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 l'échange d'informations en vertu du principe de disponibilité (COM (2005) 490 final)

(2006/C 116/04)

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

1. La Commission a transmis au CEPD, par lettre datée du 12 octobre 2005, la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité. 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. Pour le CEPD, il convient de mentionner le présent avis dans le préambule de la décision-cadre.

2. Il faut replacer le présent avis dans le contexte décrit dans la partie II: il n'est pas sûr du tout que la proposition en question — ou l'approche qui y est adoptée à l'égard de la disponibilité — aboutira finalement à l'adoption d'un instrument juridique. De nombreux États membres préconisent d'autres approches.

3. Toutefois, il est évident que la question de la disponibilité des informations en matière répressive à travers l'UE — ou, plus généralement, l'échange de ces informations — figure parmi les priorités des États membres, au sein ou en-dehors du Conseil, et du Parlement européen.

4. Il est tout aussi évident que cette question revêt une très grande importance sous l'angle de la protection des données à caractère personnel, comme le montre le présent avis. Le CEPD rappelle que la Commission a présenté cette proposition en lien étroit avec 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, qui a fait l'objet d'un avis du CEPD rendu le 19 décembre 2005.

5. Le CEPD profitera du présent avis pour présenter des considérations générales et plus fondamentales sur l'échange d'informations en matière répressive et sur les approches envisageables pour régler cette question. Le CEPD espère que le présent avis contribuera à ce que la question de la protection des données soit dûment prise en considération lors des débats qui auront lieu.

6. Le CEPD pourra évidemment être à nouveau consulté ultérieurement, en fonction de l'évolution du parcours législatif de cette proposition, ainsi que sur d'autres propositions dans le même domaine.

II. LA PROPOSITION DANS SON CONTEXTE

7. Le principe de disponibilité est un nouveau principe juridique important qui a été introduit dans le programme de La Haye et selon lequel les informations nécessaires dans le cadre de la lutte contre la criminalité doivent pouvoir traverser sans entraves les frontières intérieures de l'UE. L'objectif de la proposition à l'examen est de mettre en œuvre ce principe dans un acte juridique contraignant.

8. L'échange d'informations policières entre les différents pays intéresse beaucoup le législateur, que ce soit à l'intérieur ou à l'extérieur du cadre de l'UE. Plusieurs initiatives récentes ont retenu l'attention du CEPD.

9. Premièrement, le 4 juin 2004, la Suède a proposé 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. Le Conseil a dégagé une orientation générale sur cette proposition lors de sa session du 1er décembre 2005.

10. Deuxièmement, le 27 mai 2005, sept États membres ont signé à Prüm (Allemagne) un traité relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et l'immigration illégale. Ce traité introduit entre autres des mesures visant à améliorer l'échange d'informations sur les profils ADN et les empreintes digitales. Tout État membre de l'Union européenne peut adhérer à ce traité. Les parties contractantes souhaitent incorporer les dispositions du traité dans le cadre juridique de l'Union européenne.

11. Troisièmement, la disponibilité des informations en matière répressive de part et d'autre des frontières intérieures de l'Union européenne se trouvera également facilitée par d'autres instruments juridiques, comme les propositions relatives à un système d'information Schengen de deuxième génération (SIS II), la proposition concernant l'accès en consultation au système d'information sur les visas (VIS) et la proposition de décision-cadre relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres. Il convient également de citer à cet égard la communication sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases de données, présentée par la Commission le 25 novembre 2005.

12. Vu l'existence de toutes ces initiatives, la présente proposition de décision-cadre relative à la disponibilité ne doit pas examinée isolément, mais il faut également prendre en considération les autres approches relatives à l'échange d'informations en matière répressive. Cela est d'autant plus important que la tendance actuelle au sein du Conseil est de privilégier les autres approches en matière d'échange d'informations et de disponibilité par rapport à la démarche générale proposée par la Commission dans la proposition qui nous occupe et dont le texte pourrait ne même pas aboutir sur la table du Conseil.

13. Par ailleurs, cette proposition est étroitement liée à la proposition de décision-cadre relative à la protection des données à caractère personnel. Le présent avis s'inscrit donc dans la même ligne que l'avis plus approfondi sur la décision-cadre précitée.

14. Dans son avis sur la proposition de décision-cadre relative à la protection des données à caractère personnel, le CEPD a souligné qu'un instrument juridique sur le principe de disponibilité ne devrait être adopté que s'il existe une protection adéquate des données. Selon le CEPD, un tel instrument juridique ne devrait pas être adopté sans garanties fondamentales en matière de protection des données.

15. Le CEPD adopte la même position à l'égard de l'adoption d'autres instruments juridiques visant à faciliter le flux des informations en matière répressive à travers les frontières intérieures de l'UE. Le CEPD se félicite donc que le Conseil et le Parlement européen aient accordé la priorité à la proposition de décision-cadre relative à la protection des données à caractère personnel déjà mentionnée.

III. LE PRINCIPE DE DISPONIBILITÉ

16. Le principe de disponibilité est en soi un principe simple. Les informations accessibles à certaines autorités dans un État membre doivent également être communiquées aux services équivalents des autres États membres. Ces informations doivent être échangées aussi rapidement et aussi facilement que possible entre les services des États membres et de préférence dans le cadre d'un accès en ligne.

17. Les difficultés résultent des conditions dans lesquelles le principe de disponibilité doit s'appliquer:

— Hétérogénéité de l'organisation de la police et de l'appareil judiciaire dans les États membres, avec des mécanismes différents de «freins et contrepoids».

— Diversité des types d'informations (sensibles) (ADN ou empreintes digitales, par exemple).

— Diversité des moyens d'accès à l'information recherchée par les services compétents, y compris à l'intérieur des États membres.

