CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

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 (COM (2005) 475 final)

(2006/C 47/12)

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,

vu la demande d'avis formulée conformément à l'article 28, paragraphe 2, du 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,

A ADOPTÉ L'AVIS SUIVANT:

I. REMARQUES PRÉLIMINAIRES

Consultation du CEPD

1. La Commission a transmis au CEPD 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 par lettre datée du 4 octobre 2005. Le CEPD interprète cette lettre comme une demande d'avis à formuler à l'intention des institutions et organes communautaires, comme cela est prévu à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001. Le CEPD est d'avis qu'il convient de mentionner le présent avis dans le préambule de la décision-cadre.

L'importance de la proposition examinée

2. Le CEPD souligne l'importance que revêt la proposition en question, sous l'angle des droits et des libertés fondamentaux des personnes physiques, pour la protection de leurs données à caractère personnel. L'adoption de cette proposition constituerait un pas en avant considérable pour la protection des données à caractère personnel dans un domaine important qui requiert, notamment, un système cohérent et efficace capable de garantir la protection des données à caractère personnel à l'échelle de l'Union européenne.

3. À cet égard, le CEPD souligne l'importance croissante de la coopération policière et judiciaire entre les États membres en tant qu'élément de la mise en place progressive d'un espace de liberté, de sécurité et de justice. Le programme de La Haye a instauré le principe de disponibilité en vue d'améliorer l'échange transfrontière d'informations en matière répressive. Aux termes de ce programme ([1]), le simple fait que ces informations franchissent les frontières ne devrait plus être pris en considération. La mise en place du principe de disponibilité traduit une tendance plus générale qui vise à faciliter l'échange d'informations en matière répressive (voir par exemple le Traité de Prüm ([2]) signé par sept États membres ainsi que la proposition, présentée par la Suède, de décision-cadre relative à la simplification de l'échange d'informations et de renseignements entre services répressifs ([3])). L'adoption très récente par le Parlement européen d'une directive du Parlement européen et du Conseil sur la conservation des données de communications ([4]) s'inscrit dans la même perspective. Cette évolution rend nécessaire l'adoption d'un instrument juridique afin de garantir, sur la base de normes communes, une protection efficace des données à caractère personnel dans tous les États membres de l'Union européenne.

([1]) Page 18 du programme.

([2]) Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm (Allemagne) le 27 mai 2005.

([3]) Initiative du Royaume de Suède en vue de l'adoption d'une décision-cadre relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, notamment en ce qui concerne les infractions graves, y compris les actes terroristes (JO C 281 du 18.11.2004).

([4]) Directive adoptée sur la base de la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE (COM (2005) 438 final).

4. Le CEPD attire l'attention sur le fait que le cadre général actuel mis en place pour la protection des données dans ce domaine est insuffisant. En premier lieu, la directive 95/46/CE ne s'applique pas au traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues au titre VI du traité sur l'Union européenne (article 3, paragraphe 2, de la directive). Bien que dans la plupart des États membres le champ d'application de la législation de mise en œuvre soit plus étendu que ce qui est exigé par la directive elle-même et qu'il n'exclue pas le traitement de données à des fins répressives, il existe d'importantes différences entre les législations nationales. En deuxième lieu, la Convention nº 108 du Conseil de l'Europe, ([1]) qui lie tous les États membres, n'offre pas la précision nécessaire en termes de protection, ce qui a déjà été constaté au moment de l'adoption de la directive 95/46/CE. En troisième lieu, aucun de ces deux instruments juridiques ne tient compte des aspects spécifiques de l'échange de données par des autorités policières et judiciaires ([2]).

Une contribution au succès de la coopération en tant que telle

5. Une protection efficace des données à caractère personnel est non seulement importante pour les personnes concernées, mais elle contribue aussi au succès de la coopération policière et judiciaire à proprement parler. À de nombreux égards, ces deux intérêts publics vont de pair.

6. Il ne faut pas perdre de vue que les données à caractère personnel concernées revêtent très souvent un caractère sensible et qu'elles sont obtenues par les autorités policières et judiciaires à la suite d'une enquête menée sur des personnes. Une autorité sera d'autant plus disposée à échanger ces données avec les autorités d'un autre État membre qu'elle aura des garanties quant au niveau de protection dans cet État membre. Parmi les aspects à prendre en considération pour la protection des données, le CEPD mentionne la confidentialité et la sécurité des données ainsi que les limitations concernant l'accès et l'utilisation ultérieure.

7. Par ailleurs, un niveau élevé de protection des données peut constituer une garantie pour l'exactitude et la fiabilité des données à caractère personnel. L'exactitude et la fiabilité des données sont encore plus importantes lors de l'échange des données entre les autorités policières et/ou judiciaires, notamment en raison du fait que, après avoir été échangées et transmises à maintes reprises par les services répressifs, les données finissent par être traitées loin de leur source et en dehors du contexte dans lequel elles ont été initialement collectées et utilisées. En règle générale, les autorités qui reçoivent les informations ne disposent d'aucun élément supplémentaire et doivent s'appuyer totalement sur les données elles-mêmes.

8. L'harmonisation des règles nationales relatives aux données à caractère personnel dans le domaine de la police et de la justice — y compris les garanties appropriées pour la protection de ces données — peut dès lors renforcer la confiance mutuelle ainsi que l'efficacité des échanges proprement dits.

Respect des principes de la protection des données, conjugué à un ensemble complémentaire de règles

9. La nécessité et l'importance de la proposition à l'examen ont été soulignées à diverses occasions. Ainsi, lors de la conférence de printemps qui s'est tenue à Cracovie en avril 2005, les autorités européennes de protection des données ont adopté une déclaration et un document de synthèse appelant à l'adoption d'un nouveau cadre juridique pour la protection des données applicable aux activités relevant du troisième pilier. Ce nouveau cadre devrait non seulement respecter les principes de la protection des données énoncés dans la directive 95/46/CE — il importe de garantir la cohérence de la protection des données au sein de l'Union européenne —, mais aussi prévoir un ensemble complémentaire de règles tenant compte de la nature spécifique du domaine répressif ([3]). Le CEPD note avec satisfaction que la proposition à l'examen tient compte de ces principes de base puisque le texte respecte les principes de la protection des données énoncés dans la directive 95/46/CE et prévoit un ensemble complémentaire de règles.

10. Le présent avis s'attachera à examiner dans quelle mesure les effets de la proposition sont acceptables du point de vue de la protection des données, en tenant pleinement compte du contexte spécifique de la protection des données dans le domaine répressif. D'une part, les données à caractère personnel concernées revêtent la plupart du temps un caractère très sensible (voir le point 6 ci-dessus); d'autre part, de fortes pressions sont exercées pour y avoir accès, vu le souci des services répressifs d'obtenir des résultats positifs, notamment lorsqu'il s'agit de protéger la vie et la sécurité physique des personnes. Le CEPD estime que les règles relatives à la protection des données devraient tenir compte des besoins légitimes des services répressifs, mais aussi protéger la personne concernée contre le traitement et l'accès non justifiés. Pour être conforme au principe de proportionnalité, le résultat des délibérations du législateur européen devra tenir compte du respect de ces deux intérêts publics potentiellement opposés. À cet égard, le CEPD signale une fois encore que, très souvent, ces deux intérêts vont de pair.

Le contexte du titre VI du traité sur l'Union européenne

11. Enfin, il convient de mentionner que la proposition à l'examen s'inscrit dans le cadre du titre VI du traité sur l'Union européenne, qu'il est convenu d'appeler le troisième pilier. L'intervention du législateur européen est subordonnée à des limitations clairement définies: limitation des compétences législatives de l'Union aux domaines visés aux articles 30 et 31; limitations concernant la procédure législative, à laquelle le Parlement européen ne participe pas pleinement; limitations en termes de contrôle juridictionnel puisque, en vertu de l'article 35 du TUE, les compétences de la Cour européenne de justice sont limitées. Ces limitations rendent nécessaire un examen d'autant plus rigoureux du texte de la proposition.

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

([2]) En 1987, le Conseil de l'Europe a arrêté la recommandation nº R (87) 15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police; toutefois, celle-ci n'est, en tant que telle, pas contraignante à l'égard des États membres.

([3]) Dans le même ordre d'idées, voir le document intitulé «Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes», daté du 18 mars 2005 et publié sur le site du CEPD (www.edps.eu.int).

II. CONTEXTE: ÉCHANGE D'INFORMATIONS EN VERTU DU PRINCIPE DE DISPONIBILITÉ, CONSERVATION DES DONNÉES RELATIVES AUX COMMUNICATIONS ET CADRES SPÉCIFIQUES DU SIS II ET DU VIS

II.1 Le principe de disponibilité

12. La proposition est étroitement liée à la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité (COM(2005) 490 final). Celle-ci a pour objectif de mettre en œuvre le principe de disponibilité et, partant, de faire en sorte que les informations dont disposent les autorités compétentes d'un État membre en matière de lutte contre la criminalité soient communiquées aux autorités équivalentes des autres États membres. Elle devrait conduire à la suppression des frontières intérieures en ce qui concerne l'échange de ces informations, moyennant l'imposition de conditions uniformes pour l'échange des informations applicables sur l'ensemble du territoire de l'Union.

13. Ce lien étroit entre les deux propositions s'explique par le fait que les informations en matière répressive portent principalement sur des données à caractère personnel. On ne saurait adopter des dispositions législatives sur l'échange d'informations en matière répressive sans garantir une protection appropriée des données à caractère personnel. Dès lors qu'une action entreprise à l'échelle de l'Union européenne entraîne la suppression des frontières intérieures en ce qui concerne l'échange de ces informations, la protection des données à caractère personnel ne peut plus être régie uniquement par le droit national. C'est à l'Union européenne qu'il incombe d'assurer la protection des données à caractère personnel sur l'ensemble du territoire d'une Union sans frontières intérieures. Cette tâche, qui est explicitement énoncée à l'article 30, paragraphe 1, point b), du TUE, est une conséquence de l'obligation qu'a l'Union de respecter les droits fondamentaux (article 6 du TUE). En outre:

— l'article 1er, paragraphe 2, de la proposition à l'examen dispose expressément que les États membres ne peuvent plus ni restreindre ni interdire le flux transfrontière des informations pour des motifs liés à la protection des données à caractère personnel;

— la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité contient plusieurs références à la proposition à l'examen.

14. Le CEPD souligne qu'une décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité ne devrait être adoptée qu'à la condition qu'une décision-cadre relative à la protection des données à caractère personnel le soit également. Néanmoins, la proposition de décision-cadre relative à la protection des données, qui fait l'objet du présent avis, est en soi justifiée et nécessaire, même en l'absence d'un instrument juridique portant sur la disponibilité. Cet aspect est mis en exergue dans la partie I du présent avis.

15. Les deux instruments évoqués au point précédent étant effectivement proposés, chacune des propositions pertinentes fera l'objet d'un avis distinct du CEPD, ce qui s'explique aussi par des raisons pratiques: rien ne permet d'affirmer que les deux propositions seront examinées simultanément par le Conseil et le Parlement européen, ni avec la même célérité.

II.2 Conservation des données

16. Le 26 septembre 2005, le CEPD a présenté son avis sur la proposition de directive relative à la conservation des données relatives aux communications ([1]). Dans cet avis, le CEPD a attiré l'attention sur certaines lacunes importantes constatées dans la proposition; il a proposé d'ajouter à la directive des dispositions spécifiques concernant l'accès des autorités compétentes aux données relatives au trafic et aux données de localisation et l'utilisation ultérieure de ces données, ainsi que des garanties supplémentaires pour la protection des données. Le texte de la directive, tel qu'adopté par le Parlement européen et le Conseil, contient une disposition limitée — mais en aucun cas suffisante — sur la protection des données et leur sécurité; il contient aussi une disposition relative à l'accès, encore moins suffisante, qui renvoie au droit national pour l'adoption des mesures relatives à l'accès aux données conservées, sous réserve des dispositions pertinentes du droit de l'Union européenne et du droit international public.

17. L'adoption de la directive sur la conservation des données relatives aux communications rend encore plus impérieuse la nécessité de mettre en place un cadre juridique relatif à la protection des données dans le cadre du troisième pilier. En adoptant la directive précitée, le législateur communautaire oblige les fournisseurs de services de télécommunications et de services Internet à conserver des données à des fins répressives, sans qu'il y ait les garanties nécessaires et appropriées pour la protection de la personne concernée. Une lacune demeure en ce qui concerne la protection, car la directive ne se préoccupe pas (suffisamment) de l'accès aux données, ni de leur utilisation ultérieure après que les autorités compétentes ont pu y accéder à des fins répressives.

18. La proposition considérée comble une part importante de cette lacune dans la mesure où elle s'applique à l'utilisation ultérieure des données après leur utilisation par les services répressifs. Le CEPD regrette néanmoins que la proposition non plus ne traite pas de l'accès à ces données. Contrairement à ce qui est prévu pour les systèmes SIS II et VIS (voir la partie II.3 ci-dessous), cette question est laissée à la discrétion du législateur national.

