Deuxième avis du contrôleur européen de la protection des données sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

(2007/C 91/02)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

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

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

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

A ADOPTÉ L'AVIS SUIVANT:

1. Le 19 décembre 2005, le CEPD a émis un avis ([3]) sur la proposition, présentée par la Commission, de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Dans cet avis, le contrôleur a souligné l'importance que revêt la proposition en tant qu'instrument efficace capable de garantir la protection des données à caractère personnel dans le domaine visé par le titre VI du traité UE. Cet instrument devrait non seulement respecter les principes de la protection des données énoncés dans la Convention n° 108 du Conseil de l'Europe ([4]), et plus particulièrement dans la directive 95/46/CE, mais aussi prévoir un ensemble complémentaire de règles tenant compte de la nature spécifique du domaine répressif. Le CEPD estime qu'il est indispensable que la décision-cadre s'applique à tous les traitements de données policières et judiciaires, même si celles-ci ne sont pas transmises ou mises à disposition par les autorités compétentes d'autres États membres. La cohérence de la protection des données à caractère personnel est essentielle, quel que soit le lieu où elles sont traitées, par qui et à quelle fin. Le CEPD a formulé plusieurs propositions visant à améliorer le niveau de protection.

2. Le 27 septembre 2006, le Parlement européen a adopté une résolution législative sur la proposition de la Commission. D'une manière générale, la résolution a les mêmes objectifs que l'avis du CEPD: elle soutient dans l'ensemble la proposition tout en proposant des modifications visant à renforcer le niveau de protection offert par la décision-cadre.

3. La proposition de la Commission est actuellement examinée par le Conseil. Selon les informations disponibles ([5]), le Conseil enregistre des progrès et modifie des éléments essentiels du texte de la proposition. Par ailleurs, la présidence du Conseil s'emploie activement à faire en sorte que des progrès plus importants encore soient réalisés, son objectif étant de parvenir à dégager d'ici décembre 2006 une orientation commune sur les principaux éléments de la proposition.

4. Le CEPD se félicite que le Conseil accorde une grande attention à cette proposition importante. Il s'inquiète néanmoins de la direction prise par les travaux. En effet, les textes actuellement examinés au Conseil ne reprennent pas les amendements proposés par le Parlement européen et ne tiennent pas non plus compte des avis émis par le CEPD et la conférence des autorités européennes chargées de la protection des données. Au contraire, dans un nombre non négligeable de cas, des dispositions de la proposition de la Commission offrant des garanties aux citoyens ont été supprimées ou considérablement affaiblies. *Il existe par conséquent un risque important que le niveau de protection soit inférieur à celui offert par la directive 95/46/CE ou même à celui offert par la Convention n° 108 du Conseil de l'Europe formulée en termes plus généraux, qui est contraignante pour les États membres.*

([1]) JO L 281 du 23.11.1995, p. 31.
([2]) JO L 8 du 12.1.2001, p. 1.
([3]) JO C 47 du 25.2.2006, p. 27.
([4]) 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.
([5]) Officiellement, aucun document public n'est disponible et le CEPD n'est pas directement associé aux travaux du groupe du Conseil compétent. Il est toutefois possible de consulter des documents faisant le point sur l'état d'avancement des travaux au sein du Conseil sur le site web de l'organisation Statewatch (www.statewatch.org).

5. Le CEPD note que la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a aussi récemment fait part de ses préoccupations quant aux choix faits par le Conseil en ce qui concerne cette proposition de décision-cadre.

6. C'est pour ces raisons que le CEPD formule aujourd'hui un deuxième avis. Celui-ci porte essentiellement sur certaines préoccupations centrales et ne reproduit pas l'ensemble des observations formulées dans l'avis du CEPD publié en décembre 2005, qui restent néanmoins toutes valables.

Préoccupation générale

7. Dans un espace de liberté, de sécurité et de justice en constante évolution, l'échange d'informations policières et judiciaires entre les États membres devient de plus en plus important. Plusieurs instruments juridiques sont proposés ou ont été adoptés afin de faciliter cet échange d'informations. Le CEPD souligne une fois encore que, dans ce contexte, un cadre juridique solide protégeant la personne concernée est nécessaire pour garantir le respect des droits fondamentaux des citoyens. La (proposition de) décision-cadre à l'examen est directement liée aux propositions facilitant cet échange d'informations.

