I

(Communications)

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

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

(2005/C 298/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

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

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ([1]) et la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ([2]),

vu le règlement (CE) nº 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 ([3]), et notamment son article 41,

vu la demande d'avis formulée par la Commission conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001, reçue le 23 septembre 2005,

A ADOPTÉ L'AVIS SUIVANT:

I. **Introduction**

1. Le Contrôleur européen de la protection des données (CEPD) note avec satisfaction qu'il est consulté sur la base de l'article 28, paragraphe 2, du règlement (CE) nº 45/2001. Cependant, vu le caractère impératif de cette disposition, le présent avis devrait être mentionné dans le préambule de la directive.

2. Le CEPD convient qu'il est important que les services répressifs des États membres disposent de tous les instruments juridiques nécessaires, en particulier aux fins de la lutte contre

([1]) JO L 281 du 23.11.1995, p. 31.

([2]) JO L 201 du 31.7.2002, p. 37.

([3]) JO L 8 du 12.1.2001, p. 1.

le terrorisme et les autres formes graves de criminalité. La disponibilité suffisante de certaines données relatives au trafic et données de localisation générées par l'utilisation de services électroniques accessibles au public peut constituer un instrument précieux pour ces services répressifs et contribuer à la sécurité physique des personnes. Il convient toutefois de noter que les nouveaux instruments prévus dans la proposition en question n'en deviennent pas automatiquement nécessaires pour autant.

3. Il est tout aussi évident que la proposition a une incidence considérable sur la protection des données à caractère personnel. Si l'on considère la proposition du seul point de vue de la protection des données, les données relatives au trafic et les données de localisation ne devraient tout simplement pas être conservées à des fins de maintien de l'ordre. C'est pour des motifs de protection des données que la directive 2002/58/CE établit comme principe de droit l'obligation d'effacer les données relatives au trafic dès que leur stockage n'est plus nécessaire à des fins liées à la communication elle-même (y compris à des fins de facturation). Les exceptions à ce principe de droit doivent être assorties de conditions strictes.

4. Dans le présent avis, le CEPD va mettre en évidence l'incidence de la proposition sur la protection des données à caractère personnel. Il tiendra en outre compte du fait que, nonobstant son importance aux fins du maintien de l'ordre, la proposition ne doit pas avoir pour effet de priver les personnes de leur droit fondamental à la protection de leur vie privée.

5. Le présent avis du CEPD doit être lu à la lumière de ces considérations. Le CEPD a en vue une approche équilibrée, dans laquelle la nécessité et la proportionnalité de l'entrave à la protection des données jouent un rôle central.

6. Quant à la proposition elle-même, il faut y voir une réaction à l'initiative présentée par la République française, l'Irlande, le Royaume de Suède et le Royaume-Uni en vue de l'adoption d'une décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, de la recherche, de la détection et de la poursuite de délits et d'infractions pénales, y compris du terrorisme (ci-après dénommée «projet de décision-cadre»), que le Parlement européen a rejetée (dans le cadre de la procédure de consultation).

7. Le CEPD n'a pas été consulté sur le projet de décision-cadre et n'a pas rendu d'avis de sa propre initiative. Il n'entend pas donner d'avis comme tel sur le projet de décision-cadre, mais il renverra à ce projet dans le présent avis lorsqu'il le jugera nécessaire.

II. **Observations d'ordre général**

L'incidence de la proposition sur la protection des données à caractère personnel

8. Pour le CEPD, il est essentiel que la proposition respecte les droits fondamentaux. Une mesure législative qui porterait atteinte à la protection garantie par le droit communautaire et, plus particulièrement, par la jurisprudence de la Cour de justice et de la Cour européenne des droits de l'homme est non seulement inacceptable, mais également illégale. La société est peut-être confrontée à une conjoncture différente en raison des attentats terroristes, mais cette évolution ne peut avoir pour effet de mettre en péril les normes élevées de protection garanties par l'État de droit. La protection est assurée par la loi quels que soient les besoins réels en matière de maintien de l'ordre. De plus, la jurisprudence elle-même autorise des exceptions, lorsque celles-ci sont nécessaires dans une société démocratique.