II.3 Traitement dans le cadre du SIS II et du VIS

19. L'Union européenne utilise ou développe de vastes systèmes d'information (Eurodac, SIS II, VIS); elle s'emploie, en outre, à mettre en place des synergies entre ces systèmes. On constate par ailleurs une tendance croissante à accorder un accès plus large à de tels systèmes à des fins répressives. Cette évolution de grande ampleur doit tenir compte, conformément au programme de La Haye, de la «nécessité de trouver le juste milieu entre les objectifs répressifs et la préservation des droits fondamentaux des personnes».

([1]) Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE (COM(2005) 438 final), publié sur le site du CEPD (www.edps.eu.int).

20. Dans l'avis qu'il a rendu le 19 octobre 2005 sur les propositions relatives à un système d'information Schengen de deuxième génération (SIS-II) ([1]), le CEPD met en évidence certains éléments concernant l'application concomitante de règles générales (*lex generalis*) et de règles plus spécifiques (*lex specialis)* relatives à la protection des données. La proposition à l'examen peut être considérée comme une *lex generalis,* destiné à se substituer à la convention nº 108 dans le cadre du troisième pilier ([2]).

21. Le CEPD souligne, à cet égard, que la proposition définit également un cadre général pour la protection des données en ce qui concerne des instruments spécifiques, notamment la partie du SIS II relevant du troisième pilier et l'accès au système d'information sur les visas par les services répressifs. ([3])

III. LE CŒUR DE LA PROPOSITION

III.1 Normes communes applicables à tous les traitements

Point de départ

22. Conformément à son article 1er, paragraphe 1, la proposition a pour objet de fixer des normes communes visant à assurer la protection des données à caractère personnel dans le cadre d'activités relevant de la coopération policière et judiciaire en matière pénale. Il convient de lire cette disposition conjointement à l'article 3, paragraphe 1, qui dispose que la proposition s'applique au traitement des données à caractère personnel […] par une autorité compétente aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière.

23. Il ressort de ces dispositions que la décision-cadre proposée revêt deux principaux aspects: d'une part, elle définit des normes communes, d'autre part, elle s'applique à tous les traitements réalisés aux fins de l'application du droit pénal, même si les données concernées n'ont pas été transmises ou mises à disposition par les autorités compétentes des autres États membres.

24. Le CEPD souligne l'importance de ces deux grands aspects. La proposition à l'examen devrait avoir pour ambition de mettre en place un cadre pour la protection des données qui vienne compléter totalement le cadre juridique existant dans le premier pilier. Ce n'est qu'à cette condition que l'Union européenne se conformera pleinement à l'obligation qui lui incombe en vertu de l'article 6, paragraphe 2, du TUE, de respecter les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne des droits de l'homme.

Normes communes

25. Pour ce qui est du premier aspect évoqué ci-dessus, la proposition considérée vise à faire en sorte que les principes existants de la protection des données s'appliquent dans le domaine du troisième pilier. Elle définit par ailleurs des normes communes qui précisent ces principes en vue de leur application dans ce domaine. Le CEPD insiste sur l'importance de ces aspects de la proposition, qui traduisent la nature spécifique et le caractère sensible du traitement des données à caractère personnel dans ce domaine. Le CEPD salue en particulier l'instauration du principe visant à établir une distinction entre les données à caractère personnel selon les catégories de personnes auxquelles elles se rapportent. Ce principe, qui est propre à la protection des données dans le domaine de la coopération policière et judiciaire en matière pénale, vient s'ajouter aux principes existants de la protection des données (article 4, paragraphe 4). Le CEPD est d'avis que le principe en tant que tel et ses conséquences juridiques pour la personne concernée devraient être définis de façon encore *plus* précise (voir les points 88 à 92 ci-après).

26. Étant donné que les règles doivent s'appliquer dans des situations différentes, elles ne peuvent pas être trop détaillées. Elles doivent cependant offrir au citoyen la sécurité juridique nécessaire et garantir une protection appropriée de ses données à caractère personnel. Le CEPD estime que, globalement, la proposition trouve le juste milieu entre ces deux exigences législatives potentiellement contradictoires. Les dispositions autorisent la souplesse lorsque cela est nécessaire, tout en étant dans la plupart des cas suffisamment précises pour protéger le citoyen.

27. Sur certains points, cependant, la proposition prévoit une trop grande souplesse et n'offre pas les garanties nécessaires. Ainsi, à l'article 7, paragraphe 1, elle autorise une dérogation générale aux garanties prévues, à la seule condition que le droit national en dispose autrement («sauf disposition contraire du droit national»). Permettre l'exercice d'un pouvoir discrétionnaire aussi étendu afin de conserver les données pendant une durée excédant celle nécessaire à la réalisation de la finalité envisagée serait non seulement incompatible avec le droit fondamental à la protection des données, mais porterait aussi atteinte à la nécessité élémentaire d'harmoniser la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

28. Les dérogations, lorsqu'elles sont nécessaires, devraient se cantonner à des dispositions légales — nationales ou européennes — arrêtées dans le but de protéger des intérêts publics spécifiques qui devraient être mentionnés à l'article 7, paragraphe 1.

29. Cela nous amène à un autre point. Chaque fois qu'un autre instrument juridique spécifique adopté en vertu du titre VI du traité UE prévoit des conditions ou des limitations plus précises en ce qui concerne l'accès aux données et leur traitement, cette législation plus spécifique devrait s'appliquer en tant que *lex specialis*. L'article 17 de la proposition à l'examen prévoit des dérogations aux articles 12, 13, 14 et 15 lorsqu'une législation spécifique adoptée en vertu du titre VI énonce des conditions précises pour la transmission des données. Cela illustre le

([1]) Point 2.2.4 de l'avis.

([2]) 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.

([3]) 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), publiée le 24 novembre 2005. Le CEPD entend formuler un avis sur cette proposition au début de 2006.

caractère général de la proposition (comme cela est expliqué ci-avant), mais n'envisage pas toutes les hypothèses. Le CEPD est d'avis que l'article 17 devrait:

— être rédigé de façon plus générale: dans les cas où il existe une législation plus spécifique régissant un aspect, quel qu'il soit, du traitement des données (pas uniquement leur transmission), cette législation s'applique;

— être assorti d'une garantie prévoyant que les dérogations ne pourront pas entraîner un niveau de protection inférieur.

Applicabilité à tous les traitements

30. En ce qui concerne le deuxième aspect susmentionné, il conviendrait, idéalement, que toutes les collectes et tous les traitements de données à caractère personnel réalisés dans le cadre du troisième pilier soient pris en considération.

31. Il est indispensable, pour la réalisation de son objectif, que la décision-cadre s'applique à toutes les données policières et judiciaires, même si elles ne sont pas transmises ou mises à disposition par les autorités compétentes d'autres États membres.

32. Cela est extrêmement important car toute limitation concernant les données transmises aux autorités compétentes des autres États membres ou mises à leur disposition rendrait le domaine d'application de la décision-cadre particulièrement incertain et aléatoire, ce qui serait contraire à son objectif essentiel ([1]). Il serait porté atteinte à la sécurité juridique des personnes. Dans des circonstances normales, il est impossible de savoir à l'avance — c'est-à-dire au moment de la collecte ou du traitement des données à caractère personnel — si ces données seront susceptibles de donner lieu à un échange avec les autorités compétentes d'autres États membres. Le CEPD renvoie à cet égard au principe de disponibilité et à la suppression des frontières intérieures en ce qui concerne l'échange des données en matière répressive.

33. Enfin, le CEPD note que la proposition ne s'applique pas:

— aux traitements réalisés dans le cadre du deuxième pilier du traité UE (politique étrangère et de sécurité commune);

— aux traitements de données par les services de renseignement, ni à l'accès de ces services à ces données lorsque celles-ci sont traitées par les autorités compétentes ou d'autres parties (ceci découle de l'article 33 du traité UE).

Dans ces domaines, le droit national doit garantir une protection appropriée des personnes concernées. Cette lacune en ce qui concerne la protection à l'échelle de l'UE doit être prise en compte dans l'appréciation de la proposition: ([2]) dans la mesure où tous les traitements dans le domaine répressif ne peuvent pas être pris en considération, le législateur doit veiller à une protection d'autant plus efficace dans les domaines qui le sont.

([1]) Le CEPD renvoie au même raisonnement développé par la Cour dans (entre autres) son arrêt rendu dans les affaires jointes C-465/00, C-138/01 et C-139/01, Österreichischer Rundfunk et autres, Recueil 2003, p. I-4989.

([2]) Dans le même ordre d'idées, voir le point 33 de l'avis du CEPD du 26 septembre 2005 sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE.

III.2 **La base juridique**

34. Le préambule de la proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité mentionne une base juridique précise, à savoir l'article 30, paragraphe 1, point b). Par contre, la proposition à l'examen ne précise pas quelles dispositions de l'article 30 ou de l'article 31 constituent sa base juridique.

35. Bien que le CEPD, en tant que conseiller pour la législation de l'Union européenne, n'ait pas pour rôle de déterminer la base juridique d'une proposition, on peut toutefois supposer que la proposition considérée pourrait elle aussi être fondée sur l'article 30, paragraphe 1, point b). Elle pourrait également reposer sur l'article 31, paragraphe 1, point c) du traité UE et devrait s'appliquer, dans son intégralité, aux situations internes aux États membres, à condition que cela soit nécessaire à l'amélioration de la coopération policière et judiciaire entre les États membres. À cet égard, le CEPD souligne une fois encore que toutes les données à caractère personnel collectées, stockées, traitées et analysées à des fins répressives pourraient, notamment en vertu du principe de disponibilité, faire l'objet d'un échange avec les autorités compétentes d'un autre État membre.

36. Le CEPD partage l'opinion selon laquelle l'article 30, paragraphe 1, point b) et l'article 31, paragraphe 1, point c) du traité UE constituent une base juridique pour l'adoption de règles relatives à la protection des données dont le champ d'application ne se limite pas à la protection des données à caractère personnel effectivement échangées entre les autorités compétentes des États membres, mais qui englobe aussi les situations internes. Plus particulièrement:

— l'article 30, paragraphe 1, point b), qui peut servir de base juridique pour les règles concernant la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes, n'est pas limité aux informations qui ont été mises à la disposition des autres États membres ou qui leur ont été transmises. La seule limitation imposée par l'article 30, paragraphe 1, point b) est la pertinence des informations pour la coopération policière;

— en ce qui concerne la coopération judiciaire, l'article 31, paragraphe 1, point c) est encore plus explicite, puisque l'action en commun doit, entre autres, viser à «assurer, dans la mesure nécessaire à l'amélioration de cette coopération, la compatibilité des règles applicables dans les États membres»;

— il ressort de l'affaire Pupino ([3]) que la Cour de justice applique les principes du droit communautaire aux questions relevant du troisième pilier. Cette jurisprudence reflète l'évolution d'une simple coopération entre les autorités des États membres dans le cadre du troisième pilier vers la mise en place d'un espace de liberté, de sécurité et de justice comparable au marché intérieur tel qu'il a été établi dans le cadre du traité CE;

([3]) Arrêt rendu par la Cour le 16 juin 2005 dans l'affaire C-105/03, Pupino.

— le CEPD est d'avis que le principe d'efficacité implique que le traité ne doit pas être interprété d'une manière qui empêche les institutions de l'Union européenne d'accomplir leurs missions efficacement, notamment celle qui consiste à protéger les droits fondamentaux;

— comme cela a été évoqué plus haut, une limitation aux situations transfrontalières irait à l'encontre du principe de disponibilité et porterait atteinte à la sécurité juridique des personnes.

37. Le CEPD attire plus particulièrement l'attention sur *l'échange de données avec des pays tiers*. De même que les États membres utilisent des données à caractère personnel collectées et traitées dans des pays tiers que ceux-ci leur transmettent à des fins répressives, ils transmettent aux autorités compétentes de pays tiers ou à des instances internationales des données à caractère personnel qu'ils ont eux-mêmes collectées et/ou traitées.

38. Les articles 30 et 31 du TUE ne prévoient pas que les données à caractère personnel collectées par les autorités de pays tiers doivent faire l'objet d'un traitement différent de celui appliqué aux données qui ont été initialement collectées par les autorités compétentes des États membres. Une fois qu'elles ont été reçues, les données provenant d'un pays tiers doivent respecter les mêmes normes que les données collectées dans un État membre. Toutefois, il n'est pas toujours facile de garantir la qualité des données (cet aspect sera abordé dans le chapitre suivant).

39. La transmission de données à caractère personnel par les autorités compétentes d'un État membre à un pays tiers se situe, à proprement parler, en dehors du champ d'application du titre VI du traité UE. Toutefois, dans l'hypothèse où des données pourraient être transmises à un pays tiers sans que la protection de la personne concernée soit garantie, cela porterait gravement atteinte à la protection envisagée par la proposition considérée sur le territoire de l'Union européenne, pour les raisons évoquées dans la partie III.4 ci-dessous. En résumé:

— Il serait directement porté atteinte aux droits de la personne concernée, tels qu'ils sont garantis par la proposition considérée, si la transmission aux pays tiers n'était pas soumise aux règles régissant la protection des données;

— il existerait un risque que les autorités compétentes des États membres contournent les normes strictes applicables à la protection des données.

