Groupe de travail «ARTICLE 29» sur la protection des données

1868/05/FR
WP 113

Avis 4/2005 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 du 21.09.2005)

Adopté le 21 octobre 2005

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la Direction C (Justice civile, droits fondamentaux et citoyenneté) de la Direction Générale Justice, liberté et sécurité de la Commission européenne, B-1049 Bruxelles, Belgique, bureau N° LX-46 01/43.

Adresse Internet: http://europa.eu.int/comm/justice_home/fsj/privacy/index_fr.htm

SYNTHESE

La proposition de directive de la Commission européenne sur la conservation des données nous place devant une décision historique.

La conservation des données relatives au trafic constitue une infraction au droit fondamental et inviolable à la confidentialité des communications.

Toute restriction à ce droit fondamental doit être justifiée par une nécessité urgente, n'être accordée que dans des cas exceptionnels et être assortie de garanties suffisantes.

Les fournisseurs de services de communication accessibles au public pourraient plus que jamais être tenus de stocker des milliards de données sur les communications de tous les citoyens à des fins d'enquête.

Le terrorisme représente pour notre société une menace réelle et pressante. Les gouvernements doivent réagir afin de répondre efficacement au besoin des citoyens de vivre en paix et en sécurité, tout en veillant à ne pas porter atteinte aux droits de l'homme - notamment au droit à la confidentialité des données - qui constituent un des fondements de notre société démocratique.

L'initiative de la Commission européenne pourrait, à terme, déboucher sur la fixation de périodes maximales de conservation plus courtes que celles qui ont été prévues dans d'autres propositions récentes.

Le groupe de travail se demande si la justification d'une conservation systématique et obligatoire des données, présentée par les autorités compétentes au sein des États membres, est étayée par des preuves limpides. Le groupe de travail doute également du bien-fondé des durées de conservation des données prévues dans la proposition de directive.

Comme indiqué ci-dessus, la justification d'une conservation systématique et obligatoire des données doit être clairement démontrée et étayée de preuves. Ce principe s'applique également aux périodes maximales à fixer. En tout état de cause, les conditions dans lesquelles les autorités compétentes pourront avoir accès à ces données et les utiliser pour lutter contre la menace de terrorisme devraient également être énoncées explicitement.

Les finalités de la conservation des données devraient être clairement définies dans la directive par référence à la lutte contre le terrorisme et la criminalité organisée plutôt qu'à la lutte contre des «infractions graves» indéterminées.

Il conviendrait également de tenir compte de l'existence d'approches moins préjudiciables pour la vie privée, notamment la procédure de «quick-freeze» (gel rapide).

La durée de conservation des données devrait, le cas échéant, être la plus courte possible et constituer le seuil maximal de conservation applicable à l'ensemble des États membres, même s'ils sont libres de déterminer des périodes plus courtes. Les mesures qui seront éventuellement introduites devraient faire l'objet d'une large diffusion.

Les preuves de la nécessité de ces mesures devraient être évaluées périodiquement. Les mesures prévues en matière de conservation des données devraient être limitées dans le temps sur la base d'une évaluation périodique (concept de «sunset legislation»), qui sera réalisée au minimum tous les deux ou trois ans. Le groupe de travail estime qu'une période de trois ans serait judicieuse.

En tout état de cause, il est inacceptable, dans le cadre juridique européen actuel, d'imposer une telle obligation aux fournisseurs de services de communication sans avoir prévu de garanties spécifiques suffisantes.

Enfin, le groupe de travail a défini vingt garanties spécifiques à envisager, notamment en ce qui concerne les exigences applicables aux destinataires et aux traitements ultérieurs des données, les

autorisations et contrôles nécessaires, les mesures applicables aux fournisseurs de services en termes de sécurité et de séparation logique des données, la détermination des catégories de données concernées ainsi que leur actualisation, et la nécessité d'exclure les données relatives au contenu.

créé par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30, paragraphe 1, point a) et paragraphe 3, de ladite directive et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002,

vu son règlement intérieur, et notamment ses articles 12 et 14,

a adopté l'avis suivant:

I. Contexte

Le 21 septembre 2005, dans le cadre des initiatives menées par l'Europe pour lutter contre le terrorisme et la criminalité organisée, la Commission européenne a présenté une *«Proposition de directive sur la conservation des données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE*[1]*»*.