— Il est difficile de s'assurer que les informations en provenance d'un autre État membre seront correctement interprétées à cause de la diversité des langues, des systèmes technologiques (interopérabilité) et des systèmes juridiques.

— Ce principe doit s'intégrer dans le patchwork actuel des dispositions juridiques qui traitent de l'échange entre pays d'informations en matière répressive.

18. Indépendamment de cet environnement complexe, il est communément admis que ce principe ne peut pas fonctionner isolément. Des mesures supplémentaires sont nécessaires pour qu'il soit possible de trouver les informations et d'y accéder effectivement. En tout état de cause, ces mesures doivent permettre aux services répressifs de savoir plus facilement si leurs homologues dans les autres États membres disposent des informations recherchées et où il est possible de les trouver. Il pourrait s'agir d'interfaces offrant un accès direct à toutes les données ou à des données particulières détenues par d'autres États membres. C'est la raison pour laquelle la proposition de décision-cadre relative au principe de disponibilité introduit les «données d'index», qui ont des données spécifiques accessibles directement depuis un autre pays.

19. De façon générale, le principe de disponibilité devrait faciliter le flux d'informations entre les États membres. Les frontières intérieures vont être supprimées et les États membres doivent accepter que les informations disponibles pour leurs services de police deviennent de plus en plus accessibles à d'autres services. Les États membres perdent leur compétence en matière de contrôle des flux d'informations, ce qui a également pour résultat que leur législation nationale n'est plus un instrument suffisant pour leur permettre d'assurer une protection adéquate de l'information.

20. C'est la raison pour laquelle il faut examiner la proposition avec une attention particulière pour ce qui est de la protection des données à caractère personnel. En premier lieu, des informations a priori confidentielles et sécurisées doivent être communiquées aux autorités d'autres États membres. En second lieu, pour que le système fonctionne, il faut créer des données d'index et les rendre accessibles aux services des autres États membres. L'application de ce principe va donc générer plus de données que ce qui est actuellement disponible.

IV. **PRINCIPAUX ÉLÉMENTS**

Champ d'application du principe de disponibilité

21. Il est d'abord essentiel de définir à quel type d'informations le principe de disponibilité s'appliquera. Son champ d'application est défini en termes généraux à l'article 2 de la proposition, en combinaison avec l'article 1er, paragraphe 1, et l'article 3, point a). Ce principe s'applique aux informations suivantes:

    — les informations existantes;

    — énumérées à l'annexe II (qui définit six types d'informations);

    — et qui sont accessibles aux autorités compétentes.

    Ce sont, dans la proposition de la Commission, les trois éléments fondamentaux du champ d'application du principe. Le champ d'application est davantage précisé à l'article 2. L'article 2, paragraphe 1, limite l'application du principe de disponibilité à l'étape préalable à l'engagement de poursuites, alors que les paragraphes 2, 3 et 4 du même article apportent des restrictions plus spécifiques.

22. Pour comprendre les conséquences de la proposition, il est nécessaire d'approfondir l'analyse des trois éléments fondamentaux susmentionnés. Les deux premiers sont suffisamment clairs en eux-mêmes. La définition des «informations existantes» est détaillée à l'article 2, paragraphe 2: la décision-cadre n'entraîne aucune obligation de recueillir et de stocker des informations dans le seul but de les rendre accessibles; quant à la liste figurant à l'annexe II, elle ne peut prêter à différentes interprétations. C'est le troisième élément fondamental, en lui-même et en combinaison avec les deux premiers, qui doit être clarifié.

23. La proposition ne précise pas si les «informations disponibles» consistent essentiellement en informations déjà gérées par les autorités compétentes ou si elles comprennent également des informations que ces autorités sont susceptibles d'obtenir. Toutefois, selon le CEPD, on pourrait considérer que la proposition couvre ces deux types d'informations.

24. En effet, si l'article 2, paragraphe 2, semble suggérer un champ d'application plus étroit, en précisant que la décision-cadre «n'entraîne aucune obligation de recueillir et de stocker des informations […] dans le seul but de les rendre accessibles», l'article 3, point a), autorise quant à lui une interprétation plus large, puisqu'il précise que par «informations», on entend «les informations existantes énumérées à l'annexe II».

25. L'annexe II mentionne au moins deux catégories de données généralement détenues par d'autres services que la police. La première catégorie concerne les informations relatives à l'immatriculation des véhicules. Dans beaucoup d'États membres, les bases de données contenant ces informations ne sont pas tenues par les services répressifs, même si ces derniers accèdent régulièrement à ces informations. Ce type d'informations doit-il entrer dans le champ d'application des «informations disponibles» qui, selon l'article 1er, doivent être fournies aux autorités compétentes des autres États membres? La seconde catégorie de données énumérées à l'annexe II concerne les numéros de téléphone et les autres données relatives aux communications: ces données doivent-elles être considérées comme «disponibles» même si elles ne sont pas détenues par les autorités compétentes mais par des sociétés privées?

26. Par ailleurs, d'autres dispositions de la proposition, et plus particulièrement l'article 3, point d), et l'article 4, paragraphe 1, point c), montrent que des «autorités désignées» et même des «parties désignées» peuvent contrôler les informations qui sont «disponibles» pour les «autorités compétentes». Il découle également du texte de la proposition que «l'autorité compétente» d'un État membre désigne «toute autorité nationale visée à l'article 29, premier tiret, du traité UE» alors que toute autorité nationale peut être considérée comme autorité désignée.

27. Selon le CEPD, l'application du principe de disponibilité aux informations placées sous le contrôle des autorités désignées et des parties désignées, amène à se poser les questions suivantes:

    — L'article 30, paragraphe 1, point b), fournit-il une base juridique suffisante, puisque les informations doivent être rendues accessibles par les autorités désignées et les parties désignées à partir de bases de données qui ne relèvent pas du troisième pilier?