8. Tout en étant conscient qu'il importe que le Conseil adopte la décision-cadre dans les meilleurs délais, le CEPD tient à souligner que la rapidité de la prise de décision ne devrait pas entraîner une diminution des normes de protection. Compte tenu des textes actuellement examinés par le Conseil, on peut se demander si le résultat sera suffisamment solide pour offrir un niveau de protection efficace au citoyen. En l'état actuel des choses, l'objectif de rapidité poursuivi pourrait avoir pour conséquence que des dispositions potentiellement controversées soient supprimées ou affaiblies. Le manque de temps pour parvenir à un consensus sur des questions susceptibles de susciter des controverses pourrait être préjudiciable à la qualité du texte de la décision-cadre.

9. Compte tenu de ce qui précède, le CEPD recommande au Conseil de prévoir plus de temps pour les négociations, de manière à parvenir à un résultat offrant une protection suffisante.

Applicabilité aux traitements internes

10. Cette question, qui a été un élément essentiel de l'avis de décembre 2005, a ensuite fait l'objet d'un examen approfondi. Les règles communes relatives à la protection des données devraient s'appliquer à toutes les données en rapport avec le domaine de la coopération policière et judiciaire et ne pas être limitées aux échanges transfrontières entre les États membres. Un champ d'application plus limité n'offrirait pas une protection appropriée, telle qu'exigée par l'article 30, paragraphe 1, point b), du traité UE. Cet aspect a été souligné à plusieurs reprises, également par des parties intéressées autres que le CEPD.

11. Dans son avis de décembre 2005, le CEPD a indiqué qu'une limitation aux données échangées avec d'autres États membres rendrait le domaine d'application de la décision-cadre particulièrement incertain et aléatoire, ce qui serait contraire à son objectif essentiel. Au moment de la collecte ou du traitement des données à caractère personnel, il est impossible de savoir si ces données seront susceptibles de donner lieu par la suite à un échange avec les autorités compétentes d'autres États membres.

12. Pour cette raison, *un champ d'application plus limité est impossible à mettre en œuvre. Si un tel champ d'application était appliqué, des distinctions précises et difficiles à établir devraient être mises en place au sein des bases de données des services répressifs, ce qui ne ferait qu'accroître la complexité et les coûts que ceux-ci doivent supporter et porterait en outre atteinte à la sécurité juridique des personnes.*

13. Deux exemples peuvent illustrer ces conséquences. En premier lieu, l'accroissement de la complexité et des coûts tient au fait que, dans un nombre non négligeable de cas, les dossiers judiciaires contiennent des informations émanant de différentes autorités. Un champ d'application limité aurait pour conséquence que certaines parties de ces dossiers mixtes — celles contenant les informations communiquées par les autorités d'autres États membres — seraient protégées en vertu de la décision-cadre et que d'autres parties ne le seraient pas. En second lieu, il serait porté atteinte à la sécurité juridique des personnes puisque — dans le cas d'un champ d'application plus limité — les informations émanant des pays tiers, mais ne faisant pas l'objet d'échanges entre les États membres, ne seraient pas couvertes par la décision-cadre. Il est évident que le traitement de telles données présente des risques particuliers pour la personne concernée dans le cas où, par exemple, il n'existerait pas d'obligation légale de vérifier l'exactitude de ces données. Un bon exemple serait l'utilisation dans un État membre, à des fins répressives, d'une liste de personnes interdites de vol établie par un pays tiers.

14. Le CEPD rappelle qu'un niveau élevé de protection des données est nécessaire dans le domaine de la coopération policière et judiciaire, domaine dans lequel le traitement des données à caractère personnel présente, par sa nature même, des risques particuliers pour le citoyen, comme cela est notamment reconnu à l'article 30, paragraphe 1, point b), du traité UE. Par ailleurs, de grandes disparités, en termes de protection des données, entre le premier et le troisième pilier porteraient atteinte non seulement au droit du citoyen à la protection des données à caractère personnel, mais aussi à l'efficacité de l'action répressive et à la confiance mutuelle entre les États membres.