La question qui y est abordée revêt une grande importance pour l'ensemble des citoyens.

La liberté et la confidentialité de la correspondance ainsi que de toutes les formes de communications font partie des fondements des démocraties modernes. Leur inviolabilité est énoncée dans plusieurs instruments, notamment des chartes constitutionnelles et elle est expressément garantie par la Convention européenne des droits de l'homme, sur laquelle est fondé le droit communautaire.

La proposition de directive nous place devant une décision historique. Elle vise en effet à introduire pour la première fois, à l'échelle européenne, l'obligation de conserver, à des fins d'enquête, des milliards de données relatives aux communications de tous les citoyens. Conformément au droit communautaire, ces données ne sont actuellement pas stockées ou elles sont conservées, à titre provisoire uniquement, par des fournisseurs de services de communications électroniques. Dans ce cas, elles sont exclusivement stockées à des fins contractuelles.

La conservation de données relatives au trafic porte atteinte au droit fondamental à la confidentialité des communications, qui est garanti aux particuliers en vertu de l'article 8 de la Convention européenne des droits de l'homme. Dans une société démocratique, toute atteinte à ce droit fondamental peut se justifier si elle est nécessaire dans l'intérêt de la sécurité nationale. Cette conservation des données peut déboucher sur le suivi et l'enregistrement de l'intégralité des relations et des contacts établis par des particuliers, ainsi que des lieux où ils se déroulent et des moyens utilisés à cet effet. La Cour européenne des droits de l'homme a également souligné que la surveillance secrète risquait de saper, voire de détruire, la démocratie au motif de la

[1] [COM (2005) 438 final] du 21.9.2005, *non encore publié au J.O.*

défendre. En outre, la Cour a affirmé que les États ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure qu'ils jugeraient appropriée.[2]

Aussi toute restriction de ce droit fondamental doit-elle être justifiée par une nécessité urgente, n'être autorisée que dans des cas exceptionnels et être assortie de garanties suffisantes. La conservation de données relatives au trafic - notamment des données de localisation - à des fins de répression, devrait être soumise à des conditions strictes[3]. Elle ne doit notamment être autorisée que pour une durée limitée et lorsqu'elle constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique.

Les pouvoirs dont disposent les services répressifs pour lutter contre le terrorisme doivent certes être effectifs mais ne peuvent être illimités ni utilisés abusivement. Un juste équilibre doit être atteint afin de ne pas mettre en péril le type de société que nous cherchons à protéger. Cet équilibre est particulièrement vital lorsqu'il s'agit d'obliger les fournisseurs de services de communication à conserver des données dont ils n'ont eux-mêmes aucune utilité. Il est en effet possible, à terme, d'en arriver à un contrôle sans précédent, continu et envahissant, de tous les types de communications et de mouvements de la totalité des citoyens au quotidien. La masse d'informations ainsi stockée ne serait en fin de compte utile, à des fins d'enquête, que dans un nombre limité de cas.

Il conviendrait également de tenir compte de l'impact d'une obligation de conservation des données aussi radicale sur des communications qui abordent des sujets délicats liés à certaines catégories de professionnels et/ou à des secrets d'enquête, ou à des activités menées par certaines institutions, qui sont expressément protégées par la loi.

C'est pourquoi, depuis plusieurs années déjà, la position du groupe de travail «article 29» et de la Conférence des autorités européennes chargées de la protection des données est claire et nette. A plusieurs reprises depuis 1997, le groupe de travail[4] et la Conférence européenne[5] ont contesté la nécessité d'adopter des mesures générales de conservation des données.

---

[2] Affaire Klass et autres contre République fédérale d'Allemagne, paragraphe 49.

[3] Voir, en particulier, l'article 15, paragraphe 1, de la directive 2002/58/CE.