    — La décision-cadre relative à la protection des données à caractère personnel s'appliquera-t-elle, comme cela est supposé à l'article 8 de la proposition, par exemple?

    — À défaut, le traitement des données est-il en conformité avec les obligations découlant de la directive 95/46/CE?

28. L'application d'un principe aussi large que le «principe de disponibilité» nécessite une définition claire et précise des données qui seront considérées comme disponibles. Le CEPD recommande donc:

— de clarifier le champ d'application;

— de limiter de préférence le champ d'application du principe de disponibilité aux informations gérées par les autorités compétentes;

— à défaut, si le champ d'application est plus large, de prévoir des garanties suffisantes pour la protection des données à caractère personnel. Les questions soulevées ci-dessus au point 27 doivent être prises en considération.

Autres questions liées au champ d'application

29. Aux termes de l'article 2, paragraphe 1, de la proposition, la décision-cadre s'appliquera aux traitements des informations réalisés préalablement à l'engagement de poursuites. Son champ d'application est plus limité que celui de la proposition de décision-cadre relative à la protection des données à caractère personnel qui couvre l'ensemble de la coopération judiciaire en matière pénale.

30. Toutefois, selon le CEPD, cette restriction n'a pas en soi pour effet de limiter à la coopération policière le champ d'application de la proposition. La décision-cadre pourrait également porter sur la coopération judiciaire en matière pénale puisque, dans un certain nombre d'États membres, les autorités judiciaires exercent également des compétences en matière d'enquêtes pénales, préalablement à l'engagement de poursuites. Cependant, le fait que la proposition soit fondée uniquement sur l'article 30, paragraphe 1, point b), du traité UE semble indiquer qu'elle s'applique uniquement à la coopération policière. Des éclaircissements sur ce point seraient les bienvenus.

31. La proposition qui nous occupe s'applique à la transmission d'informations à Europol alors que la proposition de décision-cadre relative à la protection des données à caractère personnel exclut le traitement des données à caractère personnel par Europol. Le CEPD conseille de limiter l'échange d'informations avec Europol aux objectifs d'Europol, tels que définis à l'article 2 et à l'annexe de la convention Europol. Par ailleurs, il devrait être tenu compte des modalités de l'échange de données avec Europol, qui sont déjà fixées dans plusieurs actes du Conseil.

Pas de nouvelle base de données contenant des données à caractère personnel

32. Le point de départ de la proposition est que celle-ci ne doit pas aboutir à la constitution de nouvelles bases de données contenant des données à caractère personnel. L'article 2, paragraphe 2, est clair sur ce point: la décision-cadre n'entraîne aucune obligation de recueillir et de stocker des informations dans le seul but de les rendre accessibles. Du point de vue de la protection des données, il s'agit d'un élément important et positif de cette proposition. Le CEPD rappelle son avis sur la proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ([1]), dans lequel il a souligné que les obligations légales qui entraînent la constitution de bases de données de taille importante font courir des risques particuliers à la personne concernée, notamment en matière d'utilisation abusive.

33. Toutefois:

— Il importe de veiller à ce que la proposition ne favorise pas une interconnexion sans restrictions des bases de données et, par conséquent, la création d'un réseau de bases de données qu'il sera difficile de contrôler.

— Il y a une objection au point de départ susmentionné: l'article 10 de la proposition, qui garantit que les données d'index sont disponibles en ligne. Les données d'index peuvent contenir des données à caractère personnel ou, en tout état de cause, révéler leur existence.

Accès direct et indirect aux informations

34. La proposition prévoit un accès direct et indirect à l'information. Son article 9 prévoit un accès direct en ligne aux informations contenues dans les bases de données auxquelles les autorités nationales correspondantes ont un accès direct en ligne. L'article 10 prévoit quant à lui un accès indirect. Les données d'index renvoyant à des informations auxquelles on ne peut pas accéder en ligne doivent pouvoir être consultées en ligne par les autorités compétentes équivalentes des autres États membres et par Europol. Lorsqu'en consultant des données d'index, l'autorité compétente trouve une correspondance, elle peut émettre une demande d'informations et la transmettre à l'autorité désignée de manière à obtenir les informations identifiées par les données d'index.

35. L'accès direct n'entraîne pas la constitution de nouvelles bases de données, mais il nécessite l'interopérabilité des bases de données des systèmes compétents équivalents des États membres. Par ailleurs, il induira forcément un nouveau mode d'utilisation des bases de données déjà existantes en offrant à toutes les autorités compétentes des États membres une possibilité qui était jusque là ouverte aux seules autorités nationales. L'accès direct multipliera automatiquement le nombre de personnes qui auront accès à une base de données et donc les risques d'utilisation abusive.

([1]) Avis 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 (COM (2005) 438 final).

36. En cas d'accès direct par une autorité compétente d'un autre État membre, les autorités désignées de l'État membre d'origine n'ont aucun contrôle sur l'accès aux données ni sur l'utilisation ultérieure qui en est faite. Il faut bien mesurer cette conséquence de l'accès direct tel que prévu par la proposition:

— Cela semble annuler le pouvoir qu'ont les autorités désignées de refuser de fournir les informations (en vertu de l'article 14).

— Cela soulève des questions quant à la responsabilité de l'exactitude et de la mise à jour des données, une fois que l'accès à ces données a été autorisé. Comment une autorité désignée de l'État membre d'origine peut-elle s'assurer que les données sont actualisées?

— Non seulement l'autorité désignée n'est plus en mesure de remplir toutes ses obligations au titre de la législation sur la protection des données, mais l'autorité nationale chargée de la protection des données dans l'État membre d'origine ne peut plus surveiller l'application des obligations puisqu'elle n'a aucune compétence vis-à-vis des services répressifs des autres États membres.