15. La proposition concourt à la réalisation de ces deux objectifs. Elle devrait offrir au citoyen des garanties contre une utilisation inappropriée de ses données à caractère personnel. Pour la personne concernée, il importe peu de savoir si les données la concernant sont traitées dans le cadre d'un échange entre États membres ou dans un contexte purement interne. La proposition devrait par ailleurs contribuer au renforcement de la confiance mutuelle entre les États membres, ce qui constitue une condition pour un échange d'informations efficace. Si des normes communes sont appliquées au traitement des données, cela facilitera l'acceptation des informations échangées par les États membres.

16. Le CEPD attire l'attention sur le fait qu'une limitation du champ d'application de la décision-cadre aux données faisant l'objet d'un échange ne permettrait pas pleinement d'instaurer la confiance nécessaire entre les autorités des États membres. En outre, un texte de portée limitée ne protège pas le citoyen de manière appropriée. Dans ces conditions, la décision-cadre n'offrirait plus au citoyen une garantie suffisante contre une utilisation abusive éventuelle de ses données par les autorités publiques. Le CEPD est d'avis que ce «rôle de bouclier» que doit jouer la législation est essentiel, ne serait-ce que pour garantir que l'Union européenne respecte les droits fondamentaux, conformément à l'article 6 du traité UE.

17. Enfin, un argument d'ordre stratégique vient étayer le point de vue selon lequel la décision-cadre doit être applicable à tous les traitements. Comme l'ont montré les négociations menées récemment avec les États-Unis concernant un nouvel accord sur le traitement et le transfert de données relatives aux voyageurs aériens ([1]), une législation européenne forte protégeant le citoyen dans toutes les situations internes à l'UE renforcerait également la position de l'UE lors de négociations avec des pays tiers. En l'absence d'une telle législation solide, il serait plutôt difficile de poser comme condition préalable au transfert de données un niveau de protection adéquat dans les pays tiers.

Autres préoccupations

18. *Mettre l'accent sur la qualité des données.* L'article 4 de la proposition de la Commission reprend non seulement les principaux principes relatifs à la qualité des données énoncés dans la directive 95/46/CE, mais il prévoit aussi certaines règles spécifiques en la matière. Ainsi il établit une distinction entre différents types de personnes concernées (suspects, personnes condamnées, victimes, témoins, etc.). Les données relatives à ces personnes devraient être traitées différemment, en prévoyant des garanties spécifiques, notamment en ce qui concerne les personnes non soupçonnées. Cet article oblige par ailleurs les États membres à faire une distinction entre les données selon leur degré d'exactitude et de fiabilité. Cette disposition est importante, car les services répressifs utilisent aussi des données non vérifiées fondées sur des présomptions et pas nécessairement sur des faits. Le CEPD considère ces dispositions comme des garanties indispensables, qui ne devraient pas être supprimées de la proposition, ni rendues facultatives.

19. *Traitement des données et limitation de la finalité.* Dans son avis de décembre 2005, le CEPD s'est penché sur la nécessité de prévoir des dispositions légales de meilleure qualité en ce qui concerne l'utilisation ultérieure de données qui ont été collectées par une autorité pour une finalité déterminée. Actuellement, les préoccupations du CEPD concernant l'article 5 ont principalement trait à son point de vue selon lequel, si d'un côté il est nécessaire d'autoriser le traitement (ultérieur) des données pour des finalités plus larges, d'un autre côté, la loi doit prévoir les conditions précises régissant ce traitement afin de protéger la personne concernée. Le CEPD met en garde contre les solutions qui font relever la question de la seule compétence de la loi nationale ou qui ne limitent pas les conditions régissant le traitement ultérieur conformément à la directive 95/46/CE et à la Convention n° 108 du Conseil de l'Europe ([2]). Pour ce qui est du traitement des catégories particulières de données, la question est traitée dans la directive 95/46/CE et dans la Convention n° 108 sous la forme d'une interdiction générale assortie d'exceptions ([3]). Le CEPD craint que, dans la décision-cadre, l'interdiction générale soit supprimée et que, de ce fait, l'exception devienne la règle. Une telle solution serait non seulement incompatible avec la directive 95/46/CE, mais elle serait également contraire à la Convention n° 108.