40. En résumé, si l'on veut accroître l'efficacité des règles communes relatives à la protection des données à caractère personnel échangées entre les autorités compétentes des États membres et donc améliorer la coopération entre les États membres, il est nécessaire de rendre ces règles applicables aux données à caractère personnel échangées par les autorités compétentes des États membres et les autorités de pays tiers ou des organisations internationales. Les articles 30 et 31 du TUE offrent la base juridique nécessaire à cet effet.

III.3 **Observations spécifiques concernant le champ d'application de la proposition**

Données à caractère personnel traitées par les autorités judiciaires

41. À l'instar des services de police, les autorités judiciaires traitent et échangent des données à caractère personnel. La proposition, qui est fondée sur les articles 30 et 31 du traité UE, s'applique tant à la coopération entre les services de police qu'à la coopération entre les autorités judiciaires. À cet égard, son champ d'application est plus étendu que celui de la décision-cadre du Conseil relative à l'échange d'informations, qui est limité à la coopération policière et s'applique uniquement aux traitements des informations réalisés préalablement à l'engagement de poursuites.

42. Le CEPD se réjouit du fait que la proposition englobe les données à caractère personnel traitées par les autorités judiciaires. Il est tout indiqué d'aborder dans une même proposition les données des services de police et celles des autorités judiciaires traitées à des fins répressives. En premier lieu, le passage de l'enquête pénale aux poursuites n'est pas organisé de la même manière dans les États membres, les autorités judiciaires intervenant à des stades différents. En deuxième lieu, il est possible que toutes les données à caractère personnel traitées au cours de cette procédure finissent par figurer dans un dossier judiciaire. Il n'est donc pas logique d'appliquer des régimes différents régissant la protection des données lors des étapes évoquées ci-dessus.

43. En revanche, pour ce qui est du contrôle du traitement des données, une approche différente s'impose. L'article 30 de la proposition énumère les tâches qui incombent aux autorités de contrôle. L'article 30, paragraphe 9, dispose que les prérogatives de l'autorité de contrôle ne portent pas atteinte à l'indépendance du pouvoir judiciaire. Le CEPD recommande de préciser, dans la proposition, que les autorités de contrôle ne supervisent pas les traitements de données réalisés par les autorités judiciaires dans l'exercice de leurs fonctions. ([1])

Traitement par Europol et Eurojust (ainsi que dans le cadre du système d'information douanier)

44. Conformément à l'article 3, paragraphe 2, de la proposition, la décision-cadre ne s'applique pas au traitement de données à caractère personnel par Europol, Eurojust et le système d'information douanier ([2]).

([1]) Cette disposition pourrait être similaire à celle figurant à l'article 46 du règlement (CE) n° 45/2001.

([2]) Le système d'information douanier est un système de portée limitée, mais plutôt complexe. Il comprend des éléments nationaux et supranationaux comme le système d'information Schengen. Étant donné que la proposition revêt une importance relativement limitée pour le système d'information douanier et vu la complexité du système proprement dit, celui-ci ne sera pas abordé dans le présent avis. Le CEPD se penchera sur la question dans un autre contexte.

45. Cette disposition est, à proprement parler, superflue, du moins en ce qui concerne Europol et Eurojust. En effet, conformément à l'article 34, paragraphe 2, point b) du traité UE, une décision-cadre ne peut être arrêtée qu'aux fins du rapprochement des dispositions législatives et réglementaires des États membres; elle ne peut donc pas porter sur Europol et Eurojust.

46. Pour ce qui est du fond, le texte de l'article 3, paragraphe 2, appelle les observations suivantes:

— la proposition considérée prévoit un cadre général qui devrait en principe être applicable à toutes les situations relevant du troisième pilier. La cohérence du cadre juridique régissant la protection des données est en soi un élément qui renforce l'efficacité de la protection des données;

— à l'heure actuelle, Europol et Eurojust disposent de systèmes de protection des données bien définis, y compris un système de contrôle. Il n'est donc pas indispensable d'adapter, dans l'immédiat, les règles applicables en la matière au texte de la proposition;

— en revanche, à plus long terme, les règles régissant la protection des données dans le cadre d'Europol et d'Eurojust devraient être rendues totalement compatibles avec la décision-cadre considérée;

— cela est d'autant plus important que la proposition de décision-cadre en question — à l'exception de son chapitre III — s'applique à la collecte et au traitement des données à caractère personnel transmises par les États membres à Europol et Eurojust.

III.4 **Structure de la proposition**

47. Le CEPD conclut de l'examen de la proposition que, d'une manière générale, celle-ci envisage la protection des données selon une structure par niveau. Ainsi les normes communes énoncées au chapitre II de la proposition (et aux chapitres IV à VII en ce qui concerne des questions spécifiques) comportent deux niveaux de protection, à savoir:

— la transposition au troisième pilier, des principes généraux de la protection des données, tels qu'ils sont définis dans la directive 95/46/CE et d'autres instruments juridiques des Communautés européennes, ainsi que dans la convention n° 108 du Conseil de l'Europe.

— la définition de règles supplémentaires régissant la protection des données applicables à tous les traitements de données à caractère personnel réalisés dans le cadre du troisième pilier. On trouvera des exemples de ces règles supplémentaires à l'article 4, paragraphes 3 et 4, de la proposition.

48. Le chapitre III constitue un troisième niveau de protection pour les formes spécifiques de traitement. Le titre des deux sections de ce chapitre ainsi que le libellé de plusieurs dispositions de la proposition laissent supposer que ce chapitre ne s'applique qu'aux données transmises ou mises à disposition par les autorités compétentes des autres États membres. Il en résulte que d'importantes dispositions régissant la protection des données à caractère personnel ne s'appliqueraient pas aux données qui ne seraient pas échangées entre les États membres. Cela étant, le texte est ambigu car les dispositions elles-mêmes semblent aller au-delà des activités directement liées aux données échangées. En tout état de cause, aucune explication claire ou justification concernant cette limitation du champ d'application n'est fournie, que ce soit dans l'exposé des motifs ou dans l'analyse d'impact.

49. Le CEPD souligne la valeur ajoutée qu'apporte cette structure organisée par niveaux, qui, en tant que telle, peut garantir une protection optimale de la personne concernée, compte tenu des besoins spécifiques des services répressifs. Cela répond à la nécessité exprimée lors de la conférence de printemps des autorités de protection des données qui s'est tenue à Cracovie en avril 2005 de garantir une protection adéquate des données; cela est également, quant au principe, conforme à l'article 8 de la Charte des droits fondamentaux de l'Union européenne et à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, notamment son article 8.

50. L'analyse du texte de la proposition conduit toutefois à formuler les observations ci-après.

51. En premier lieu, il convient de veiller à ce que les règles supplémentaires régissant la protection des données qui sont énoncées au chapitre II (le deuxième niveau de protection évoqué au point 47 ci-dessus) ne dérogent pas aux principes généraux de la protection des données. Le CEPD est d'avis que les règles supplémentaires énoncées au chapitre II devraient offrir aux personnes concernées une protection supplémentaire dans le cadre spécifique du troisième pilier (informations policières et judiciaires). En d'autres termes, ces règles supplémentaires ne peuvent pas entraîner un niveau de protection inférieur.

52. Par ailleurs, le chapitre III, qui porte sur les formes spécifiques de traitement (et qui comprend le troisième niveau de protection), ne devrait pas déroger aux dispositions du chapitre II. Pour le CEPD, les dispositions du chapitre III devraient offrir aux personnes concernées une protection supplémentaire dans les situations où interviennent les autorités compétentes de plusieurs États membres; ces dispositions ne peuvent toutefois pas entraîner un niveau de protection inférieur.

53. En deuxième lieu, le chapitre III ne devrait pas contenir de règles revêtant un caractère général. Le CEPD recommande de déplacer ces dispositions au chapitre II. Seules doivent figurer dans le chapitre III les dispositions qui concernent à proprement parler la protection des données à caractère personnel dans le cas d'un échange de données entre États membres. Cela est d'autant plus important que le chapitre III contient d'importantes dispositions eu égard à un niveau élevé de protection de la personne concernée dans le cadre répressif (voir la partie IV.1 du présent avis).

IV. **ANALYSE DES ÉLÉMENTS DE LA PROPOSITION**

IV.1 **Points de départ de l'analyse**

54. Lors de l'examen des différents éléments de fond de la proposition, le CEPD tiendra compte de sa structure et de son contenu particuliers. Il ne formulera pas d'observations sur chacun des articles de la proposition.

55. Tout d'abord, la plupart des dispositions de la proposition sont le reflet de celles d'autres instruments juridiques de l'UE relatifs à la protection des données à caractère personnel. Ces dispositions correspondent au cadre juridique défini par l'UE pour la protection des données et sont suffisantes pour offrir des garanties appropriées en ce qui concerne la protection des données dans le cadre du troisième pilier.

56. Le CEPD constate néanmoins que certaines dispositions qui figurent actuellement dans le chapitre III de la proposition — et qui concernent des aspects spécifiques du traitement ou qui, d'une manière générale (voir plus haut, point 48), ne sont applicables qu'aux données échangées avec d'autres États membres — intègrent les principes généraux et essentiels du droit de l'UE relatif à la protection des données. Par conséquent, ces dispositions devraient être déplacées du chapitre III vers le chapitre II afin qu'elles s'appliquent à tous les traitements de données réalisés par les services répressifs. Il s'agit notamment des dispositions relatives à la vérification de la qualité des données (article 9, paragraphes 1 et 6) et de celles réglementant le traitement ultérieur des données à caractère personnel (article 11, paragraphe 1).

57. Certains autres articles du chapitre III de la proposition ne font pas de distinction entre, d'une part, les conditions supplémentaires expressément liées aux échanges de données avec d'autres États membres — comme le consentement de l'autorité compétente de l'État membre qui transmet les données — et, d'autre part, les garanties utiles et nécessaires, également en ce qui concerne les données traitées au sein d'un État membre. À cet égard, le CEPD recommande de faire en sorte que ces garanties soient applicables d'une manière générale, y compris en ce qui concerne les données à caractère personnel qui n'ont pas été transmises ou mises à disposition par un autre État membre. Cette recommandation concerne:

— la transmission de données à des personnes privées et à des autorités autres que les autorités répressives (articles 13 et 14, points a) et b));

— le transfert à des pays tiers ou à des instances internationales (article 15, à l'exception du point c)).

58. Cette partie de l'avis attirera également l'attention du législateur sur certaines garanties supplémentaires qui ne figurent pas dans la proposition actuelle. Le CEPD est d'avis que de telles garanties supplémentaires devraient être prévues en ce qui concerne les décisions individuelles automatisées, les données à caractère personnel reçues de pays tiers, l'accès aux bases de données des personnes privées, le traitement des données biométriques et les profils ADN.

59. L'analyse développée ci-après sera en outre assortie de recommandations visant à améliorer le libellé actuel, afin de garantir l'efficacité des dispositions, la cohérence du texte ainsi que sa conformité avec le cadre juridique actuel régissant la protection des données.

IV.2 **Limitation de la finalité et traitement ultérieur**

60. L'article 4, paragraphe 1, point b), dispose que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. En règle générale, les données sont collectées en rapport avec un délit précis (ou, dans certaines circonstances, pour enquêter sur un groupe ou un réseau criminel, etc.). Ces données, qui peuvent être utilisées pour cette finalité initiale, pourraient ensuite être traitées pour une autre finalité, à condition que celle-ci soit compatible avec la première (par exemple, les données collectées sur une personne reconnue coupable de trafic de drogue pourraient être utilisées dans le cadre d'une enquête portant sur un réseau de revendeurs de drogue). Cette approche repose sur le principe de limitation de la finalité, tel que consacré notamment à l'article 8 de la Charte des droits fondamentaux de l'Union européenne; elle est donc conforme à la législation en vigueur régissant la protection des données.

Traitement ultérieur pour des finalités entrant dans le champ d'application de la décision-cadre

61. Le CEPD note que la proposition ne tient pas compte de manière tout à fait satisfaisante d'une situation à laquelle les services de police peuvent être confrontés dans le cadre de leurs activités, à savoir la nécessité d'utiliser ultérieurement des données pour une finalité considérée comme incompatible avec celle pour laquelle elles ont été collectées. Une fois collectées par les services de police, des données pourraient s'avérer nécessaires pour élucider un délit complètement différent. Par exemple, les données collectées aux fins de poursuites relatives à des infractions de roulage pourraient ensuite être utilisées pour localiser un voleur de voitures et le poursuivre en justice. La deuxième finalité, bien que légitime, ne saurait être considérée comme totalement compatible avec la finalité initiale de la collecte des données. Si les services répressifs n'étaient pas autorisés à utiliser les données pour cette deuxième finalité, ils pourraient être tentés de collecter des données pour des finalités très larges ou mal définies, ce qui viderait le principe de limitation de la finalité de sa substance pour ce qui est de la collecte des données. Par ailleurs, cela porterait atteinte à d'autres principes, notamment les principes de proportionnalité, d'exactitude et de fiabilité (voir l'article 4, paragraphe 1, points c) et d)).