— Ces problèmes se posent avec encore plus d'acuité lorsqu'il s'agit de l'accès à des bases de données d'autorités désignées et de parties désignées qui ne sont pas des services répressifs (voir les points 25-28 du présent avis).

Cette conséquence de l'accès direct est une raison importante de subordonner l'adoption de la proposition à l'étude à l'adoption d'une décision-cadre relative à la protection des données à caractère personnel. Un problème reste posé: il est difficile de voir comment les autorités désignées pourraient refuser de communiquer des informations en vertu de l'article 14.

37. Quant à l'accès indirect via des données d'index qui donnent des informations selon un système «hit-no hit», il ne s'agit pas d'un phénomène nouveau. C'est la base du fonctionnement des systèmes européens d'information à grande échelle, comme le système d'information Schengen. La mise en place d'un système de données d'index présente l'avantage de permettre à l'État membre d'origine de contrôler l'échange des informations provenant des fichiers de ses services de police. Si la consultation des données d'index fait apparaître une correspondance, l'autorité requérante peut établir une demande d'informations sur la personne concernée. Cette demande peut être valablement évaluée par l'autorité requise.

38. Il faut néanmoins sérieusement étudier cette question, car la mise en place d'un système de données d'index — dans les domaines où ces systèmes n'existent pas encore, autres que les systèmes européens d'information à grande échelle — est de nature à créer de nouveaux risques pour la personne concernée. Le CEPD rappelle que, bien que les données d'index ne contiennent pas beaucoup d'informations sur la personne concernée, leur consultation peut donner des résultats extrêmement sensibles. Elle peut révéler qu'une personne figure dans un fichier de police dans le cadre d'une infraction pénale.

39. Il est donc de la plus haute importance que le législateur européen prévoie des règles appropriées, au moins en ce qui concerne la création des données d'index, la gestion des fichiers contenant ces données et l'accès à ces données. Selon le CEPD, la proposition n'est pas satisfaisante sur ces points. À ce stade, le CEPD formule trois observations:

— La définition des données d'index n'est pas claire. On ne sait pas s'il s'agit de métadonnées, de clés primaires ou des deux? Cette notion doit être clarifiée, car elle a une incidence directe sur le degré de protection des données et sur les garanties nécessaires.

— La proposition devrait clarifier le rôle des points de contact nationaux à l'égard des données d'index. Il pourrait être nécessaire de les associer, en particulier lorsque l'interprétation des données d'index nécessite des connaissances spécialisées, par exemple en cas d'éventuelle comparaison des empreintes digitales.

— La proposition prévoit que les règles relatives à la création des données d'index feront l'objet de mesures d'exécution arrêtées conformément à la procédure de comité décrite à l'article 19. Même si des mesures d'exécution seront peut-être nécessaires, les règles de base régissant la création des données d'index devraient figurer dans la décision-cadre elle-même.

Autorisation préalable des autorités judiciaires

40. L'échange d'informations ne doit pas dispenser l'État membre requis de demander aux autorités judiciaires l'autorisation préalable de transmettre à l'autorité requérante des informations qui seraient sous contrôle judiciaire. Il s'agit d'un point important puisque, comme l'a montré une enquête sur les pouvoirs des services de police en matière d'échange des données à caractère personnel [1], il y a des États membres où la police n'a pas accès de façon autonome à ce type de données. Selon le CEPD, le principe de disponibilité ne devrait pas porter atteinte aux dispositions nationales rendant obligatoire l'autorisation préalable d'accès aux informations, ou, à tout le moins, il conviendrait d'établir des règles spécifiques concernant les catégories de données soumises à une autorisation préalable, qui seront applicables dans tous les États membres.

[1] Réponses au questionnaire sur la 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 (document nº 5815/1/05 du Conseil).

41. Cette obligation doit être interprétée en combinaison avec l'article 11, paragraphe 2, de la proposition de décision-cadre relative à la protection des données à caractère personnel qui prévoit également que l'État membre qui transmet les données ait un droit de regard sur leur traitement ultérieur dans l'État membre qui les reçoit. Le CEPD note l'importance de ce principe, qui est nécessaire pour garantir que le principe de disponibilité ne servira pas à contourner la législation restrictive nationale sur l'utilisation ultérieure des données à caractère personnel.

Remarque finale

42. Ces éléments nécessitent des normes très élevées en matière de protection des données. Il convient de veiller tout particulièrement à garantir les principes de limitation de la finalité et de traitement ultérieur ainsi que les principes d'exactitude et de fiabilité des informations auxquelles l'accès est accordé (voir l'avis du CEPD sur la décision-cadre relative à la protection des données à caractère personnel, IV.2 et IV.6).

V. AUTRES APPROCHES

La proposition suédoise

43. La proposition suédoise ne se limite pas à certains types d'informations; elle porte sur toutes les informations *et les renseignements*, y compris ceux qui sont détenus par d'autres autorités que les services répressifs compétents. La proposition favorise la coopération en fixant des délais pour répondre aux demandes d'informations et en supprimant toute distinction entre les échanges d'informations au sein d'un État membre et les échanges transfrontières. Elle ne prévoit pas de mesures supplémentaires garantissant un accès effectif aux informations. On peut dès lors comprendre pourquoi la Commission n'a pas considéré la proposition suédoise était en tant que telle un instrument propre à mettre en œuvre le principe de disponibilité ([1]).

44. L'approche retenue dans la proposition suédoise a, du point de vue de la protection des données, les implications générales suivantes:

— Il est intéressant que la proposition se limite strictement au traitement de données existantes et n'entraîne pas la création de nouvelles bases de données, pas même de «données d'index».