([1]) Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (JO L 298 du 27.10.2006, p. 29).

([2]) Voir l'article 13 de la directive 95/46/CE, en liaison avec son article 6, paragraphe 1, point b), et l'article 9 de la Convention n° 108, en liaison avec son article 5, point b).

([3]) Voir l'article 8 de la directive 95/46/CE et l'article 6 de la Convention n° 108.

20. *Échange de données avec d'autres autorités et des personnes privées*. La proposition de la Commission prévoit des limitations et des garanties spécifiques en ce qui concerne l'échange d'informations avec des autorités autres que les autorités policières et judiciaires, les personnes privées et les autorités des pays tiers. Le CEPD souligne l'importance que revêtent ces dispositions spécifiques, et ce pour les raisons suivantes. En premier lieu, l'échange d'informations avec ces «parties tierces» comporte des risques spécifiques (manquement aux règles de sécurité, traitement ultérieur pour des finalités différentes, etc.). En deuxième lieu, il est de plus en plus courant d'associer des tiers à l'action répressive ainsi qu'au traitement des informations dans ce domaine. La directive 2006/24/CE sur la conservation des données ([1]), l'accord sur les données PNR conclu avec les États-Unis et l'affaire dite «affaire Swift» ([2]) en sont de bons exemples. En troisième lieu, dans son arrêt PNR rendu le 30 mai 2006 ([3]), la Cour de justice européenne émet de sérieux doutes quant à la protection des données à caractère personnel collectées par des personnes privées à des fins commerciales et traitées ultérieurement à des fins répressives.

21. En ce qui concerne le transfert vers d'autres instances publiques ou personnes privées ou en provenance de celles-ci au sein de l'UE, il importe que la proposition traite la question de manière précise et offre des solutions conformes à la directive 95/46/CE. Ces solutions doivent garantir que les conséquences de la structure en piliers — en particulier l'incertitude quant à la délimitation de ces deux piliers en ce qui concerne l'échange des données à caractère personnel entre les services répressifs et d'autres parties — ne porteront pas atteinte à l'efficacité de la protection.

22. Pour ce qui est du transfert de données vers des pays tiers ou en provenance de ceux-ci, la proposition prévoit que la Commission prend une décision concernant le caractère adéquat du niveau de protection. Si cela n'est pas acceptable pour le Conseil, chaque État membre se prononcera alors lui-même sur le caractère adéquat du niveau de protection ou, pire encore, transférera les données sans vérifier le niveau de protection dans le pays tiers concerné. L'absence d'un système harmonisé pour l'échange de données à caractère personnel avec des pays tiers pourrait aussi:

— porter atteinte à la confiance entre les autorités des États membres, dans la mesure où une autorité pourrait être moins disposée à échanger des informations avec une autorité d'un autre État membre qui pourrait également communiquer ces informations aux autorités de pays tiers en l'absence de garanties claires,

— entraîner des comportements versatiles. Si l'autorité d'un État membre ne peut pas recevoir directement les informations d'un autre État membre en raison de la protection offerte par la décision-cadre, il est possible qu'il demande l'aide d'une autorité d'un pays tiers,

— inciter les autorités de pays tiers à recourir au «forum shopping»: ces autorités pourraient s'adresser à l'État membre ayant le plus bas niveau d'exigences légales en matière de transferts pour obtenir les informations souhaitées.

Le CEPD estime qu'il est essentiel de mettre en place des mécanismes garantissant l'application de normes communes et la prise de décisions coordonnées en ce qui concerne le caractère adéquat du niveau de protection, et ce également afin de se conformer à la Convention n° 108 du Conseil de l'Europe (en particulier son article 12) ([4]). Le texte de la décision-cadre devrait prévoir de tels mécanismes.