62. Conformément au droit de l'UE relatif à la protection des données, les données à caractère personnel doivent être collectées pour des finalités déterminées et explicites, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Cependant, le CEPD est d'avis qu'il faut autoriser une certaine souplesse en ce qui concerne l'utilisation ultérieure. La limitation relative à la collecte a plus de chances d'être correctement respectée si les autorités en charge de la sécurité intérieure savent qu'elles peuvent avoir recours, moyennant des garanties appropriées, à une dérogation concernant la limitation applicable à l'utilisation ultérieure.

63. Il convient de préciser que l'article 11 de la proposition tient compte de cette nécessité en ce qui concerne le traitement ultérieur, mais de manière plutôt insuffisante. En effet, cet article ne s'applique qu'aux données reçues des autorités compétentes des autres États membres ou mises à disposition par celles-ci et ne prévoit pas de garanties suffisantes.

64. Le CEPD recommande d'appliquer l'article 11, paragraphe 1, à toutes les données, qu'elles aient ou non été reçues d'un autre État membre. Par ailleurs, il convient de prévoir des garanties supplémentaires plus strictes que celles prévues à l'article 11, paragraphe 1, point b): l'utilisation ultérieure de données pour une finalité considérée comme incompatible avec la finalité initiale ne devrait être autorisée que lorsque cela est strictement nécessaire, dans un cas précis, à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou pour protéger les intérêts ou les droits fondamentaux d'une personne. Concrètement, le CEPD propose d'énoncer une telle disposition dans un nouvel article 4 bis (en tout état de cause au chapitre II de la proposition).

65. L'article 11, paragraphes 2 et 3, reste applicable en l'état; ces dispositions prévoient des garanties supplémentaires en ce qui concerne les données reçues d'autres États membres. Le CEPD souligne que l'article 11, paragraphe 3, s'applique aux échanges de données réalisés dans le cadre du SIS II: le CEPD a déjà indiqué, dans son avis sur le SIS II, qu'il convient de veiller à ce que les données SIS ne puissent pas être utilisées pour une finalité autre que celles du système proprement dit.

Traitement ultérieur pour des finalités ne relevant pas du champ d'application de la coopération policière et judiciaire

66. Il arrive parfois que des données doivent être traitées afin de sauvegarder d'autres intérêts importants. En pareil cas, les données pourraient même être traitées par des autorités autres que les autorités compétentes prévues par la décision-cadre. Il est possible que ces compétences des États membres donnent lieu à un traitement portant atteinte à la vie privée (par exemple la vérification des antécédents d'une personne qui n'est pas suspectée). Elles devraient donc être assorties de conditions très strictes, comme l'obligation, pour les États membres, d'adopter des dispositions législatives spécifiques s'ils veulent avoir recours à une telle dérogation. Pour ce qui est du premier pilier, cette question est traitée à l'article 13 de la directive 95/46/CE, qui prévoit que, dans des cas précis, l'imposition de limitations à certaines dispositions de la directive est autorisée. Les États membres qui appliquent de telles limitations doivent le faire en respectant l'article 8 de la convention européenne des droits de l'homme.

67. Dans le même ordre d'idées, il conviendrait que la décision-cadre à l'examen prévoie, au chapitre II, que les États membres devraient avoir la possibilité de prendre des mesures législatives visant à autoriser le traitement ultérieur lorsqu'une telle mesure est nécessaire aux fins de:

— la prévention des menaces contre la sécurité publique, la défense ou la sécurité nationale;

— la protection d'un intérêt économique ou financier important d'un État membre ou de l'Union européenne;

— la protection de la personne concernée.

IV.3 **Critères relatifs à la licéité du traitement des données**

68. L'article 5 de la proposition dispose que les données ne peuvent être traitées par les autorités compétentes qu'en vertu d'une loi établissant que ce traitement est nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée et aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière. Le CEPD souscrit aux conditions strictes énoncées audit article 5.

69. Néanmoins, le texte de l'article 5 ne tient pas suffisamment compte de la nécessité de rendre légitime le traitement de données pour d'autres motifs légaux, dans des cas précis. Cette disposition importante ne devrait pas, par exemple, empêcher les services de police de respecter l'obligation légale qui leur incombe en vertu du droit national de divulguer des informations aux services d'immigration et aux autorités fiscales. C'est pourquoi le CEPD propose qu'il soit tenu compte, à l'article 5, d'autres motifs légaux fondés pour autoriser le traitement de données à caractère personnel, notamment la nécessité, pour le responsable du traitement, de respecter une obligation légale à laquelle il est soumis, le consentement sans équivoque de la personne concernée, à condition que le traitement soit réalisé dans l'intérêt de celle-ci, ou la nécessité de protéger les intérêts vitaux de la personne concernée.

70. Le CEPD signale que le respect des critères relatifs à la licéité du traitement des données revêt une importance particulière en ce qui concerne la coopération policière et judiciaire. En effet, des données à caractère personnel collectées de manière illicite par les services de police pourraient ne pas être admises comme élément de preuve dans une procédure judiciaire.

IV.4 **Nécessité et proportionnalité**

71. Les articles 4 et 5 de la proposition visent également à faire en sorte — de façon globalement satisfaisante — que les limites imposées à la protection des données à caractère personnel soient nécessaires et proportionnées, comme cela est exigé en vertu du droit de l'Union européenne et de la jurisprudence de la Cour européenne des droits de l'homme fondée sur l'article 8 de la convention européenne des droits de l'homme:

— l'article 4, paragraphe 1, point c) énonce la règle générale selon laquelle les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;

— l'article 5 précise que le traitement devrait être *nécessaire* pour l'accomplissement des tâches légitimes de l'autorité concernée et aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière;

— l'article 4, paragraphe 4, dispose que le traitement des données à caractère personnel n'est nécessaire que si certaines conditions précises sont respectées.

72. Le CEPD note que la formulation proposée pour l'article 4, paragraphe 4, ne respecte pas les critères établis par la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la convention européenne des droits de l'homme, selon laquelle il n'est possible d'imposer des restrictions au droit à la vie privée que lorsque cela est nécessaire dans une société démocratique. Aux termes de la proposition, le traitement des données serait considéré comme nécessaire non seulement lorsqu'il *rendrait possible* l'accomplissement de leurs tâches par les autorités répressives et judiciaires, mais aussi lorsqu'il y a *de bonnes raisons de croire* que les données à caractère personnel concernées *faciliteraient ou accéléreraient* simplement la prévention et la détection des infractions pénales, et les enquêtes et poursuites en la matière.

73. De tels critères ne sont pas conformes au prescrit de l'article 8 de la convention européenne des droits de l'homme, dans la mesure où pratiquement tous les traitements de données à caractère personnel pourraient être considérés comme facilitant les activités des autorités judiciaires ou de police, même si les données concernées ne sont pas véritablement nécessaires pour l'accomplissement de ces activités.

74. En l'état, l'article 4, paragraphe 4, ouvrirait la voie à des collectes de données à caractère personnel d'une étendue inacceptable, fondées uniquement sur la conviction que les données concernées *peuvent faciliter* la prévention et la détection des infractions pénales, ainsi que les enquêtes et poursuites en la matière. Au contraire, le traitement de données à caractère personnel ne doit être considéré comme nécessaire que lorsque les autorités compétentes peuvent clairement en démontrer le besoin, et à condition qu'il ne soit pas possible de recourir à des mesures plus respectueuses de la vie privée.

75. Par conséquent, le CEPD recommande de reformuler le premier tiret de l'article 4, paragraphe 4, de manière à ce que la jurisprudence relative à l'article 8 de la convention européenne des droits de l'homme soit respectée. Par ailleurs, le CEPD propose, pour des raisons de logique, de déplacer l'article 4, paragraphe 4, à la fin de l'article 5.

IV.5 **Traitements portant sur des catégories particulières de données**

76. L'article 6 prévoit une interdiction de principe du traitement des données sensibles, à savoir les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle. Cette interdiction ne s'applique pas lorsque le traitement est prévu par un texte de loi et qu'il est absolument nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière. Des données sensibles peuvent également être traitées si la personne concernée y a expressément consenti. Dans les deux cas, des garanties spécifiques appropriées sont prévues.

77. Le libellé de l'article 6 appelle deux observations. En premier lieu, cet article repose dans une trop large mesure sur le consentement de la personne concernée. Le CEPD souligne que le traitement de données sensibles fondé sur le consentement explicite de la personne concernée ne devrait être autorisé que dans la mesure où le traitement est réalisé dans l'intérêt de celle-ci; par ailleurs, le refus de consentir ne devrait pas avoir d'effets négatifs pour la personne concernée. Le CEPD recommande de modifier l'article 6 dans ce sens, et ce également afin qu'il soit conforme au droit existant de l'UE relatif à la protection des données.

78. En second lieu, le CEPD considère que l'on pourrait aussi tenir compte d'autres motifs légaux pour justifier le traitement, notamment la nécessité de protéger les intérêts vitaux de la personne concernée ou d'une autre personne (lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement).

79. Dans le domaine de la coopération policière et judiciaire, le traitement d'autres catégories de données à caractère personnel potentiellement sensibles, notamment les données biométriques et les profils ADN, revêt une importance croissante. Ces données ne sont pas expressément visées par l'article 6 de la proposition. Le CEPD invite le législateur européen à être particulièrement attentif lorsqu'il s'agira de mettre en œuvre les principes généraux de la protection des données énoncés dans la proposition à l'examen dans de nouvelles dispositions législatives qui auront pour conséquence le traitement de ces catégories particulières de données. Citons, à titre d'exemple, la proposition actuelle de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité (voir plus haut, points 12 à 15). Cet instrument autorise expressément le traitement et l'échange des données biométriques et des profils ADN (se reporter à l'annexe II de la proposition), mais n'aborde pas la question du caractère sensible et de la nature particulière de ces données du point de vue de la protection des données.

80. Le CEPD recommande que des garanties spécifiques soient prévues, notamment pour veiller à ce que:

— les données biométriques et les profils ADN ne soient utilisés que sur la base de normes techniques clairement définies et interopérables,

— il soit tenu dûment compte du niveau d'exactitude de ces données et que celui-ci puisse être contesté par la personne concernée par des moyens facilement accessibles;

— le respect de la dignité des personnes soit totalement garanti.

Il appartient au législateur de décider si ces garanties supplémentaires doivent être prévues dans la décision-cadre à l'examen ou dans les instruments juridiques spécifiques régissant la collecte et l'échange de ces catégories particulières de données.

IV.6 **Exactitude et fiabilité**

81. L'article 4, paragraphe 1, point d), établit les règles générales en matière de qualité des données. Selon cet article, le responsable du traitement doit faire en sorte que les données soient exactes et, si nécessaire, mises à jour. Il prend toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées. Cette disposition est conforme aux principes généraux de la législation de l'UE en matière de protection des données.

82. L'article 4, paragraphe 1, point d), troisième phrase, dispose que les États membres peuvent prévoir un traitement des données selon divers degrés d'exactitude et de fiabilité. Le CEPD comprend cette disposition comme une exception au principe général d'exactitude et recommande de clarifier le caractère exceptionnel de cette clause, en insérant le terme «cependant» ou «néanmoins» au début de l'article 4, paragraphe 1, point d), troisième phrase. Dans ce cas, c'est-à-dire lorsque l'exactitude des données ne peut être entièrement garantie, le responsable du traitement sera tenu de distinguer les données en fonction de leur degré d'exactitude et de fiabilité, en tenant compte en particulier de la différence essentielle qui existe entre les données factuelles et les données fondées sur des opinions ou des appréciations personnelles. Le CEPD souligne l'importance de cette obligation à la fois pour la personne concernée et pour les services répressifs, surtout lorsque les données sont traitées dans un contexte éloigné de leur source (voir le point 7 du présent avis).

Vérification de la qualité des données

83. Le principe général énoncé à l'article 4, paragraphe 1, point d), est complété par les mesures de protection plus spécifiques établies à l'article 9 relatif à la vérification de la qualité des données. L'article 9 dispose notamment que:

1. la qualité des données à caractère personnel est vérifiée au plus tard avant la transmission ou la mise à disposition de celles-ci. De plus, pour les données mises à disposition par accès direct automatisé, la qualité doit être vérifiée régulièrement (article 9, paragraphes 1 et 2);

2. les décisions de justice et les décisions d'arrêt des poursuites doivent être indiquées lors de toute transmission de données, les données fondées sur des opinions ou des appréciations personnelles doivent être vérifiées à la source avant d'être transmises et leur degré d'exactitude ou de fiabilité doit être précisé (article 9, paragraphe 1);

3. les données à caractère personnel sont «annotées» à la demande de la personne concernée si leur exactitude est niée par celle-ci et si leur exactitude ou inexactitude ne peut être vérifiée (article 9, paragraphe 6).