— Toutefois, l'absence de «données d'index» ne constitue pas, en soi, un élément positif. Pour autant qu'elles soient correctement sécurisées, les données d'index peuvent faciliter, pour les données à caractère sensible, une recherche ciblée et donc moins intrusive. Elles peuvent également permettre de mieux filtrer et vérifier les demandes.

— En tout état de cause, la proposition entraîne une augmentation des échanges transfrontières de données à caractère personnel, et des risques pour la protection de ces données, notamment parce qu'elle porte atteinte à la capacité des États membres à contrôler rigoureusement les services qui procèdent aux échanges de données. Son adoption et celle de la décision-cadre relative à la protection des données à caractère personnel ne devraient pas être dissociées.

([1]) Voir document de travail des services de la Commission intitulé «Annexe à la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité», SEC(2005) 1270 du 12.10.2005.

Le traité de Prüm

45. Le traité de Prüm aborde la mise en œuvre du principe de disponibilité sous un angle différent. Alors que la proposition de décision-cadre à l'examen envisage les choses d'une manière générale — elle ne prévoit pas de règles spécifiques pour l'échange de certains types d'informations, mais s'applique à tous les types d'informations pour autant qu'ils soient énumérés à l'annexe II (voir points 21 à 28 du présent avis) —, le traité de Prüm adopte une approche progressive.

46. Cette approche est parfois qualifiée d'approche «catégorie de données par catégorie de données». Elle s'applique à certains types d'informations (ADN, données dactyloscopiques et données concernant l'immatriculation des véhicules) et prévoit l'obligation de tenir compte de la nature spécifique des données. Le traité prévoit l'obligation de créer et de conserver des fichiers d'analyse ADN pour des enquêtes pénales. Les données dactyloscopiques font l'objet d'une obligation similaire. Pour ce qui est des données concernant l'immatriculation des véhicules, les points de contact nationaux des autres États membres doivent pouvoir y accéder directement.

47. L'approche adoptée dans le traité de Prüm appelle trois types d'observations.

48. Premièrement, il va sans dire que le CEPD n'approuve pas le processus qui a abouti à ce traité, en dehors du cadre institutionnel de l'Union européenne et donc sans véritable intervention de la Commission. Cela signifie en outre que le Parlement européen n'exerce aucun contrôle démocratique et la Cour de justice aucun contrôle juridictionnel et, qu'en conséquence, les garanties d'un juste équilibre entre tous les intérêts (publics) sont moins nombreuses. Cela vaut aussi pour la protection des données. En d'autres termes, les institutions de l'Union européenne n'ont pas l'occasion d'évaluer — avant la mise en place du système — l'incidence sur la protection des données à caractère personnel des orientations choisies.

49. Deuxièmement, certains éléments du traité de Prüm ont à l'évidence un caractère plus intrusif à l'égard de la personne concernée que la proposition de décision-cadre relative au principe de disponibilité. Le traité entraîne nécessairement la création de nouvelles bases de données, ce qui présente des risques pour la protection des données à caractère personnel. Il conviendrait de démontrer que la création de ces nouvelles bases de données est nécessaire et proportionnée. Il faudrait prévoir des garanties adéquates pour la protection des données à caractère personnel.

Une approche «catégorie de données par catégorie de données»

50. Troisièmement, le traité adopte, comme indiqué précédemment, une approche «catégorie de données par catégorie de données». Le CEPD a mentionné ci-dessus les difficultés et les incertitudes liées au contexte dans lequel le principe de disponibilité doit être rendu effectif. Dans ces conditions, il juge préférable de ne pas établir un système portant sur toute une série de données, mais de commencer par une approche plus prudente portant sur un seul type de données et d'évaluer dans quelle mesure le principe de disponibilité peut réellement contribuer au respect de la loi, ainsi que les risques spécifiques pour la protection des données à caractère personnel. Sur la base de ces expériences, le système pourrait être étendu à d'autres types de données et/ou modifié pour être plus efficace.

51. Par ailleurs, cette approche «catégorie de données par catégorie de données» satisferait mieux aux exigences du principe de proportionnalité. Selon le CEPD, la nécessité d'améliorer les échanges transfrontières de données à des fins répressives pourrait justifier l'adoption d'un instrument juridique au niveau de l'UE mais, pour être proportionné, cet instrument devrait être adapté à son objectif, lequel pourra être défini plus correctement après une période d'expériences pratiques. Par ailleurs, cet instrument ne devrait pas affecter de façon disproportionnée la personne concernée. Les échanges ne devraient pas porter sur plus de types de données que ce qui est strictement nécessaire, avec la possibilité d'échanges de données anonymes, et devraient intervenir dans des conditions strictes de protection des données.

52. En outre, cette approche plus prudente préconisée par le CEPD pourrait consister, éventuellement en plus de l'approche «catégorie de données par catégorie de données», à se limiter, dans un premier temps, à l'accès indirect, par le biais de données d'index pour mettre en œuvre le principe de disponibilité. Cette suggestion du CEPD pourrait être examinée dans la suite du processus législatif.

VI. **QUELLES DONNÉES?**

53. L'annexe II énumère les six types d'informations qui peuvent être obtenues en vertu de la proposition de décision-cadre, qui portent sur des données à caractère personnel, dans la plupart des cas parce qu'elles impliquent un lien avec une personne identifiée ou identifiable.

54. Conformément à l'article 3, point g), de la proposition, on entend par données d'index les «données ayant pour finalité d'identifier clairement des informations et pouvant être interrogées dans le cadre d'une routine de recherche afin de vérifier si des informations sont ou non disponibles». Dans l'«approche concernant la mise en œuvre du principe de disponibilité» ([1]), les données suivantes sont considérées comme des données d'index:

— l'identification des personnes concernées;

— un numéro d'identification des objets concernés (véhicules/documents);

— des empreintes digitales/des photographies numériques.