23. Le CEPD croit comprendre que plusieurs États membres contestent la base juridique concernant l'inclusion d'une disposition sur l'échange de données à caractère personnel avec des pays tiers lorsque ces données ne sont pas reçues d'une autorité compétente d'un autre État membre ou mises à disposition par celle-ci. Le CEPD estime qu'il n'y a pas lieu de contester cette base juridique. Les exemples développés dans l'avis de décembre 2005 ainsi que les arguments mentionnés au point précédent montrent le lien direct qui existe entre cet échange avec des pays tiers et la coopération policière et judiciaire visée à l'article 29 du traité UE. Une disposition sur l'échange de données à caractère personnel avec des pays tiers doit être vue comme une clause supplémentaire et nécessaire pour atteindre les objectifs énoncés à l'article 29 UE, en liaison avec l'article 6 UE, notamment une coopération plus étroite entre les forces de police dans le respect des droits fondamentaux.

([1]) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105 du 13.4.2006, p. 54).

([2]) Voir l'avis 10/2006 du Groupe de l'article 29 du 22 novembre 2006 sur le traitement des données à caractère personnel par la Société mondiale de télécommunications financières (SWIFT).

([3]) Arrêt dans les affaires C-317/04 et C-318/04.

([4]) Voir aussi plus précisément l'article 2 du protocole additionnel (ratifié par plusieurs États membres), qui correspond aux articles 25 et 26 de la directive 95/46/CE.

24. *Droits des personnes concernées*. La personne concernée a le droit d'être informée du traitement des données à caractère personnel la concernant. Ce droit est lié au principe du traitement loyal et licite des données à caractère personnel, qui en soi est respecté par la décision-cadre et est en outre protégé par la Convention n° 108 du Conseil de l'Europe, notamment par son article 5, point a), et son article 8. Un élément essentiel de ce droit est que cette information devrait être communiquée d'office par le responsable du traitement. Dans la mesure où, en règle générale, la personne concernée ne sait pas et ne peut pas savoir que des informations la concernant sont traitées, exiger d'elle qu'elle fasse une demande d'information serait contraire à l'esprit de ce droit. Bien entendu, ce droit d'être informé fait l'objet d'exceptions et il est évident que celles-ci peuvent jouer un rôle important dans le domaine répressif dans la mesure où des informations concernant une enquête pénale pourraient être préjudiciables à l'enquête elle-même. Néanmoins, toute solution qui subordonnerait le droit d'être informé à la présentation d'une demande par la personne concernée ne serait pas acceptable, ni compatible avec la Convention n° 108 du Conseil de l'Europe.

25. Le CEPD souligne que *la fonction des autorités chargées de la protection des données* devrait être compatible avec la fonction qui leur est dévolue par la directive 95/46/CE. Cette fonction est d'autant plus importante dans ce domaine de la coopération policière et judiciaire. La coopération entre les services répressifs dans le but de lutter efficacement contre le terrorisme et d'autres formes de criminalité grave nécessite de traiter des données à caractère personnel très souvent sensibles et de prévoir des exceptions aux droits des personnes concernées (voir par exemple le point précédent concernant le droit d'être informé).

26. Le CEPD attire en premier lieu l'attention sur la nécessité de prévoir un contrôle et une inspection efficaces par les autorités du traitement des données à caractère personnel dans les limites du champ d'application de la décision-cadre à l'examen, en particulier lorsque des données à caractère personnel sont échangées entre les États membres dans le cadre de la coopération policière. En second lieu, le rôle consultatif des autorités devrait être garanti, tant au sein de la juridiction nationale qu'au niveau du réseau institutionnalisé des autorités chargées de la protection des données, à savoir le groupe des autorités (dénommé «Groupe de l'Article 29» dans la directive). La participation des autorités chargées de la protection des données est nécessaire afin de renforcer la cohérence de la protection au titre de l'instrument à l'examen avec la protection dans le cadre de la directive 95/46/CE, d'assurer le respect des obligations légales et de parvenir à une harmonisation complète entre les États membres, également sur le plan pratique.