84. Dès lors, l'application conjointe de l'article 4, paragraphe 1, et de l'article 9 garantit que la qualité des données est vérifiée correctement, à la fois par la personne concernée et par les services qui sont les plus proches de la source des données traitées et qui sont donc le mieux à même de les vérifier.

85. Le CEPD accueille favorablement ces dispositions, étant donné que, tout en se concentrant sur les besoins des services répressifs, elles garantissent que chaque donnée est prise en compte de façon appropriée et utilisée en fonction de son exactitude et de sa fiabilité, ce qui permet d'éviter que la personne concernée soit affectée de façon disproportionnée par l'éventuelle inexactitude de données le concernant.

86. La vérification de la qualité des données constitue un élément essentiel de la protection pour la personne concernée, en particulier en ce qui concerne les données à caractère personnel traitées par les autorités policières et judiciaires. Dès lors, le CEPD déplore le fait que l'applicabilité de l'article 9 sur la vérification de la qualité des données soit limitée aux données transmises à d'autres États membres ou mises à la disposition de ceux-ci. Cette disposition est regrettable, puisqu'elle implique que la qualité des données à caractère personnel, qui est également essentielle aux fins de la répression, ne sera pleinement garantie que lorsque ces données seront transmises à d'autres États membres ou mises à la disposition de ceux-ci, mais pas lorsqu'elles sont traitées à l'intérieur d'un État membre donné ([1]). Il est pourtant essentiel — aussi bien dans l'intérêt de la personne concernée que dans celui des autorités compétentes — de veiller à ce que la qualité de toutes les données à caractère personnel, y compris celles qui ne sont pas transmises ou mises à disposition par un autre État membre, soient vérifiées de manière appropriée.

87. C'est pourquoi le CEPD recommande de supprimer en tout cas la limitation du champ d'application de l'article 9, paragraphes 1 et 6, en transférant ces dispositions au chapitre II de la proposition.

Distinction entre différentes catégories de données

88. L'article 4, paragraphe 3, dispose que le responsable du traitement est tenu de distinguer clairement les données à caractère personnel en fonction de différentes catégories de personnes (les personnes suspectes, les personnes condamnées, les témoins, les victimes, les personnes pouvant fournir des renseignements et les autres personnes). Le CEPD est favorable à cette approche. Les services de police et les autorités judiciaires pouvant être amenés à traiter des données relatives à des catégories de personnes très diverses, il est essentiel de distinguer ces données selon les différents degrés d'implication dans une infraction pénale. En particulier, les conditions de collecte des données, la durée de conservation, les conditions auxquelles l'accès ou l'information est refusé à la personne concernée ainsi que les modalités d'accès des autorités compétentes aux données devraient tenir compte de la spécificité des diverses catégories de données traitées et des différentes finalités pour lesquelles ces données sont collectées par les services de police et les autorités judiciaires.

89. À cet égard, le CEPD demande qu'une attention particulière soit accordée aux données relatives aux personnes non suspectes. Des conditions et des mesures de protection spécifiques sont nécessaires pour garantir le respect de la proportionnalité et éviter de porter préjudice à des personnes qui ne sont pas impliquées activement dans une infraction pénale. Pour cette catégorie de personnes, la proposition devrait contenir des dispositions supplémentaires visant à limiter les finalités du traitement, à fixer des durées de conservation précises et à restreindre l'accès aux données. Le CEPD recommande de modifier la proposition en conséquence.

([1]) De plus, cela ne serait pas conforme à la recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police adoptée par le Conseil de l'Europe. Son principe 7.2 prévoit notamment que des «contrôles périodiques» sur la qualité des données à caractère personnel devraient être établis en accord avec l'autorité de contrôle ou conformément au droit interne.

90. Le libellé actuel de la proposition contient une mesure de protection relative aux personnes non suspectes, à savoir l'article 7, paragraphe 1. Le CEPD estime qu'il s'agit d'une protection importante, essentiellement parce que les États membres ne sont pas autorisés à prévoir des dérogations. Malheureusement, cet article prévoit des mesures de protection spécifiques uniquement pour la durée de conservation, et son applicabilité est limitée à la catégorie de personnes visée à l'article 4, paragraphe 3, dernier tiret, de la proposition. Dès lors, les garanties qu'il établit ne sont pas suffisantes et il ne s'applique pas à l'ensemble des personnes non suspectes ([1]).

91. Les données relatives aux personnes condamnées doivent également faire l'objet d'une attention spéciale. En effet, en ce qui concerne ce type de données, il y a lieu de tenir dûment compte des initiatives récentes et futures relatives aux échanges d'informations extraites du casier judiciaire et de veiller à préserver une cohérence d'ensemble ([2]).

92. À la lumière des observations qui précèdent, le CEPD recommande d'ajouter à l'article 4 un paragraphe contenant les éléments suivants:

— des dispositions supplémentaires visant à limiter les finalités du traitement, à fixer des durées de conservation précises et à restreindre l'accès aux données, en ce qui concerne les personnes non suspectes;

— l'obligation, pour les États membres, de prévoir les conséquences sur le plan légal des distinctions à établir dans les données à caractère personnel en fonction des différentes catégories de personnes, en tenant compte de la spécificité des diverses catégories de données traitées et des différentes finalités pour lesquelles ces données sont collectées par les services de police et les autorités judiciaires;

— les conséquences sur le plan légal devraient concerner les conditions de collecte des données, la durée de conservation, le transfert et l'utilisation ultérieurs ainsi que les conditions auxquelles l'accès aux données ou la fourniture d'informations peuvent être refusés à la personne concernée.

IV.7 **Durée de conservation des données à caractère personnel**

93. Les principes généraux régissant la durée de conservation des données à caractère personnel sont énoncés à l'article 4, paragraphe 1, point e), et à l'article 7, paragraphe 1, de la proposition. En règle générale, les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées. Ce principe est conforme à la législation de l'UE en matière de protection des données ([3]).

94. Cependant, la règle générale énoncée à l'article 7, paragraphe 1, ne s'applique pas en cas de «disposition contraire du droit national.» Le CEPD est d'avis que cette exception est très large et qu'elle va plus loin que les exceptions autorisées en vertu de l'article 4, paragraphe 1, point e). Il propose de supprimer l'exception générale prévue à l'article 7, paragraphe 1, ou au moins de limiter expressément les intérêts publics justifiant le recours à cette dérogation par les États membres ([4]).

95. L'article 7, paragraphe 2, dispose que le respect des durées de conservation est garanti par des mesures procédurales et techniques appropriées et fait l'objet d'un contrôle régulier. Le CEPD se félicite de cette disposition, mais recommande de prévoir expressément que ces mesures incluent l'effacement automatique et périodique des données à caractère personnel après un certain temps.

IV.8 **Échanges de données à caractère personnel avec des pays tiers**

96. L'efficacité de la coopération policière et judiciaire à l'intérieur des frontières de l'UE dépend de plus en plus de la coopération avec les pays tiers et les organisations internationales. Nombre de mesures visant à améliorer la coopération policière et judiciaire avec des pays tiers ou des organisations internationales sont actuellement examinées ou prévues à l'échelle nationale ou de l'UE ([5]). Le renforcement de cette coopération internationale devrait recourir largement à l'échange de données à caractère personnel.

97. Dès lors, il est essentiel que les principes de traitement loyal et licite — ainsi que les principes liés au respect des procédures en général — s'appliquent également à la collecte et à l'échange de données à caractère personnel sur l'ensemble du territoire de l'UE, et que les données à caractère personnel ne soient transférées à des pays tiers ou des organisations internationales que si ces tiers garantissent un niveau de protection adéquat ou des mesures de protection appropriées.

([1]) Voir le point 94 du présent avis pour plus de précisions.

([2]) La décision 2005/876/JAI du Conseil relative à l'échange d'informations extraites du casier judiciaire a pris effet le 9 décembre. Elle complète et facilite les mécanismes existants de transmission des informations relatives aux condamnations qui se fondent sur les dispositions conventionnelles en vigueur, notamment celles qui figurent dans la Convention européenne d'entraide judiciaire en matière pénale de 1959 et dans la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de 2000. Ce texte sera ultérieurement remplacé par une décision-cadre du Conseil plus spécifique. La Commission a l'intention de proposer une nouvelle décision-cadre dans ce domaine.

([3]) En plus de la règle générale sur la durée de conservation des données à caractère personnel énoncée à l'article 7, la proposition établit des dispositions spécifiques pour les données à caractère personnel échangées avec d'autres États membres. En particulier, l'article 9, paragraphe 7, dispose que les données à caractère personnel sont effacées:
1) si ces données n'auraient pas dû être transmises, mises à disposition ou reçues;
2) à l'expiration d'un délai communiqué par l'autorité transmettrice, sauf si ces données restent nécessaires à des fins de procédure judiciaire;
3) si ces données ne sont pas ou plus nécessaires pour la finalité pour laquelle elles ont été transmises.

([4]) On pourrait se limiter à la lutte contre le terrorisme et/ou aux intérêts publics visés à l'article 4, paragraphe 1, point e): l'utilisation à des fins historiques, statistiques ou scientifiques.

([5]) Voir, par exemple, la récente communication de la Commission intitulée «Une stratégie relative à la dimension externe de l'espace de liberté, de sécurité et de justice» (COM (2005) 491 final).

Transfert de données à caractère personnel à des pays tiers

98. Dans ce contexte, le CEPD accueille avec satisfaction l'article 15 de la proposition, qui prévoit une protection en cas de transfert aux autorités compétentes de pays tiers ou à des organisations internationales. Cependant, cette disposition, qui figure au chapitre III de la proposition, ne s'applique qu'aux données reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci. À cause de cette limitation, le système de protection des données à l'échelle de l'Union européenne continue à présenter une lacune pour ce qui est des données qui n'émanent pas d'une autorité compétente d'un autre État membre. Le CEPD juge que cette lacune est inacceptable pour les raisons exposées ci-après.

99. Premièrement, le niveau de protection garanti par la législation de l'UE en cas de transfert à un pays tiers ne devrait pas être déterminé en fonction de la source des données — selon qu'il s'agit d'un service de police de l'État membre qui transfère les données audit pays tiers ou d'un service de police d'un autre État membre.

100. Deuxièmement, il convient de noter que les règles régissant le transfert de données à caractère personnel à des pays tiers constituent un des principes fondamentaux de la législation en matière de protection des données. Ce principe ne constitue pas uniquement une des dispositions fondamentales de la directive 95/46/CE; il est en outre consacré par le protocole additionnel de la Convention n° 108 ([1]). Le respect des normes communes visant à assurer la protection des données à caractère personnel mentionnées à l'article 1er de la proposition ne peut être garanti si les règles communes applicables aux transferts de données à caractère personnel à des pays tiers ne portent pas sur tout l'éventail des traitements. En conséquence, le transfert de données à caractère personnel à des pays tiers ne garantissant pas un niveau de protection adéquat, s'il était possible, constituerait une atteinte directe aux droits de la personne concernée, tels qu'ils sont garantis dans la proposition.

101. Troisièmement, la limitation du champ d'application des ces règles aux «données échangées» signifierait en ce qui concerne les données traitées dans un seul pays — qu'il n'y aurait aucune mesure de protection. Paradoxalement, les données à caractère personnel pourraient être transférées à des pays tiers — au mépris de toute règle visant la protection adéquate des données à caractère personnel — plus «facilement» qu'elles ne pourraient être transmises à d'autres États membres. Cela fournirait des possibilités de «blanchiment de l'information». Les autorités compétentes des États membres pourraient contourner les règles strictes en matière de protection des données en transférant des données à des pays tiers ou des organisations internationales. Ces données deviendraient alors accessibles aux autorités compétentes d'un autre État membre et elles pourraient même être transmises en retour à ces autorités.

102. Dès lors, le CEPD recommande de modifier cette proposition de façon à ce que l'article 15 s'applique à l'échange de *toutes* les données à caractère personnel avec des pays tiers. Cette recommandation ne porte pas sur l'article 15, paragraphe 1, point c), qui, par nature, ne peut s'appliquer qu'aux données à caractère personnel échangées avec d'autres États membres.

Transferts exceptionnels vers des pays qui n'offrent pas un niveau adéquat de protection

103. L'article 15 prévoit une série de conditions pour les transferts aux autorités compétentes de pays tiers ou aux organisations internationales, qui sont comparables à celles énoncées à l'article 25 de la directive 95/46/CE. L'article 15, paragraphe 6, prévoit néanmoins la possibilité de transférer des données à des pays tiers ou des organisations internationales n'assurant pas un niveau adéquat de protection des données, en cas d'absolue nécessité afin de sauvegarder les intérêts essentiels d'un État membre, ou à des fins de prévention de menaces imminentes graves à l'encontre de la sécurité publique ou d'une ou de plusieurs personnes en particulier.