[4] Voir (*tous les documents sont accessibles à l'adresse: http://europa.eu.int/comm/internal_market/privacy*):

- **avis 9/2004** sur le projet de décision cadre [..] (Document du Conseil 8958/04 du 28 avril 2004). Un récapitulatif des déclarations suivantes est repris dans l'annexe au présent avis;
- **avis 1/2003** sur le stockage de données relatives au trafic à des fins de facturation;
- **avis 5/2002** sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff (9-11 septembre 2002), relative à la conservation systématique et obligatoire des données de trafic des télécommunications;
- **avis 10/2001** sur la nécessité d'une approche équilibrée dans la lutte contre le terrorisme et la criminalité;
- **avis 4/2001** concernant le projet de convention du Conseil de l'Europe sur la cybercriminalité;
- **avis 7/2000** sur la proposition de la Commission européenne d'une directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000 COM (2000) 385;
- **recommandation 3/99** relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit;
- **recommandation 2/99** sur le respect de la vie privée dans le contexte de l'interception des télécommunications;
- **recommandation 3/97** sur l'anonymat sur Internet.

[5] Voir les déclarations adoptées à Stockholm (avril 2000) et Cardiff (avril 2002).

II. ÉVALUATION PRELIMINAIRE ET CONDITIONS PREALABLES GENERALES

1. La conservation des données peut constituer un instrument utile pour les enquêteurs. Toutefois, il va de soi que les conditions énoncées ci-dessus devraient être prouvées et justifiées.

Tout d'abord, la finalité d'une telle mesure devrait être énoncée très clairement. Deuxièmement, il convient de démontrer explicitement, preuves à l'appui, que cette conservation systématique et obligatoire des données est justifiée. Ce principe s'applique également aux périodes maximales à fixer. Troisièmement, les conditions dans lesquelles les autorités compétentes peuvent avoir accès à ces données et les utiliser pour lutter contre la menace de terrorisme devraient être expressément énoncées.

Les preuves avancées doivent être évaluées périodiquement, au minimum, et les résultats doivent être publiés, en tenant également compte du fait que les organisations liées au terrorisme et à la criminalité organisée risquent de réagir à l'introduction de moyens de surveillance générale des citoyens en élaborant des stratégies visant à éviter certains moyens de communication. Il serait alors indispensable de développer de nouveaux moyens de surveillance encore plus stricts, ce qui entraînerait une spirale de violations possibles des droits fondamentaux des citoyens qu'il sera difficile d'enrayer. Par ailleurs, une telle approche risque d'altérer la nature de la société que nous cherchons à préserver.

Le groupe de travail reconnaît que certaines conditions ont changé dans nos sociétés en raison des risques qu'entraîne la menace terroriste. Il est également conscient du fait que certaines données peuvent parfois se révéler utiles et être utilisées légitimement dans le cadre de certaines enquêtes. Par ailleurs, le groupe de travail reconnaît que l'initiative de la Commission européenne pourrait, à terme, déboucher sur la fixation de durées maximales de conservation plus courtes que celles qui ont été prévues dans le passé et sur lesquelles le groupe de travail avait émis un avis défavorable – en dernier lieu dans son avis n° 9/2004, adopté le 9 novembre 2004, WP 99.

Cependant, les circonstances qui justifient la conservation des données, même si elles sont censées s'appuyer sur les demandes émanant des autorités compétentes des États membres, ne semblent pas être étayées par des preuves limpides. De même, les conditions proposées ne nous paraissent pas suffisamment convaincantes à ce stade.

Il existe pourtant d'autres mesures utiles à prendre en compte à des fins d'enquête, qui portent moins atteinte aux droits fondamentaux des citoyens, notamment la procédure de «gel rapide», en vertu de laquelle ni les fournisseurs de services de communications ni les fournisseurs de services Internet ne sont contraints de stocker des données relatives au trafic. Par exemple, lorsque les circonstances le justifient, les services répressifs consultent les entreprises et leur demandent de stocker certaines données. Les services répressifs disposent alors de quelques semaines pour réunir les preuves qui leur permettront d'obtenir une ordonnance judiciaire. Grâce à ce document, elles pourront ensuite avoir accès à ces données.

