ainsi que la communication des données sous une *forme intelligible*. En outre, les exceptions énoncées au paragraphe 2 — tel que le cas où l'accès porterait atteinte aux intérêts nationaux — sont trop larges et imprévisibles. Enfin, il n'existe pas de mécanisme assurant que le recours auprès de l'autorité de contrôle débouche sur l'obtention du droit d'accès, lorsque celui-ci a été refusé de manière illicite.

#### V. NOUVELLES QUESTIONS SOULEVÉES PAR LA PROPOSITION RÉVISÉE

38. La proposition révisée comprend un élément entièrement nouveau par rapport à la proposition de la Commission. Elle s'étend aux activités des institutions et organes européens du troisième pilier (article 1<sup>er</sup>, paragraphe 2, de la proposition). Selon le considérant 20, ceci comprend le traitement de données par Europol, Eurojust et par le Système d'information douanier du troisième pilier. L'article 1<sup>er</sup>, paragraphe 2, ne mentionne pas seulement les organes européens, mais aussi les institutions, ce qui

<sup>(28)</sup> 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).

<sup>(29)</sup> 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 (JO L 298 du 27.10.2006, p. 29).

<sup>(30)</sup> Voir l'avis 10/2006 sur le traitement des données à caractère personnel par la Society for Worldwide Interbank Financial Telecommunication (SWIFT), qu'a rendu le groupe de travail «Article 29» et qui peut être consulté sur le site suivant: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp128\\_fr.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf). Voir également l'avis du CEPD sur le rôle de la Banque centrale européenne dans l'affaire SWIFT, qui peut être consulté sur le site web du CEPD.

signifie par exemple que le traitement des données effectué au sein du Conseil devrait être soumis à la décision-cadre du Conseil. On ne peut affirmer avec certitude si les auteurs du projet souhaitent un champ d'application aussi étendu ou s'ils entendaient limiter l'application aux trois organes mentionnés dans le considérant 20. En tout état de cause, il est nécessaire de préciser le texte afin d'éviter toute insécurité juridique.

39. Ceci conduit à une remarque d'ordre plus général. Selon le CEPD, il est extrêmement important de garantir, dans l'ensemble du troisième pilier, un niveau de protection des données approprié, étant donné que le libre échange d'informations au sein d'un espace de liberté, de sécurité et de justice sans frontières intérieures ne pourra s'améliorer qu'à cette condition. Ceci suppose l'application du cadre général relatif à la protection des données aux organes européens du troisième pilier. Le CEPD a souligné cette nécessité dans la partie IV de son avis concernant la proposition de décision pour Europol.
40. Toutefois, pour des raisons d'efficacité dans le processus législatif le CEPD a des doutes sérieux quant au bien-fondé d'une application de la présente décision-cadre aux activités des organes européens agissant dans le troisième pilier. Le premier argument s'opposant à un champ d'application étendu a trait à la politique législative. Le CEPD craint qu'en incluant les organes européens dans le présent texte, les discussions au sein du Conseil se concentrent sur ce nouvel élément et non sur les dispositions essentielles relatives à la protection des données. Ceci compliquera le processus législatif. Le second argument est de nature juridique. A première vue, une décision-cadre du Conseil — un instrument comparable à une directive selon le traité CE — ne semble pas l'instrument juridique approprié pour régler les droits et les obligations des organes européens. L'article 34 du traité UE introduit cet instrument afin d'harmoniser les lois et les règlements des États membres. En tout état de cause, la base juridique risque fort d'être remise en cause durant le processus législatif ou après.
41. Le CEPD a un point de vue similaire, notamment en ce qui concerne l'instrument juridique choisi, sur l'article 26 du projet, qui prévoit la mise en place d'une nouvelle autorité de contrôle commune remplaçant les autorités actuelles qui supervisent le traitement des données au sein des organes du troisième pilier. En soi, l'intention de mettre en place une telle autorité peut sembler logique. Elle pourrait conduire à un système de contrôle encore plus efficace et assurer la cohérence du niveau de protection au sein des organes établis dans le cadre du troisième pilier.
42. Toutefois, il n'y a pas pour le moment de nécessité immédiate à la création d'une telle autorité de contrôle. Le contrôle fonctionne de manière satisfaisante. En outre, le président d'Eurojust a émis des objections quant à l'application de ce système de contrôle à Eurojust. Sans se pencher sur le fond de ces objections, il est clair que le fait d'ajouter le contrôle des organes de l'UE dans la décision-cadre du Conseil rendrait le processus législatif encore plus difficile. En outre, cette approche ne serait pas cohérente avec d'autres propositions dans ce domaine qui sont actuellement en cours d'élaboration <sup>(31)</sup> ou qui ont été adoptées récemment <sup>(32)</sup>.
43. En résumé, le CEPD conseille de ne pas ajouter dans le texte de la décision-cadre du Conseil de dispositions relatives au traitement des données par les organes de l'UE. Le CEPD fait cette recommandation dans un souci d'efficacité du processus législatif. Il est important que tous les efforts du Conseil se concentrent sur les dispositions fondamentales de la protection des données afin de fournir aux citoyens la protection nécessaire.