104. Les conditions d'applicabilité de l'exception prévue au paragraphe 6 devraient être précisées. À cet effet, le CEPD recommande de préciser que:

— cette exception permet de déroger uniquement au critère de «protection adéquate», sans préjudice des autres critères énumérés à l'article 15, paragraphe 1;

— les transferts de données effectués en vertu de cette exception doivent satisfaire à des conditions appropriées (comme par exemple la condition explicite que les données doivent être traitées uniquement temporairement et pour des finalités spécifiques) et être notifiés à l'autorité de contrôle compétente.

Traitement de données à caractère personnel reçues de pays tiers

105. Dans le cadre de l'augmentation des échanges de données à caractère personnel avec les services de police et les autorités judiciaires de pays tiers, il y a lieu d'accorder aussi une attention particulière aux données à caractère personnel «importées» de ces pays tiers lorsque le respect de normes adéquates de respect des droits de l'homme — en particulier en ce qui concerne la protection des données à caractère personnel — n'est pas garanti.

([1]) Le protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et le flux transfrontalier de données a été signé le 8 novembre 2001 et est entré en vigueur le 1er juillet 2004. Cet instrument juridique international contraignant a été signé à ce jour par 11 États, dont 9 sont membres de l'UE. L'article 2, paragraphe 1, du protocole établit le principe général selon lequel «Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un État ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet État ou cette organisation assure un niveau de protection adéquat pour le transfert considéré.»

106. Dans un contexte plus large, le CEPD estime que le législateur devrait faire en sorte que les données à caractère personnel reçues de pays tiers soient au moins conformes aux normes internationales en matière de respect des droits de l'homme. Par exemple, les données obtenues sous la torture ou moyennant une violation des droits de l'homme et les listes noires basées uniquement sur les convictions politiques ou l'orientation sexuelle ne devraient pas être traitées ni prises en compte par les services de police et les autorités judiciaires, à moins de servir les intérêts de la personne concernée. Dès lors, le CEPD recommande que cet aspect soit clarifié au moins dans un considérant de la proposition, éventuellement en faisant référence à des instruments internationaux pertinents ([1]).

107. En ce qui concerne plus particulièrement la protection des données à caractère personnel, le CEPD fait observer que, lorsque de telles données sont transférées par des pays dans lesquels il n'existe aucune norme ni garantie adéquate en ce qui concerne la protection de ce type de données, il y a lieu d'évaluer dûment si la qualité des données n'est pas insuffisante, afin d'éviter que des services répressifs de l'UE se fondent à tort sur ces données et que la personne concernée subisse un préjudice.

108. En conséquence, le CEPD recommande d'ajouter à l'article 9 de la proposition une disposition selon laquelle la qualité des données à caractère personnel transférées par des pays tiers doit faire l'objet d'une évaluation spécifique dès leur réception, le degré d'exactitude et de fiabilité de ces données devant être indiqué.

IV.9 **Échange de données à caractère personnel avec des personnes privées et des autorités autres que les services répressifs**

109. Les articles 13 et 14 de la proposition prévoient une série d'obligations à respecter lorsque des données à caractère personnel sont transmises ultérieurement à des personnes privées et à des autorités autres que les services répressifs. Comme il a été indiqué plus haut, ces articles complètent les conditions plus générales établies au chapitre II, qui doivent de toute façon être appliquées.

110. Le CEPD est d'avis que, si la transmission à des personnes privées et à d'autres services publics peut s'avérer nécessaire, en particulier aux fins de prévenir et de lutter contre la criminalité, elle doit néanmoins être soumise à des conditions spécifiques strictes. Cela rejoint l'avis des commissaires européens à la protection des données tel qu'il figure dans le document de synthèse de Cracovie ([2]).

111. Dans ce sens, le CEPD considère que les conditions supplémentaires énoncées aux articles 13 et 14 pourraient être jugées satisfaisantes si elles sont appliquées conjointement avec les conditions générales fixées au chapitre II, et notamment moyennant l'application généralisée des règles en matière de traitement ultérieur (voir plus haut, IV.2). La proposition actuelle limite cependant l'applicabilité des articles 13 et 14 aux données à caractère personnel transmises ou mises à disposition par les autorités compétentes d'un autre État membre.

112. L'applicabilité générale des conditions supplémentaires susmentionnées est d'autant plus importante que les échanges de données entre les services répressifs et les autres autorités ou les personnes privées, y compris à l'intérieur des différents États membres, se multiplient. Les partenariats public-privé dans le cadre des activités de répression en sont une illustration ([3]).

113. Le CEPD recommande donc de modifier la proposition de façon à ce que les articles 13 et 14 s'appliquent à l'échange de *toutes* les données à caractère personnel, y compris celles qui ne sont pas transmises ou mises à disposition par un autre État membre. Cette recommandation ne vaut pas pour l'article 13, sous c), ni pour l'article 14, sous c).

Accès aux données à caractère personnel contrôlées par des personnes privées et utilisation ultérieure des ces données

114. L'échange de données à caractère personnel avec des personnes privées est à double sens. Il implique aussi que des données à caractère personnel sont transmises à des services répressifs et des autorités judiciaires ou mises à la disposition de ceux-ci par les personnes privées.

115. Dans ce cas, des autorités publiques accèdent à des données à caractère personnel qui ont été collectées à des fins commerciales (transactions commerciales, marketing, fourniture de services etc.) et sont gérées par des responsables du traitement privés, et utilisent ultérieurement ces données pour les finalités très différentes, que constituent la prévention et la détection des infractions pénales, et les enquêtes et les poursuites en la matière. De plus, l'exactitude et la fiabilité des données traitées à des fins commerciales doivent être évaluées avec soin lorsque ces données sont utilisées à des fins de répression ([4]).

([1]) La Convention des Nations unies contre la torture et autres peines ou traitements cruels, inhumains ou dégradants, signée par tous les États membres de l'UE et entrée en vigueur le 26 juin 1987, dont, en particulier, l'article 15 dispose que «Tout État partie veille à ce que toute déclaration dont il est établi qu'elle a été obtenue par la torture ne puisse être invoquée comme un élément de preuve dans une procédure, si ce n'est contre la personne accusée de torture pour établir qu'une déclaration a été faite».

([2]) *Document de synthèse sur la répression et l'échange d'informations dans l'UE (Position paper on Law Enforcement and Information Exchange in the EU)*, adopté par la Conférence de printemps des commissaires européens à la protection des données, Cracovie, 25 et 26 avril 2005.

([3]) Voir le programme législatif et de travail de la Commission pour 2006 - COM (2005) 531 final

([4]) Par exemple, une facture téléphonique est fiable pour des finalités commerciales, pour autant que les appels effectués y soient correctement mentionnés. Quoi qu'il en soit, il est possible que les services répressifs ne puissent pas entièrement se fier à cette même facture pour prouver de façon concluante qu'une personne déterminée a effectué un appel téléphonique.

116. Un exemple très récent et très important d'accès à des bases de données privées à des fins de répression est le texte (récemment approuvé) de la directive sur la conservation des données de communication (voir plus haut, points 16 à 18). Cette directive oblige les fournisseurs de services de communications électroniques accessibles au public ou de réseaux de communications publics à stocker pendant une période pouvant aller jusqu'à deux ans certaines données relatives aux communications, afin de garantir que ces données soient disponibles à des fins de détection des infractions pénales graves et d'enquêtes et de poursuites en la matière. Selon ce texte, les questions ayant trait à l'accès à ces données sortent du cadre du droit communautaire et pourraient ne pas être soumises à la directive même. Ces questions importantes peuvent toutefois faire l'objet d'une législation nationale ou de mesures adoptées en vertu du titre VI du traité sur l'Union européenne ([1]).

117. Dans son avis sur le texte de la proposition concernant la directive susmentionnée, le CEPD a plaidé en faveur d'une interprétation large du traité CE, car une restriction de l'accès est nécessaire pour garantir une protection adéquate de la personne dont les données de communication doivent être conservées. Malheureusement, le législateur européen n'a pas inclus de dispositions relatives à l'accès dans la directive susmentionnée.

118. Dans le présent avis, le CEPD réaffirme sa préférence marquée pour l'établissement, dans le cadre du droit de l'UE, de normes communes sur l'accès des services répressifs aux données et leur utilisation ultérieure par ces services. Tant que cet aspect n'est pas traité dans le premier pilier, un instrument relevant du troisième pilier pourrait prévoir la protection nécessaire. Cette position du CEPD se trouve encore renforcée par l'augmentation générale des échanges de données entre États membres et par la récente proposition relative au principe de disponibilité. Des dispositions nationales différentes en matière d'accès et d'utilisation ultérieure ne seraient pas compatibles avec la «libre circulation», à l'échelle de l'UE, des informations en matière répressive qui est proposée et qui vise également les données provenant de bases de données privées.

119. Dès lors, le CEPD estime que des normes communes devraient s'appliquer à l'accès des services répressifs aux données à caractère personnel détenues par des personnes privées, de façon à garantir que l'accès ne soit autorisé que sur la base de conditions et de restrictions clairement définies. En particulier, les autorités compétentes ne devraient pouvoir accéder aux données qu'au cas par cas, dans des circonstances précises et pour des finalités données et cet accès devrait faire l'objet d'un contrôle juridictionnel dans les États membres.

([1]) Un des considérants de cette directive prévoit que «Les questions relatives à l'accès aux données conservées en application de la présente directive par les autorités publiques nationales aux fins des activités visées à l'article 3, paragraphe 2, premier tiret, de la directive 95/46/CE ne relèvent pas du droit communautaire. Elles peuvent toutefois faire l'objet d'une législation nationale ou de mesures relevant du titre VI du traité sur l'Union européenne, étant entendu qu'une telle législation ou mesure doit pleinement respecter les droits fondamentaux tels qu'ils découlent des traditions constitutionnelles communes des États membres et tels qu'ils sont consacrés par la Convention européenne des droits de l'homme. L'article 8 de celle-ci, tel qu'interprété par la Cour européenne des droits de l'homme (…)».

IV.10 **Droits de la personne concernée**

120. Le chapitre IV établit des règles concernant les droits de la personne concernée, qui sont en général compatibles avec la législation en vigueur en matière de protection des données et l'article 8 de la Charte des droits fondamentaux de l'UE.

121. Le CEPD juge ces règles satisfaisantes, étant donné qu'elles confèrent une série de droits harmonisés aux personnes concernées, tout en tenant compte de la spécificité du traitement par les services de police et les autorités judiciaires. Il s'agit d'un grand progrès, étant donné qu'il existe actuellement une multitude de règles et de pratiques, surtout en ce qui concerne le droit d'accès. Certains États membres ne permettent pas à la personne d'accéder directement aux données qui la concernent, mais ont mis en place un système «d'accès indirect» (en l'occurrence, c'est l'autorité nationale de protection des données qui exerce le droit d'accès au nom de la personne concernée).

122. Cette proposition harmonise les dérogations au droit d'accès direct, ce qui permet aux citoyens de se prévaloir d'une série de droits harmonisés en tant que personne concernée au sens de la proposition, quel que soit l'État membre dans lequel les données sont collectées ou traitées. Cela est d'autant plus important que les données à caractère personnel sont de plus en plus traitées et échangées par les autorités compétentes de différents États membres de l'UE ([2]).

123. Le CEPD reconnaît qu'il y a lieu de limiter les droits de la personne concernée si cela s'avère nécessaire aux fins de la prévention et de la détection des infractions pénales et des enquêtes et poursuites en la matière. De toute manière, ces limitations devant être considérées comme des dérogations aux droits fondamentaux de la personne concernée, une condition stricte de proportionnalité doit être mise en œuvre. En d'autres termes, les dérogations doivent être limitées et bien définies, et les limitations doivent, dans la mesure du possible, être partielles et temporaires.

124. À cet égard, le CEPD attire l'attention du législateur en particulier sur l'article 19, paragraphe 2, point a), sur l'article 20, paragraphe 2, point a), et sur l'article 21, paragraphe 2, point a), qui prévoient une dérogation très large et très vague aux droits de la personne concernée, en disposant que ces droits peuvent être limités si cela s'avère nécessaire «pour permettre au responsable du traitement d'accomplir ses tâches légales de manière satisfaisante». De plus, cette dérogation se recoupe avec la disposition du point b), qui autorise la limitation des droits de la personne concernée lorsque cela s'avère nécessaire

([2]) En particulier, le chapitre VI traite du droit à l'information (articles 19 et 20) et du droit d'accès, de rectification, d'effacement ou de verrouillage (article 21). En principe, ces articles confèrent à la personne concernée tous les droits dont elle jouit habituellement en vertu de la législation de l'UE en matière de protection des données, tout en prévoyant une série d'exceptions afin de tenir compte de la spécificité du troisième pilier. En particulier, des limitations des droits de la personne concernée sont autorisées, par des dispositions quasiment identiques, pour ce qui est du droit à l'information (article 19, paragraphe 2, et article 20, paragraphe 2) et du droit d'accès (article 21, paragraphe 2).