En tout état de cause, il est indispensable de fixer une durée générale de conservation. Cette durée doit être la plus courte possible et se rapprocher au maximum de la période de conservation qui avait été fixée pour atteindre l'objectif initial pour lequel les fournisseurs de services avaient stocké ces données.

2. L'harmonisation des législations des États membres actuellement proposée par la Commission devrait préciser que la fixation d'une période de conservation des données à l'échelle européenne est fondée sur une évaluation de la proportionnalité réalisée au niveau européen, qui tient compte également du caractère transnational de la criminalité organisée ainsi que des exigences de sécurité maximales de tous les États membres.

Il faudra ensuite préciser que la période de conservation mentionnée dans la directive doit être considérée comme le seuil maximal harmonisé s'appliquant à l'ensemble des États membres.

Dès lors, il conviendrait de souligner que les États membres ne devront pas prévoir de périodes de conservation plus longues que celle fixée dans la directive, mais qu'ils seront libres de déterminer des périodes plus courtes. Il conviendrait également de rappeler que les données doivent être effacées à la fin de ladite période. Dans ce contexte, la formulation actuelle de l'article 11 de la proposition de directive n'est pas satisfaisante.

Le groupe de travail «article 29» approuve l'inclusion, dans la proposition, d'un article relatif à une évaluation (article 12) à réaliser périodiquement et au minimum tous les deux ans.

Cette évaluation devrait également porter sur la nécessité de conserver les données relatives au trafic utilisées par les services répressifs dans des cas spécifiques et clairement établis et devrait faire intervenir les autorités chargées de la protection des données. En outre, les résultats de ces évaluations devraient être publiés.

Il y a toutefois lieu de souligner que ladite évaluation ne devrait pas être réalisée dans un délai indéterminé, dans la mesure où la proposition repose sur l'évaluation concrète des hypothèses et des conditions qu'elle mentionne. Par conséquent, les mesures de conservation des données envisagées devraient être limitées dans le temps conformément au concept de «sunset legislation» (législation d'une durée de validité limitée). Le groupe de travail estime qu'un délai de trois ans serait judicieux. À l'expiration de ce délai, les mesures nationales d'exécution ordonnant la conservation des données devraient cesser d'être effectives, sans préjudice de la possibilité de commencer l'analyse nécessaire pour permettre au Conseil et au Parlement européen d'élaborer une nouvelle décision portant approbation d'une nouvelle directive avant l'expiration du délai de trois ans.

En ce qui concerne le principe de proportionnalité, le groupe de travail «article 29» se félicite également de la limitation des séries de données à conserver dans le cadre de l'utilisation d'Internet. En outre, il est préférable de déterminer une série maximale de données à conserver plutôt qu'une liste minimale. De manière générale, les données à conserver devraient se limiter à celles qui sont recueillies par les fournisseurs à des fins techniques ou de facturation.

Il est indispensable de déterminer l'accès aux données ainsi que les finalités de leur utilisation afin que toute mesure générale de conservation des données soit assortie de garanties suffisantes, et de soumettre ces mesures à un contrôle.

3. Les garanties prévues par le cadre juridique existant en matière de protection des données relevant du premier pilier (directives 95/46/CE et 2002/58/CE) devraient être spécifiées au regard du contexte particulier de l'action répressive liée à la conservation des données relatives au trafic. Des garanties spécifiques sont en effet indispensables afin d'éviter que la protection

fournie par la directive 2002/58/CE, en ce qui concerne notamment le droit à la confidentialité des services de communication accessibles au public, ne soit pas fortement compromise.

Par ailleurs, le groupe de travail estime que des garanties suffisantes devraient être prévues pour les opérations de traitement des données dans des secteurs qui n'entrent actuellement pas dans le champ d'application de ces directives.

C'est pourquoi le groupe de travail considère, entre autres, que la proposition de directive devrait prévoir elle-même ces garanties ou être évaluée et adoptée avec d'autres instruments juridiques appropriés. Le groupe de travail est notamment d'avis que la «décision cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière criminelle» doit faire l'objet d'une évaluation approfondie dans ce contexte également.

Enfin, compte tenu de l'impact de cette initiative sur les droits et libertés fondamentaux des citoyens concernés, les mesures qui seront éventuellement introduites devraient, selon le groupe de travail, être largement diffusées.