Un autre type de données qui pourraient être considérées comme des données d'index sont les profils ADN. Cette liste de données d'index montre qu'il peut s'agir de données à caractère personnel et une protection adéquate s'impose donc.

55. Le CEPD accorde une attention particulière à la question des profils ADN. Les analyses d'ADN ont démontré leur utilité pour les enquêtes pénales et l'échange de données sur l'ADN peut être déterminant dans la lutte contre la criminalité. Il est cependant primordial de définir clairement ce qu'elles recouvrent et de prendre dûment en compte leurs caractéristiques spécifiques. Du point de vue de la protection des données, il existe en effet une différence de taille entre les échantillons d'ADN et les profils ADN.

56. Les échantillons d'ADN (qui sont souvent recueillis et stockés par les autorités répressives) devraient être considérés comme particulièrement sensibles car ils sont davantage susceptibles de contenir une «image» ADN complète. Ces échantillons peuvent fournir des informations sur les caractéristiques génétiques et l'état de santé d'une personne, qui pourraient servir à des fins totalement différentes telles que des avis médicaux à des personnes.

57. Par contre, les profils ADN ne contiennent que certaines informations ADN partielles, extraites d'un échantillon d'ADN; ils peuvent être utilisés pour vérifier l'identité d'une personne, mais, en principe, ils ne révèlent pas les caractéristiques génétiques. Toutefois, les progrès scientifiques peuvent augmenter le nombre d'informations que les profils ADN sont susceptibles de révéler. Un profil ADN considéré comme «innocent» à un certain stade peut ultérieurement révéler beaucoup plus d'informations que prévu et nécessaire et, en particulier, des informations concernant les caractéristiques génétiques d'une personne. Il conviendrait, par conséquent, de considérer les informations susceptibles d'être révélées par les profils ADN comme des informations dynamiques.

58. Dans cette perspective, le CEDP note que le traité de Prüm et la proposition de la Commission favorisent tous deux l'échange entre autorités répressives de données sur l'ADN, mais que leurs manières de procéder sont très différentes.

([1]) Note de la présidence au Conseil du 5 avril 2005 (doc. 7641/05).

59. Le CEPD note avec satisfaction que la proposition de la Commission ne prévoit pas d'obligation de recueillir des données sur l'ADN et qu'elle limite clairement l'échange de ces données aux profils ADN. À l'annexe II, les profils ADN sont définis au moyen d'une liste initiale commune de marqueurs d'ADN utilisés pour les analyses d'ADN effectuées dans les États membres à des fins de police scientifique. Cette liste, qui se fonde sur les sept marqueurs d'ADN de l'ensemble européen de référence (European Standard Set) tels qu'ils sont définis à l'annexe I de la résolution du Conseil du 25 juin 2001 relative à l'échange des résultats des analyses d'ADN ([1]), garantit que les profils ADN ne contiendront, lors de leur extraction, aucune information sur des caractéristiques héréditaires spécifiques.

60. Le CEPD souligne que cette résolution du Conseil établit des garanties très importantes, spécifiquement liées au caractère dynamique des profils ADN. En effet, le point III de la résolution recommande aux États membres, après avoir limité les échanges de résultats des analyses d'ADN aux «segments chromosomiques […] ne fournissant pas, en l'état actuel des connaissances, d'informations sur des caractéristiques héréditaires spécifiques», de ne plus utiliser les marqueurs d'ADN qui, en raison de l'évolution scientifique, pourraient fournir de ce type informations.

61. Le traité de Prüm propose une approche différente dans la mesure où il contraint les parties contractantes à créer et à gérer des fichiers d'analyse ADN en vue de la poursuite des infractions pénales. Il entraîne par conséquent la création de nouvelles bases de données ADN et une augmentation du nombre de données ADN recueillies. Par ailleurs, le type de données qui figurent dans les «fichiers d'analyse ADN» n'est pas clairement défini et le traité ne tient pas compte de l'évolution dynamique des profils ADN.

62. Pour le CEPD, tout instrument juridique prévoyant des échanges de données ADN devrait:

— clairement limiter et définir le type d'informations ADN pouvant faire l'objet d'échanges (y compris en ce qui concerne la différence fondamentale qui existe entre les échantillons d'ADN et les profils ADN);

— établir des normes techniques communes pour éviter que les différences qui existent entre les États membres dans la manière de traiter les bases de données ADN à des fins de police scientifique ne soient pas sources de difficultés et ne génèrent des résultats inexacts lors de l'échange de données;

— prévoir des garanties adéquates juridiquement contraignantes pour éviter que les progrès scientifiques ne permettent d'obtenir à partir de profils ADN des données à caractère personnel qui seraient non seulement sensibles, mais également inutiles au regard de la finalité pour laquelle elles ont été recueillies.

63. Dans cette perspective, le CEPD réitère les observations qu'il a déjà formulées dans son avis sur la décision-cadre relative à la protection des données à caractère personnel (point 80). Le CEPD y faisait valoir que, en ce qui concerne les données ADN, il faudrait prévoir des garanties spécifiques afin que les informations disponibles ne puissent être utilisées que dans le but d'identifier des individus en vue de prévenir ou de détecter des infractions pénales ou d'enquêter en la matière, que le niveau d'exactitude des profils ADN soit dûment pris en compte et puisse être contesté par la personne concernée par des moyens facilement accessibles, et que le respect de la dignité des personnes soit totalement garanti ([2]).

64. Les considérations qui précèdent nous amènent à conclure que l'adoption d'une législation relative à la création de fichiers ADN et à l'échange des données qu'ils contiennent ne devrait intervenir que lorsque les avantages et les risques en auront été correctement analysés. Le CEPD recommande que cette législation prévoie l'obligation de réaliser, après son entrée en vigueur, des évaluations régulières.