## VI. CONCLUSIONS

44. Le CEPD salue le nouvel élan apporté par la présidence allemande. Ainsi que le CEPD et d'autres acteurs importants l'ont déjà souligné à diverses occasions, l'adoption d'un cadre général pour la protection des données dans le troisième pilier est essentielle pour soutenir le développement d'un espace de liberté, de sécurité et de justice qui garantisse de manière uniforme le droit des citoyens à la protection des données à caractère personnel et permette la coopération transfrontière des services répressifs.
45. Toutefois, la proposition révisée ne répond à aucun de ces objectifs. En effet, la proposition ne prévoyant pas un niveau de protection des données élevé et largement applicable, les échanges d'informations restent soumis aux différentes «règles d'origine» et aux «deux poids, deux mesures» qui nuisent considérablement à l'efficacité de la coopération policière sans améliorer la protection des données à caractère personnel.

<sup>(31)</sup> Comme la récente proposition de décision de la Commission portant création de l'Office européen de police (Europol), COM(2006) 817 final.

<sup>(32)</sup> Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 381 du 28.12.2006, p. 4).

46. Pour donner un exemple concret, un service répressif, au niveau national ou européen, qui s'occupe d'un dossier pénal — composé d'informations émanant de diverses autorités nationales ainsi que des autorités des États membres et de l'UE — devrait appliquer des règles de traitement différentes pour des informations différentes en fonction des éléments suivants: les données à caractère personnel ont ou n'ont pas été collectées au niveau national; chacun des organes ayant transmis les données a donné son accord pour la finalité envisagée; la conservation des données est conforme aux délais fixés par les lois applicables de chaque organe qui transmet les données; les limitations de traitement requises par chacun des organes transmettant des données n'empêche par le traitement; en cas de demande d'un État tiers, chaque organe transmettant des données a donné son consentement conformément à sa propre évaluation du niveau de protection et/ou aux engagements internationaux. En outre, la protection et les droits des citoyens varieront considérablement et feront l'objet d'importantes dérogations diverses en fonction de l'État membre où s'effectue le traitement.
47. En outre, le CEPD regrette que la qualité législative du texte ne soit pas satisfaisante et que la proposition rende le dossier plus compliqué en étendant l'application de la décision-cadre à Europol, Eurojust et au Système d'information douanier du troisième pilier ainsi qu'en proposant la création d'une autorité de contrôle commune sur la base d'un instrument juridique inadapté.
48. Le CEPD juge préoccupant le fait que le texte actuel supprime des dispositions essentielles en matière de protection des données à caractère personnel qui figuraient dans la proposition de la Commission. Ceci conduit en effet à un affaiblissement considérable du niveau de protection des citoyens. Premièrement, le texte n'apporte aucune valeur ajoutée à la convention 108, ce qui rendrait ses dispositions appropriées du point de vue de la protection des données, ainsi que l'exige l'article 30, paragraphe 1, du traité UE. Deuxièmement, il ne répond pas, en de nombreux points, au niveau de protection exigé par la convention 108. Par conséquent, le CEPD estime que cette proposition nécessite d'importantes améliorations avant de pouvoir servir de base de discussion à un cadre général adapté sur la protection des données dans le troisième pilier. Ces améliorations devraient s'assurer que ce cadre général:
- apporte une valeur ajoutée à la convention 108 en définissant les dispositions appropriées en matière de protection des données à caractère personnel exigées par l'article 30, paragraphe 1, du traité UE,
  - soit applicable au traitement national des données à caractère personnel par les services répressifs,
  - soit cohérent avec les principes relatifs à la protection des données applicables dans le premier pilier, tout en tenant compte, si besoin est, des spécificités des activités des services répressifs,
  - soit conforme aux principes édictés par la convention 108 et la recommandation n° R (87) 15, notamment en ce qui concerne:
    - la limitation des autres finalités pour lesquelles les données à caractère personnel peuvent être traitées,
    - la qualité des données, y compris la distinction entre les différentes catégories de personnes concernées (criminels, suspects, victimes, témoins, etc.), l'évaluation des divers niveaux de précision et de fiabilité des données à caractère personnel, les mécanismes permettant une vérification et une rectification régulières,
    - les conditions de transfert des données à caractère personnel aux autorités non compétentes et aux personnes privées, de même que l'accès des services répressifs aux données à caractère personnel contrôlés par des personnes privées et leur utilisation ultérieure par ces services,
  - assure une protection adéquate lors de l'échange de données à caractère personnel avec des pays tiers, également en ce qui concerne les accords internationaux,
  - traite les autres points mentionnés dans le présent avis ainsi que dans les avis antérieurs du CEPD.
49. Le CEPD est parfaitement conscient de la difficulté de réunir l'unanimité au sein du Conseil. Toutefois, la procédure de prise de décision ne saurait justifier une approche favorisant le plus petit dénominateur commun, qui porterait atteinte aux droits fondamentaux des citoyens de l'UE et entraverait l'efficacité des services répressifs.

Fait à Bruxelles, le 27 avril 2007.

Peter HUSTINX

*Contrôleur européen de la protection des données*