27. L'article 24 de la proposition de la Commission énonce des règles détaillées concernant la *sécurité*, comparables à celles figurant dans la convention Europol. Le CEPD met en garde contre la suppression de ces règles du texte de la proposition. Un niveau harmonisé de sécurité est un moyen important de renforcer la confiance, tant pour la personne concernée qu'entre les autorités des États membres.

28. Dans son avis de décembre 2005, le CEPD a recommandé que des garanties spécifiques soient mises en place en ce qui concerne les *traitements portant sur des catégories particulières de données*, notamment les données biométriques et les profils ADN. Alors que, dans le domaine répressif, ces catégories de données sont de plus en plus utilisées, cette utilisation peut présenter des risques particuliers pour la personne concernée. Des règles communes sont donc nécessaires. Le CEPD regrette que le Conseil n'ait pas tenu compte de cette recommandation, du moins pas de façon manifeste. Le CEPD demande instamment à la Commission et au Conseil d'adopter une proposition sur la question, qu'elle soit ou non liée au principe de la disponibilité des informations.

Conclusions

29. Le CEPD recommande au Conseil de prévoir plus de temps pour les négociations, de manière à parvenir à un résultat offrant une protection suffisante. Tout en étant conscient qu'il importe que le Conseil adopte à bref délai la décision-cadre, le CEPD tient à souligner que la rapidité de la prise de décision ne devrait pas entraîner une diminution des normes de protection.

30. La cohérence de la protection des données à caractère personnel est essentielle, quel que soit le lieu où elles sont traitées, par qui et à quelle fin. Le CEPD demande instamment au Conseil de respecter un niveau de protection qui ne soit pas inférieur à celui offert par la directive 95/46/CE ni à celui garanti par la Convention n° 108 du Conseil de l'Europe formulée en termes plus généraux, qui est contraignante pour les États membres.

31. Les règles communes relatives à la protection des données devraient s'appliquer à toutes les données en rapport avec le domaine de la coopération policière et judiciaire et ne pas être limitées aux échanges transfrontières entre les États membres. Le présent avis contient des arguments montrant qu'un champ d'application plus limité est impossible à mettre en œuvre et que, s'il était appliqué, cela accroîtrait la complexité et les coûts que les autorités doivent supporter et porterait atteinte à la sécurité juridique des personnes.

32. Les autres préoccupations du CEPD sont les suivantes:

— les dispositions spécifiques de la proposition de la Commission concernant la qualité des données ne devraient pas être supprimées, ni rendues facultatives,

— les dispositions relatives à l'utilisation ultérieure des données et aux catégories particulières de données devraient être conformes à la directive 95/46/CE et à la Convention n° 108 du Conseil de l'Europe,

— les dispositions spécifiques sur l'échange de données avec des parties autres que les services répressifs au sein de l'UE ne devraient pas être supprimées de la proposition et leur champ d'application ne devrait pas être limité. Pour ce qui est de l'échange de données avec les pays tiers, il conviendrait, *au minimum*, de mettre en place des mécanismes garantissant l'application de normes communes et la prise de décisions coordonnées en ce qui concerne le caractère adéquat du niveau de protection, et ce également afin de se conformer à la Convention n° 108 du Conseil de l'Europe. Le texte de la décision-cadre devrait prévoir de tels mécanismes,

— les solutions subordonnant le droit d'être informé à la présentation d'une demande par la personne concernée ne sont pas acceptables et sont incompatibles avec la Convention n° 108 du Conseil de l'Europe,

— la fonction des autorités chargées de la protection des données devrait être compatible avec la fonction qui leur est dévolue par la directive 95/46/CE,

— les règles détaillées concernant la sécurité, qui sont comparables à celles figurant dans la convention Europol, ne devraient pas être supprimées de la proposition,

— la Commission et le Conseil devraient adopter une proposition sur les traitements portant sur des catégories particulières de données, notamment les données biométriques et les profils ADN, qu'ils soient ou non liés au principe de la disponibilité des informations.

Fait à Bruxelles, le 29 novembre 2006.

Peter HUSTINX

Contrôleur européen de la protection des données