65. Enfin, l'annexe II prévoit que d'autres types d'informations pourront être échangés. Il s'agit d'informations émanant d'entités privées, puisque les numéros de téléphone et les autres données relatives aux communications, ainsi que les données relatives au trafic proviennent généralement d'opérateurs téléphoniques. L'exposé des motifs confirme que les États membres sont tenus de veiller à ce que les informations utiles à l'action répressive, gérées par des autorités ou des entités privées désignées à cet effet, soient échangées avec les autorités compétentes équivalentes des autres États membres et avec Europol. Bien que la proposition s'applique aux données à caractère personnel émanant d'entités privées, le cadre juridique applicable devrait contenir, d'après le CEPD, des garanties supplémentaires destinées à protéger la personne concernée afin d'assurer l'exactitude des données.

VII. **PRINCIPES DE LA PROTECTION DES DONNÉES**

66. La proposition de décision-cadre du Conseil n'énonce pas expressément de règles relatives à la protection des données à caractère personnel, contrairement à d'autres instruments, tels que le traité de Prüm ou la proposition suédoise. L'absence, dans la proposition relative au principe de disponibilité, de règles spécifiques à cet égard n'est acceptable que dans la mesure où les règles générales contenues dans la proposition de décision-cadre sur la protection des données relevant du troisième pilier sont pleinement applicables et fournissent une protection suffisante. De plus, les règles sur la protection des données à caractère personnel énoncées dans des instruments spécifiques, tels que la proposition suédoise et le traité de Prüm, ne devraient pas abaisser le niveau de protection garanti par le cadre général. Le CEPD recommande l'ajout d'une clause particulière sur les conflits qui pourraient exister entre les différentes règles relatives à la protection des données.

([1]) JO C 187 du 3.7.2001, p. 1.

([2]) Dans le même ordre d'idées, voir également le «Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques» du Conseil de l'Europe, de février 2005.

67. À ce stade, le CEPD souhaiterait souligner une nouvelle fois, en rappelant l'avis qu'il a rendu au sujet de la décision-cadre relative à la protection des données à caractère personnel, l'importance de disposer, dans le cas de la coopération en matière pénale, de règles cohérentes et exhaustives dans le domaine de la protection des données qui s'appliquent à tous les traitements. Le CEPD rappelle aussi les autres observations qu'il a formulées dans cet avis. Nous reviendrons ici sur les questions relatives à la protection des données:

— Licéité du traitement des données à caractère personnel. Le CEPD est favorable au principe selon lequel les informations ne peuvent être traitées comme des informations disponibles que si elles ont été collectées légalement (comme le précise l'article 2, paragraphe 2, en ce qui concerne les informations collectées en recourant à des mesures coercitives). La licéité du traitement des données à caractère personnel garantirait également que les informations rendues disponibles et échangées peuvent aussi être valablement utilisées dans une procédure judiciaire. En effet, même si les informations traitées après l'engagement de poursuites n'entrent pas dans le champ d'application de l'instrument proposé, il est probable que les informations préalablement échangées par les autorités répressives se retrouvent finalement dans la procédure judiciaire.

— La qualité des données à caractère personnel revêt une importance particulière dès lors que, selon le principe de disponibilité, les informations seront utilisées par des autorités répressives qui opèrent en dehors du cadre dans lequel les données ont été recueillies. Ces autorités disposent même d'un accès direct aux bases de données des autres États membres. La qualité des données à caractère personnel ne peut être garantie que si leur exactitude est régulièrement et correctement vérifiée, si les informations sont différenciées en fonction des catégories de personnes concernées (victimes, suspects, témoins, etc.) et si, le cas échéant, le degré d'exactitude est indiqué (voir avis du CEPD 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, point IV.6).

  Cela montre une nouvelle fois pourquoi les règles relatives à la protection des données et, en particulier celles concernant leur exactitude, devraient s'appliquer à tous les types de traitements, y compris aux traitements nationaux. Sinon, les données à caractère personnel qui sont directement accessibles pourraient être incorrectes, obsolètes et, par conséquent, affecter les droits des personnes concernées et l'efficacité des enquêtes.

— Limitation de la finalité. Conformément au principe de disponibilité, les données à caractère personnel sont accessibles aux autorités compétentes équivalentes des autres États membres. Toutefois, les compétences des autorités répressives peuvent fortement varier d'un pays à l'autre. Il est donc essentiel de veiller à ce que le principe fondamental de limitation de la finalité soit respecté malgré les différences qui existent dans la portée des compétences des autorités compétentes qui échangent des données. Les informations recueillies et traitées par une autorité pour une finalité particulière ne peuvent ensuite être utilisées pour une finalité différente uniquement parce que l'autorité réceptrice a des compétences différentes, éventuellement plus larges.

  Le CEPD juge donc intéressant l'article 7 de la proposition de décision-cadre, qui précise en fait les règles générales énoncées dans la proposition de décision-cadre relative à la protection des données à caractère personnel. Le CEPD note en outre que l'évaluation de l'équivalence entre les différentes autorités (qui, dans la proposition à l'examen, relève d'une procédure de comité) devrait être réalisée avec soin et dans le respect du principe de limitation de la finalité.

— Les délais prévus pour la conservation des informations échangées doivent également être considérés à la lumière du principe de limitation de la finalité. Les informations auxquelles on accède ou que l'on échange dans un but déterminé devraient être supprimées dès qu'elles ne sont plus nécessaires à cet effet. Cela éviterait une duplication inutile des bases de données, tout en permettant aux autorités compétentes d'avoir à nouveau accès aux informations disponibles (actualisées) au cas où cela serait nécessaire pour une autre finalité légitime.