«pour éviter de compromettre des enquêtes, recherches ou procédures en cours, ou de nuire à l'accomplissement par les autorités compétentes de leurs tâches légales». Si cette dernière dérogation peut sembler justifiée, en revanche la première implique une limitation disproportionnée des droits de la personne concernée. Dès lors, le CEPD recommande de supprimer l'article 19, paragraphe 2, point a), l'article 20, paragraphe 2, point a), et l'article 21, paragraphe 2, point a).

125. De plus, le CEPD recommande d'améliorer les articles 19, 20 et 21 en:

— précisant que les limitations des droits de la personne concernée ne sont pas obligatoires, qu'elles ne s'appliquent pas indéfiniment et qu'elles ne sont autorisées «que» dans les cas précis énumérés dans les articles susmentionnés;

— tenant compte du fait que les informations devraient être fournies spontanément par le responsable du traitement et non à la demande de la personne concernée;

— précisant à l'article 19, paragraphe 1, point c), que des informations devraient également être fournies sur la «durée de conservation des données»;

— garantissant (en modifiant l'article 20, paragraphe 1, de manière à l'aligner sur les autres instruments de l'UE en matière de protection des données) que les informations — lorsque les données n'ont pas été collectées auprès de la personne concernée ou ont été obtenues de sa part sans qu'elle en ait connaissance — sont fournies à cette personne «au plus tard au moment de la première communication de données»;

— faisant en sorte que le mécanisme de recours contre un refus ou une limitation des droits de la personne concernée soit applicable aux cas de restriction du droit à l'information et en modifiant la dernière phrase de l'article 19, paragraphe 4, en conséquence.

Décisions individuelles automatisées

126. Le CEPD regrette que la question importante des décisions individuelles automatisées ne soit pas du tout abordée dans la proposition. En fait, dans la pratique, l'expérience montre que les services répressifs utilisent de plus en plus le traitement automatisé des données afin d'évaluer certains aspects personnels, en particulier pour apprécier la fiabilité et le comportement des personnes.

127. Le CEPD — tout en reconnaissant que ces systèmes peuvent s'avérer nécessaires dans certains cas, pour rendre les activités en matière de répression plus efficaces — note que les décisions fondées uniquement sur le traitement automatisé de données devraient être soumises à des conditions et des mesures de protection très strictes lorsqu'elles produisent des effets juridiques à l'égard d'une personne ou lorsqu'elles affectent considérablement une personne. Cette exigence est d'autant plus importante dans le cadre du troisième pilier, étant donné que dans ce contexte les autorités compétentes sont investies de pouvoirs de police et que, de ce fait, leurs décisions et leurs actions sont susceptible d'affecter des personnes ou risquent d'être plus intrusives que ne le sont en général les décisions ou les actions des personnes privées.

128. En particulier, conformément aux principes généraux en matière de protection des données, ces décisions ou actions ne devraient être permises que si elles sont expressément prévues par un texte de loi ou autorisées par l'autorité de contrôle compétente, et devraient faire l'objet de mesures appropriées visant à protéger les intérêts légitimes de la personne concernée. De plus, la personne concernée devrait avoir facilement accès à des moyens qui lui permettent de donner son avis et être en mesure de connaître la logique qui sous-tend la décision, sauf si cela n'est pas compatible avec la finalité pour laquelle les données sont traitées.

129. Dès lors, le CEPD recommande de prévoir une disposition spécifique sur les décisions individuelles automatisées qui soit conforme à la législation actuelle de l'UE en matière de protection des données.

IV.11 **Sécurité du traitement**

130. En ce qui concerne la sécurité du traitement, l'article 24 prévoit l'obligation, pour le responsable du traitement, de mette en œuvre des mesures techniques et d'organisation appropriées, qui soient conformes aux dispositions des autres instruments de l'UE en matière de protection des données. De plus, le paragraphe 2 contient une liste détaillée et complète des mesures qui doivent être mises en œuvre en ce qui concerne le traitement automatisé de données.

131. Le CEPD se félicite de cette disposition, mais suggère, en vue de faciliter un contrôle efficace par les autorités de contrôle, d'ajouter à la liste de mesures figurant au paragraphe 2, la mesure supplémentaire suivante: «*k) appliquer des mesures permettant de surveiller l'efficacité de ces mesures de sécurité et d'en rendre compte, d'une façon systématique (mécanisme d'audit interne systématique des mesures de sécurité)*» [1].

Enregistrement des données dans un journal (logging)

132. L'article 10 dispose que chaque transmission et chaque réception de données à caractère personnel (en cas de transmission automatisée) soit enregistrée dans un journal ou qu'une trace documentaire de chaque transmission et de chaque réception de données à caractère personnel soit conservée (dans le cas d'une transmission non automatisée), afin de permettre la vérification ultérieure de la licéité de la transmission et du traitement des données. Ces informations doivent être mises à la disposition de l'autorité de contrôle compétente sur demande.

[1] Dans la même ligne de pensée, voir l'avis du contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, COM (2004) 835 final, publié à l'adresse www.edps.eu.int.

133. Le CEPD accueille cette disposition avec satisfaction. Il note cependant que, afin de garantir un contrôle global et de pouvoir vérifier la bonne utilisation des données à caractère personnel, il faut également que «l'accès» aux données soit enregistré dans un journal ou qu'il en soit conservé une trace documentaire. Ces informations sont essentielles, étant donné qu'un contrôle efficace du traitement des données à caractère personnel ne doit pas être axé uniquement sur la licéité de la transmission de données à caractère personnel d'une autorité à l'autre, mais doit également porter sur la licéité de l'accès de ces autorités aux données ([1]). Dès lors, le CEPD recommande de modifier l'article 10 de façon à prévoir que l'accès aux données soit lui aussi enregistré dans un journal ou qu'il soit conservé aussi une trace documentaire de l'accès aux données.

IV.12 **Recours juridictionnels, responsabilité et sanctions**

134. Le chapitre VI de la proposition traite des recours juridictionnels (article 27), de la responsabilité (article 28) et des sanctions (article 29). Les dispositions concernées sont en général compatibles avec la législation de l'UE en vigueur en matière de protection des données.

135. En particulier, en ce qui concerne les sanctions, le CEPD accueille favorablement le fait qu'il soit précisé que les sanctions doivent être effectives, proportionnées et dissuasives en cas de violation des dispositions prises en application de la décision-cadre. De plus, les sanctions pénales en cas d'infractions commises intentionnellement et correspondant à des atteintes graves — spécialement en ce qui concerne la confidentialité et la sécurité du traitement — auront un plus grand effet dissuasif contre les violations graves de la législation en matière de protection des données.

IV.13 **Activités de contrôle, supervision et consultation**

136. Les dispositions de la proposition qui traitent du contrôle du traitement des données, ainsi que celles qui ont trait à la consultation sur les questions liées au traitement des données, ressemblent dans une large mesure aux dispositions de la directive 95/46/CE. Le CEPD salue le fait que la Commission ait retenu, dans sa proposition, des mécanismes qui ont déjà été testés et qui fonctionnent bien, et souligne en particulier l'introduction d'un système (obligatoire) de contrôles préalables. Ce système est non seulement prévu dans la directive 95/46/CE, mais aussi inclus dans le règlement (CE) nº 45/2001. Il s'agit d'un instrument efficace dont dispose le CEPD pour contrôler le traitement des données effectué par les institutions et organes communautaires.

137. La nomination par les responsables du traitement de délégués à la protection des données est un instrument de contrôle du traitement des données qui s'est lui aussi avéré efficace. Il est utilisé dans plusieurs États membres. Il est établi dans le règlement (CE) nº 45/2001 en tant qu'instrument obligatoire et il joue un rôle essentiel au niveau des Communautés européennes. Les délégués à la protection des données sont des administrateurs au sein d'une organisation qui assurent, d'une manière indépendante, l'application interne des dispositions en matière de protection des données.

138. Le CEPD recommande d'ajouter à cette proposition des dispositions relatives aux délégués à la protection des données. Ces dispositions pourraient s'inspirer des articles 24 à 26 du règlement (CE) nº 2001/45.

139. Cette proposition de décision-cadre s'adresse aux États membres. Il est donc logique que son article 30 prévoie un contrôle par des autorités de contrôle indépendantes. Cet article est rédigé d'une façon semblable à l'article 28 de la directive 95/46/CE. Les autorités nationales devraient coopérer entre elles, ainsi qu'avec les autorités de contrôle communes instituées en vertu du titre VI du traité sur l'UE et avec le CEPD. De plus, l'article 31 de la proposition prévoit la création d'un groupe qui doit jouer un rôle semblable à celui que joue le groupe de l'article 29 dans le cadre du premier pilier. Tous les acteurs importants du domaine de la protection des données sont mentionnés à l'article 31 de la proposition.

140. Il est évident que la coopération entre tous les acteurs importants du domaine de la protection des données joue un rôle important dans une proposition qui a pour but d'améliorer la coopération policière et judiciaire entre les États membres. Le CEPD se félicite donc de ce que la proposition mette l'accent sur la coopération entre les autorités de contrôle.

141. Par ailleurs, le CEPD souligne la nécessité d'une approche cohérente en matière de protection des données. Pour augmenter cette cohérence, on pourrait promouvoir la communication entre le groupe de l'article 29 existant et le groupe créé par cette proposition de décision-cadre. Le CEPD recommande de modifier l'article 31, paragraphe 2, de la proposition, de façon à autoriser aussi le président du groupe de l'article 29 à participer aux réunions du nouveau groupe ou à y être représenté.

142. Le libellé de l'article 31 de cette proposition présente une différence notable avec l'article 29 de la directive 95/46/CE. Le CEPD est un membre à part entière du groupe de l'article 29 et jouit du droit de vote au sein de ce groupe. Cette proposition prévoit également que le CEPD est membre du groupe (en vertu de l'article 31), mais ne lui accorde pas le droit de vote. Il n'apparaît pas clairement pour quelle raison cette proposition s'écarte de l'article 29 de la directive 95/46/CE. Le CEPD estime que le libellé proposé est ambigu en ce qui concerne son rôle, ce qui pourrait compromettre l'efficacité de sa participation aux travaux du groupe. Le CEPD recommande donc d'assurer la cohérence avec le libellé de la directive.

([1]) Ceci est conforme aux dispositions de l'article 18 de la proposition, selon lequel l'autorité transmettrice est informée à sa demande du traitement ultérieur des données à caractère personnel qu'elle a transmises ou mises à disposition, et de l'article 24 relatif à la mise en œuvre des mesures de sécurité, notamment en ce qui concerne le mécanisme d'audit interne systématique de ces mesures qui est proposé.

IV.14 **Autres dispositions**

143. Le chapitre VIII de la proposition contient un certain nombre de dispositions finales qui modifient la Convention de Schengen et d'autres instruments qui concernent le traitement et la protection des données à caractère personnel.

Convention de Schengen

144. L'article 33 de la proposition dispose que les articles 126 à 130 de la Convention de Schengen sont remplacés par cette décision pour ce qui est des domaines relevant du traité sur l'Union européenne. Les articles 126 à 130 de la Convention de Schengen contiennent des règles générales en matière de protection des données pour le traitement des données transmises en application de la Convention (mais en dehors du Système d'information Schengen).

145. Le CEPD accueille avec satisfaction cette substitution, dans la mesure où elle rend le régime de protection des données dans le cadre du troisième pilier plus cohérent et où elle constitue à certains égards une amélioration sensible de la protection des données à caractère personnel, notamment par le renforcement des compétences des autorités de contrôle. Cependant, cette substitution contribue involontairement — et malheureusement — à diminuer le niveau de protection des données en ce qui concerne certains autres aspects. En effet, certaines dispositions de la Convention de Schengen sont plus strictes que celles de la décision-cadre.

146. Le CEPD se réfère en particulier l'article 126, paragraphe 3, point b), de la Convention de Schengen, qui prévoit que les données ne peuvent être utilisées que par les autorités judiciaires, les services et instances qui assurent une tâche ou remplissent une fonction dans le cadre des finalités indiquées dans la Convention. Cette disposition semble exclure la transmission à des personnes privées, alors que la décision-cadre proposée l'autorise. Par ailleurs, les règles en matière de protection des données de la Convention de Schengen s'appliquent à *toutes* les données transmises depuis un fichier *non automatisé* ou intégrées dans un tel fichier (article 127), alors que les fichiers non structurés sont exclus du champ d'application de la décision-cadre proposée.

Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne

147. L'article 34 dispose que l'article 23 de la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne est remplacé par cette décision-cadre. Le CEPD note que cette substitution contribuerait, d'une manière générale, à améliorer la protection des données à caractère personnel échangées dans le cadre de la Convention, mais qu'elle pourrait aussi créer certains problèmes de compatibilité entre les deux instruments.