III. AUTRES GARANTIES SPECIFIQUES

En outre, le groupe de travail estime que les aspects suivants devraient au moins être abordés:

1. FINALITE

Les données devraient uniquement être conservées à des fins spécifiques de lutte contre le terrorisme et la criminalité organisée, plutôt que dans le cadre d'autres «infractions graves» indéterminées. Cette finalité limitée devrait également être mentionnée dans le titre de la proposition de directive.

2. BENEFICIAIRES

La directive devrait prévoir que les données ne sont mises à la disposition que des services répressifs expressément désignés, lorsqu'elles sont nécessaires à des fins de recherche, de détection, de poursuite et/ou de prévention du terrorisme. Une liste reprenant le nom de ces services répressifs devrait être rendue publique.

3. EXTRACTION DE DONNEES

La prévention du terrorisme ne devrait pas impliquer l'extraction de données à grande échelle sur la base des informations mentionnées dans la directive en ce qui concerne les habitudes de déplacement et de communication des personnes qui ne sont pas soupçonnées par les services répressifs. L'accès doit être limité aux seules données qui sont nécessaires dans le contexte d'une enquête spécifique.

4. TRAITEMENT ULTERIEUR

Tout traitement ultérieur des données conservées par les services répressifs, dans le cadre d'autres poursuites connexes, devrait être exclu ou fortement limité au moyen de garanties spécifiques. De plus, il conviendrait d'éviter tout accès à ces données par d'autres organes gouvernementaux. Les règles établies dans des instruments juridiques européens antérieurs concernant le secteur des communications électroniques ne peuvent être appliquées en violation de ce principe.

5. REGISTRES D'ACCES

Toute extraction de données devrait être consignée dans un registre. Ces registres ne devraient être mis à la disposition que de l'autorité et/ou de l'instance mentionnée au point 6 ci-après, à leur demande, ainsi que des autorités compétentes en matière de protection des données dans le cas d'un contrôle. Ils doivent être supprimés un an après leur production.

6. SURVEILLANCE JUDICIAIRE / INDEPENDANTE

L'accès aux données devrait, en principe, être dûment autorisé, au cas par cas, par une autorité judiciaire, sans préjudice des pays dans lesquels une possibilité d'accès spécifique est prévue par la loi, et devrait être soumis à une surveillance indépendante. Le cas échéant, les autorisations devraient préciser les données particulières requises pour ces cas spécifiques.

7. DESTINATAIRES

La directive devrait clairement définir les fournisseurs de services de communication accessibles au public qui sont concernés par ces obligations. Dans le cas d'Internet, il convient de prévoir une limitation pour les fournisseurs d'accès et les communications interpersonnelles (services de courrier électronique, téléphonie vocale sur Internet).

8. IDENTIFICATION

Il est également important de préciser, dans la directive, qu'il n'y a aucune obligation d'identification lorsque celle-ci n'est pas nécessaire à des fins de facturation ou autres pour l'exécution du contrat.

9. FINALITE D'ORDRE PUBLIC

Les fournisseurs de services ou de réseaux de communications électroniques accessibles au public ne devraient pas être autorisés à traiter, à des fins personnelles, des données qui ont été conservées uniquement pour des raisons d'ordre public.

10. SEPARATION DES SYSTEMES

Les systèmes de stockage de données à des fins d'ordre public devraient en particulier être logiquement séparés des systèmes utilisés à des fins commerciales par les fournisseurs et protégés par des mesures de sécurité plus strictes (notamment par le cryptage) afin d'éviter les accès et utilisations non autorisés.

11. MESURES DE SECURITE

Les mesures communautaires devraient fixer des normes minimales pour les mesures de sécurité organisationnelles et techniques que doivent prendre les fournisseurs, en précisant les exigences générales en matière de sécurité établies dans la directive 2002/58/CE.

12. TIERS

Les mesures communautaires devraient préciser que l'accès de tiers aux données conservées est illégitime.

13. DEFINITIONS

Le texte devrait inclure une définition claire des différentes catégories de données ainsi qu'une limitation des données relatives au trafic.