— Inscription dans un registre (logging) des informations transmises conformément au principe de disponibilité. Cette inscription devrait avoir lieu aussi bien dans l'État membre requis que dans l'État membre requérant. Il faudrait tenir des registres des échanges, mais également des registres des accès (voir avis du CEPD sur la protection des données à caractère personnel, point 133), y compris afin que les autorités compétentes nationales se fassent confiance et ne perdent pas totalement le contrôle sur les informations disponibles. La nécessité de conserver une trace documentaire va de pair avec la possibilité d'actualiser et/ou de corriger les informations.

— Droits des personnes concernées. Les systèmes d'échange d'informations entre les autorités répressives de l'UE augmentent le nombre de cas où des données à caractère personnel sont (provisoirement) traitées simultanément par des autorités compétentes dans différents États membres. Il faudrait donc, d'une part, que soient établies des normes communes de l'UE concernant les droits des personnes concernées et, d'autre part, que ces dernières puissent exercer leurs droits, dans la mesure où les règles de protection des données relevant du troisième pilier les y autorisent, tant à l'égard des autorités qui rendent les données disponibles qu'à l'égard des autorités qui y ont accès et qui les traitent.

— Contrôle. Le CEPD fait observer que, suivant le cas, plusieurs autorités nationales de contrôle peuvent être compétentes pour surveiller le traitement de données à caractère personnel réalisé sur la base des propositions à l'examen. Dans ces conditions, l'accès direct en ligne à des informations en matière répressive nécessite une surveillance et une coordination renforcées des autorités nationales compétentes en matière de protection des données.

VIII. CONCLUSIONS

Conclusions générales concernant le principe de disponibilité

68. Le CEPD a formulé, dans le présent avis, des considérations générales et fondamentales sur l'échange d'informations en matière répressive et sur les approches envisageables pour réglementer cette question. Le CEPD pourra évidemment être à nouveau consulté ultérieurement, en fonction de l'évolution du parcours législatif de cette proposition, ainsi que sur d'autres propositions dans le même domaine.

69. Le CEPD estime que le principe de disponibilité devrait être mis en œuvre sous la forme d'un instrument juridique contraignant par le biais d'une approche plus prudente et progressive portant sur un seul type de données et qu'il faut évaluer dans quelle mesure ce principe peut réellement contribuer au respect de la loi, ainsi que les risques spécifiques pour la protection des données à caractère personnel. Cette approche plus prudente pourrait consister à se limiter, dans un premier temps, à l'accès indirect, par le biais de données d'index, pour mettre en œuvre le principe de disponibilité. Sur la base des expériences ainsi acquises, le système pourrait éventuellement être étendu à d'autres types de données et/ou être modifié pour gagner en efficacité.

70. Aucun instrument juridique mettant en œuvre le principe de disponibilité ne devrait être adopté sans que ne soient fixées au préalable des garanties essentielles en matière de protection des données, comme dans la proposition de décision-cadre relative à la protection des données à caractère personnel.

Recommandations visant à modifier la proposition à l'examen

71. Le CEPD recommande de clarifier le champ d'application du principe de disponibilité comme suit:

    — en ajoutant une définition claire et précise des données qui seront considérées comme disponibles;

    — en limitant de préférence le champ d'application du principe de disponibilité aux informations détenues par les autorités compétentes;

    — à défaut, si le champ d'application est plus large, en prévoyant des garanties suffisantes pour la protection des données à caractère personnel. Les questions soulevées au point 27 du présent avis doivent être prises en considération.

72. Concernant l'accès direct aux bases de données par les autorités compétentes d'autres États membres, le CEPD précise ce qui suit:

    — il faut étudier cette question avec toute l'attention nécessaire car, en cas d'accès direct, les autorités désignées de l'État membre d'origine n'ont aucun contrôle sur l'accès ni sur l'utilisation ultérieure des données;

    — la proposition ne peut pas favoriser une interconnexion sans restrictions des bases de données et, par conséquent, la création d'un réseau de bases de données qu'il sera difficile de surveiller.

73. La décision-cadre devrait être plus précise en ce qui concerne la création d'un système de données d'index. Plus particulièrement:

    — la proposition devrait prévoir des règles appropriées, au moins en ce qui concerne la création des données d'index, la gestion des fichiers contenant ces données et l'accès à ces données;

    — la définition des données d'index doit être clarifiée;

    — le rôle joué par les points de contact nationaux à l'égard des données d'index devrait être clarifié;

    — les règles de base régissant la création des données d'index devraient figurer dans la décision-cadre proprement dite et ne pas relever de la législation d'application conformément à la comitologie.

74. Le CEPD estime que la proposition devrait, dans la mesure où elle prévoit des échanges de données relatives à l'ADN:

    — clairement limiter et définir le type d'informations ADN pouvant faire l'objet d'échanges (y compris en ce qui concerne la différence fondamentale qui existe entre les échantillons d'ADN et les profils ADN);

    — établir des normes techniques communes pour éviter que les différences qui existent entre les États membres dans la manière de traiter les bases de données ADN à des fins de police scientifique ne soient sources de difficultés et ne génèrent des résultats inexacts lors de l'échange de données;

    — prévoir des garanties adéquates juridiquement contraignantes pour éviter que les progrès scientifiques ne permettent d'obtenir à partir de profils ADN des données à caractère personnel qui seraient non seulement sensibles, mais également inutiles au regard de la finalité pour laquelle elles ont été recueillies;

    — ne devrait être adoptée qu'après une analyse d'impact.

75. Le CEPD recommande de limiter les échanges d'informations avec Europol aux objectifs d'Europol, visés à l'article 2 de la Convention Europol et à son annexe.

Fait à Bruxelles, le 28 février 2006.

Peter HUSTINX

Contrôleur européen de la protection des données