148. En effet, la Convention traite également de l'entraide judiciaire dans le domaine de l'interception des télécommunications. Dans ce cas, l'État membre requis peut donner son consentement — à l'interception ou à la transmission de l'enregistrement de télécommunications — sous réserve de toutes conditions qui devraient être respectées dans une affaire nationale similaire. Selon l'article 23, paragraphe 4, de la Convention, lorsque ces conditions supplémentaires concernent l'utilisation des données à caractère personnel, elles l'emportent sur les règles en matière de protection des données établies à l'article 23. De manière semblable, l'article 23, paragraphe 5, établit la primauté des dispositions supplémentaires relatives à la protection des informations obtenues par les équipes communes d'enquête. Le CEPD fait observer que, si l'article 23 est remplacé par la proposition actuelle, ou ne saura plus très bien si les dispositions supplémentaires susmentionnées demeurent applicables ou non. En conséquence, le CEPD recommande de clarifier ce point, en vue de mesurer précisément les conséquences du remplacement intégral de l'article 23 de la Convention par cette décision-cadre.

Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

149. L'article 34, paragraphe 2, dispose que toute référence à la convention n° 108 doit être interprétée comme étant une référence à cette décision-cadre. L'interprétation et l'applicabilité concrète de cette disposition sont loin d'être claires. En tout état de cause, le CEPD part du principe que cette disposition ne s'applique que dans les limites du champ d'application matériel de cette décision-cadre.

Questions finales

150. En ce qui concerne la cohérence d'ensemble de la proposition, le CEPD note qu'il serait préférable de déplacer certains articles au sein du texte de la proposition.

Dès lors, le CEPD suggère:

1. de transférer l'article 16 («Comité») du chapitre III («Formes spécifiques de traitement») vers un nouveau chapitre;

2. de transférer les articles 25 («Registre») et 26 («Contrôles préalables») du chapitre V («Confidentialité et sécurité du traitement») vers un nouveau chapitre.

V **CONCLUSIONS**

Un pas en avant considérable

a) L'adoption de cette proposition constituerait un pas en avant considérable pour la protection des données à caractère personnel dans un domaine important qui requiert, notamment, un mécanisme cohérent et efficace capable de garantir la protection des données à caractère personnel à l'échelle de l'Union européenne.

b) Une protection efficace des données à caractère personnel est non seulement importante pour les personnes concernées, mais elle contribue aussi au succès de la coopération policière et judiciaire à proprement parler. À de nombreux égards, ces deux intérêts publics vont de pair.

Normes communes

c) Le CEPD estime que ce nouveau cadre devrait non seulement respecter les principes de la protection des données énoncés dans la directive 95/46/CE — il importe de garantir la cohérence de la protection des données au sein de l'Union européenne -, mais aussi prévoir un ensemble complémentaire de règles tenant compte de la nature spécifique du domaine répressif.

d) Cette proposition remplit ces conditions, dans la mesure où elle garantit que les principes existants de la protection des données, tels qu'ils sont énoncés dans la directive 95/46/CE, s'appliquent dans le domaine du troisième pilier, étant donné que la plupart des dispositions de la proposition s'inspirent des autres instruments juridiques de l'UE en matière de protection des données à caractère personnel et sont compatibles avec ceux-ci. Elle définit par ailleurs des normes communes qui précisent ces principes en vue de leur application dans ce domaine, qui sont en général suffisantes pour fournir des mesures adéquates de protection des données dans le cadre du troisième pilier.

Applicabilité à tout l'éventail des traitements

e) Il est indispensable, pour la réalisation de son objectif, que la décision cadre s'applique à toutes les données policières et judiciaires, même si elles ne sont pas transmises ou mises à disposition par les autorités compétentes d'autres États membres.

f) L'article 30, paragraphe 1, point b) et l'article 31, paragraphe 1, point c) du traité UE constituent une base juridique pour l'adoption de règles relatives à la protection des données dont le champ d'application ne se limite pas à la protection des données à caractère personnel effectivement échangées entre les autorités compétentes des États membres, mais qui englobe aussi les situations internes.

g) La proposition ne s'applique pas au traitement réalisé dans le cadre du deuxième pilier du traité UE (politique étrangère et de sécurité commune), ni au traitement de données par les services de renseignement, ni à l'accès de ces services à ces données lorsque celles-ci sont traitées par les autorités compétentes ou d'autres parties (ceci découle de l'article 33 du traité UE). Dans ces domaines, le droit national doit garantir une protection appropriée des personnes concernées. Cette lacune en ce qui concerne la protection à l'échelle de l'UE exige une protection d'autant plus efficace dans les domaines qui relèvent, eux, de la proposition.

h) Le CEPD se réjouit du fait que la proposition englobe les données à caractère personnel traitées par les autorités judiciaires.

Lien avec les autres instruments juridiques

i) Chaque fois qu'un autre instrument juridique spécifique adopté en vertu du titre VI du traité UE prévoit des conditions ou des limitations plus précises en ce qui concerne l'accès aux données et leur traitement, cette législation plus spécifique devrait s'appliquer en tant que lex specialis.

j) Cette proposition de décision cadre relative à la protection des données est en soi justifiée et nécessaire, même si l'instrument juridique portant sur la disponibilité (tel qu'il a été proposé par le Commission le 12 octobre 2005) n'est pas adopté.

k) L'adoption de la directive sur la conservation des données de communications rend encore plus impérieuse la nécessité de mettre en place un cadre juridique relatif à la protection des données dans le cadre du troisième pilier.

Structure de la proposition

l) Les règles supplémentaires énoncées au chapitre II (qui complètent les principes généraux établis dans la directive 95/46/CE) devraient offrir aux personnes concernées une protection supplémentaire dans le cadre spécifique du troisième pilier, mais ces règles supplémentaires ne peuvent pas entraîner un niveau de protection inférieur.

m) Le chapitre III, qui porte sur les formes spécifiques de traitement (et qui comprend le troisième niveau de protection), ne peut pas déroger aux dispositions du chapitre II: les dispositions du chapitre III devraient offrir aux personnes concernées une protection supplémentaire dans les situations où interviennent les autorités compétentes de plusieurs États membres; ces dispositions ne peuvent toutefois pas entraîner un niveau de protection inférieur.

n) Les dispositions relatives à la vérification de la qualité des données (article 9, paragraphes 1 et 6) et celles réglementant le traitement ultérieur des données à caractère personnel (article 11, paragraphe 1) devraient être déplacées vers le chapitre II afin qu'elles s'appliquent à tous les traitements de données réalisés par les services répressifs, même si les données à caractère personnel n'ont pas été transmises ni mises à disposition par un autre État membre. En particulier, il est essentiel — aussi bien dans l'intérêt de la personne concernée que dans celui des autorités compétentes — de veiller à ce que la qualité de toutes les données à caractère personnel soit vérifiée de manière appropriée.

Limitation des finalités

o) La proposition ne tient pas compte de manière tout à fait satisfaisante d'une situation à laquelle les services de police peuvent être confrontés dans le cadre de leurs activités, à savoir la nécessité d'utiliser ultérieurement des données pour une finalité considérée comme incompatible avec celle pour laquelle elles ont été collectées.

p) Conformément au droit de l'UE relatif à la protection des données, les données à caractère personnel doivent être collectées pour des finalités déterminées et explicites, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Il faut autoriser une certaine souplesse en ce qui concerne l'utilisation ultérieure. La limitation relative à la collecte a plus de chances d'être correctement respectée si les autorités en charge de la sécurité intérieure savent qu'elles peuvent avoir recours, moyennant des garanties appropriées, à une dérogation concernant la limitation applicable à l'utilisation ultérieure.

q) Il conviendrait que la décision cadre prévoie, au chapitre II, que les États membres devraient avoir la possibilité de prendre des mesures législatives visant à autoriser le traitement ultérieur lorsqu'une telle mesure est nécessaire aux fins de:

— la prévention des menaces pour la sécurité publique, la défense ou la sécurité nationale;

— la protection d'un intérêt économique ou financier important d'un État membre;

— la protection de la personne concernée.

Ces compétences des États membres donnent lieu à un traitement portant atteinte à la vie privée. Elles devraient donc être assorties de conditions très strictes.

Nécessité et proportionnalité

r) Il convient de rendre les principes de nécessité et de proportionnalité de la proposition entièrement conformes à la jurisprudence de la Cour européenne des droits de l'homme, en faisant en sorte que le traitement de données à caractère personnel ne soit considéré comme nécessaire que lorsque les autorités compétentes peuvent démontrer qu'il est indispensable, et à condition qu'il ne soit pas possible de recourir à des mesures plus respectueuses de la vie privée.

Échanges de données à caractère personnel avec des pays tiers

s) Dans l'hypothèse où des données pourraient être transmises à un pays tiers sans que la protection de la personne concernée soit garantie, cela porterait gravement atteinte à la protection envisagée par la proposition considérée sur le territoire de l'Union européenne. Le CEPD recommande de modifier cette proposition de façon à ce que l'article 15 s'applique à l'échange de *toutes* les données à caractère personnel avec des pays tiers. Cette recommandation ne porte pas sur l'article 15, paragraphe 1, point c).

t) Lorsque des données à caractère personnel sont transmises par des pays tiers, il convient, avant de les utiliser, d'en évaluer avec soin la qualité au regard des critères du respect des droits de l'homme et des normes en matière de protection des données, avant qu'elles ne soient utilisées.

Échanges de données à caractère personnel avec des personnes privées et des autorités autres que les services répressifs

u) Si la transmission à des personnes privées et à d'autres services publics peut s'avérer nécessaire, en particulier aux fins de prévenir et de lutter contre la criminalité, elle doit néanmoins être soumise à des conditions spécifiques strictes. Le CEPD recommande de modifier la proposition de façon à ce que les articles 13 et 14 s'appliquent à l'échange de *toutes* les données à caractère personnel, y compris celles qui ne sont pas reçues d'un autre État membre ni mises à disposition par un tel État. Cette recommandation ne vaut pas pour l'article 13, sous c), ni pour l'article 14, sous c).

v) Des normes communes devraient s'appliquer à l'accès des services répressifs aux données à caractère personnel détenues par des personnes privées, de façon à garantir que l'accès ne soit autorisé que sur la base de conditions et de restrictions clairement définies.

Catégories de données particulières

w) Des garanties spécifiques devraient être prévues, notamment pour veiller à ce que:

— les données biométriques et les profils ADN ne soient utilisés que sur la base de normes techniques clairement définies et interopérables,

— il soit tenu dûment compte du niveau d'exactitude de ces données et que celui ci puisse être contesté par la personne concernée par des moyens facilement accessibles;

— le respect de la dignité des personnes soit totalement garanti.

Distinction entre différentes catégories de données

x) Les données à caractère personnel concernant différentes catégories de personnes (les personnes suspectes, les personnes condamnées, les victimes, les témoins, etc.) devraient être traitées selon des conditions et des mesures de protection adéquates différentes. Dès lors, le CEPD propose d'ajouter à l'article 4 un paragraphe contenant les éléments suivants:

— l'obligation, pour les États membres, de prévoir les conséquences sur le plan légal des distinctions à établir dans les données à caractère personnel en fonction des différentes catégories de personnes;

— des dispositions supplémentaires visant à limiter les finalités du traitement, à fixer des durées de conservation précises et à restreindre l'accès aux données, en ce qui concerne les personnes non suspectes.

Décisions individuelles automatisées

y) Les décisions fondées uniquement sur le traitement automatisé de données devraient être soumises à des conditions et des mesures de protection très strictes lorsqu'elles produisent des effets à l'égard d'une personne ou lorsqu'elles affectent considérablement une personne. Le CEPD recommande donc de prévoir des dispositions spécifiques sur les décisions individuelles automatisées qui soient semblables à celles de la directive 95/46/CE.

Autres recommandations

z) Le CEPD recommande:

— de reformuler le premier tiret de l'article 4, paragraphe 4, de manière à ce que la jurisprudence relative à l'article 8 de la convention européenne des droits de l'homme soit respectée, étant donné que la formulation proposée pour l'article 4, paragraphe 4, ne respecte pas les critères établis par la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la convention européenne des droits de l'homme;

— de supprimer la dérogation générale prévue à l'article 7, paragraphe 1, ou au moins de limiter expressément les intérêts publics justifiant le recours à cette dérogation par les États membres;

— de modifier l'article 10 de façon à prévoir que l'accès aux données soit lui aussi enregistré dans un journal ou qu'il soit conservé aussi une trace documentaire de l'accès aux données;

— de supprimer l'article 19, paragraphe 2, point a), l'article 20, paragraphe 2, point a) et l'article 21 paragraphe 2, point a);

— d'ajouter à cette proposition des dispositions relatives aux délégués à la protection des données. Ces dispositions pourraient s'inspirer des articles 24 à 26 du règlement (CE) n° 2001/45;

— de modifier l'article 31, paragraphe 2, de la proposition de façon à autoriser aussi le président du groupe de l'article 29 à participer aux réunions du nouveau groupe ou à y être représenté.

Fait à Bruxelles, le 19 décembre 2005.

Peter HUSTINX

Contrôleur européen de la protection des données