14. LISTE DE DONNEES ET MECANISMES DE REVISION

Il est nécessaire que la directive précise directement la liste des données personnelles à conserver, afin de permettre d'évaluer l'impact précis de cette obligation sur les droits et libertés

fondamentaux des citoyens concernés, en tenant compte des risques pour leur sphère personnelle ainsi que des aspects liés à la garantie de l'exactitude et de l'actualisation des données conservées. Toute proposition de modification de la liste des différentes catégories de données à conserver doit être soumise à un critère de nécessité strict. À la lumière de l'impact de ces mesures sur les droits et libertés fondamentaux des citoyens, la révision de ladite liste ne devrait être effectuée qu'avec l'approbation du Parlement européen, en collaboration avec les autorités compétentes en matière de protection des données. La participation de représentants des associations de consommateurs et d'utilisateurs, d'autres organes non gouvernementaux concernés et des associations européennes du secteur des communications électroniques devrait également être envisagée. À cet égard, il ne semble pas utile de procéder à la révision de ladite liste en se conformant uniquement à la procédure de comitologie, comme le prévoit la directive.

15. EXCLUSION DES DONNEES RELATIVES AU CONTENU

Dans la mesure où le champ d'application de la directive vise à exclure les données relatives au contenu des communications, des garanties spécifiques devraient être introduites afin d'assurer une distinction stricte et effective entre les données portant sur le contenu et les données relatives au trafic, tant pour Internet (c'est-à-dire, uniquement les données concernant l'ouverture/la fermeture d'une session ou des informations telles que les registres de serveurs de courrier, de cache web et de flux IP) que pour les services de téléphonie (conférences téléphoniques, télécopies, sms, téléphonie vocale).

16. TENTATIVES DE COMMUNICATION INFRUCTUEUSES

Les différentes catégories de données relatives au trafic liées à des tentatives de communication infructueuses ne devraient pas être incluses en l'absence d'une évaluation approfondie du bien-fondé de ces mesures à la lumière des principes mentionnés ci-dessus.

17. DONNEES DE LOCALISATION

La conservation des données de localisation ne devrait pas aller au-delà de l'identifiant cellulaire au début d'une communication.

18. SURVEILLANCE EFFECTIVE

Il conviendrait de prévoir des contrôles effectifs de l'utilisation initiale et de toute utilisation ultérieure compatible (y compris les duplications) par les autorités judiciaires dans le cadre et aux fins d'une procédure pénale, et en ce qui concerne la protection des données, indépendamment de l'existence d'une procédure judiciaire, par les autorités chargées de la protection des données.

19. PUBLICITE

La directive devrait prévoir l'obligation d'informer dûment l'ensemble des citoyens de toute opération de traitement de données qui sera éventuellement exécutée à la suite l'application des mesures prévues dans la directive.

20. COUTS

Le groupe de travail «article 29» constate qu'il est prévu que les États membres remboursent les coûts additionnels supportés par les fournisseurs services ou réseaux de communications électroniques accessibles au public. Le groupe de travail tient à souligner l'importance de cette question, exclusivement en ce qui concerne les caractéristiques directement liées à la protection des données. Les mesures relatives à la conservation des données devraient également prévoir le remboursement des investissements nécessaires afin d'adapter les systèmes de communication, des surcoûts liés à la divulgation de données aux services répressifs et à l'adoption de mesures

de sécurité. Il convient d'avoir une vision globale afin d'éviter toute incidence négative au niveau de la protection des données à caractère personnel et de la sphère économique des citoyens, qui pourraient être amenés à payer certains frais encourus par les fournisseurs. Dans ce contexte, il serait également utile d'examiner si le droit d'un fournisseur au remboursement de ces coûts doit être soumis au respect des normes minimales et être reconnu au cas par cas.

Le groupe de travail est convaincu que les considérations exprimées dans le présent avis seront dûment prises en compte et rappelle que toutes les garanties décrites ci-dessus doivent être mises en place avant que les obligations en matière de conservation des données n'entrent en application.

Fait à Bruxelles, le 21 octobre 2005

Par le groupe de travail

Le Président
Peter Schaar