9. La proposition a une incidence directe sur la protection garantie par l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après dénommée «la CEDH»). Selon la jurisprudence de la Cour européenne des droits de l'homme (ci-après dénommée «la CDH»):

— la conservation d'informations relatives à un particulier constitue une ingérence dans la vie privée de l'intéressé, même si les informations ne contiennent pas d'éléments à caractère sensible [arrêt Amann ([1])],

— il en va de même pour la pratique du «comptage» (*metering*) des appels téléphoniques, qui désigne l'emploi d'un mécanisme qui enregistre automatiquement les numéros formés sur un appareil de téléphone donné, ainsi que l'heure et la durée de chaque appel [arrêt Malone ([2])],

— les arguments plaidant en faveur de l'ingérence doivent être impérieux pour l'emporter sur les conséquences dommageables que l'existence même des dispositions législatives en cause pourrait entraîner sur la vie des intéressés [arrêt Dudgeon ([3])].

10. L'article 6, paragraphe 2, du traité UE prévoit que l'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la CEDH. Au point précédent, il a été montré que, selon la jurisprudence de la Cour européenne des droits de l'homme, l'obligation de conserver des données relève de l'article 8 de la CEDH et doit être étayée par des arguments impérieux qui

([1]) Arrêt de la CDH du 16 février 2000 dans l'affaire Amann, Recueil 2000-II, requête n° 27798/95.

([2]) Arrêt de la CDH du 2 août 1984 dans l'affaire Malone, série A n° 82, requête n° 8691/79.

([3]) Arrêt de la CDH du 22 octobre 1981 dans l'affaire Dudgeon, série A n° 45, requête n° 7525/76.

respectent le critère de l'arrêt Dudgeon. La nécessité et la proportionnalité de l'obligation de conserver des données — dans son intégralité — doivent être démontrées.

11. De plus, la proposition a une incidence considérable sur les principes de la protection des données reconnus par le droit communautaire:

— la durée de conservation des données est bien plus longue que celles qui sont habituellement prévues pour les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications (ci-après dénommés, pour ces deux services, «les fournisseurs»),

— conformément à la directive 2002/58/CE, et plus précisément à son article 6, des données ne peuvent être collectées et stockées que pour des motifs directement liés à la communication elle-même, y compris les fins de facturation ([1]). Elles doivent ensuite être effacées (sauf exceptions). Aux termes de la proposition, la conservation aux fins de l'application du droit pénal est impérative. Le point de départ est donc situé à l'opposé de celui de la directive 2002/58/CE,

— la directive 2002/58/CE garantit la sécurité et la confidentialité. La proposition ne peut créer de failles dans ce domaine; il faut prévoir des garanties strictes et préciser les restrictions en termes de finalités,

— l'instauration de l'obligation de conserver des données, prévue par la proposition, entraîne la constitution de bases de données de taille importante et fait courir des risques particuliers à la personne concernée. On peut ainsi penser à l'utilisation commerciale des données ou à leur utilisation pour des opérations de recherche aléatoire d'informations ou de fouille de données menées par les services répressifs ou les services de sécurité nationaux.

12. Enfin, la protection de la vie privée ainsi que la protection des données à caractère personnel sont toutes les deux consacrées par la charte des droits fondamentaux, comme l'indique l'exposé des motifs.

13. L'incidence de la proposition sur la protection des données à caractère personnel doit faire l'objet d'une analyse approfondie. En y procédant, le CEPD tiendra compte des éléments qui précèdent, et il conclura à la nécessité de prévoir davantage de garanties. Une simple référence au cadre juridique en vigueur en matière de protection des données (en particulier aux directives 95/46/CE et 2002/58/CE) n'est pas suffisante.

La nécessité de conserver des données relatives au trafic et des données de localisation

14. Le CEPD rappelle la conclusion formulée le 9 novembre 2004 par le groupe de travail «Article 29» sur la protection des données concernant le projet de décision-cadre: la conservation obligatoire de données relatives au trafic, dans les conditions prévues par le projet de décision-cadre, n'est pas acceptable. Cette conclusion reposait notamment sur le fait qu'aucune preuve n'avait pu être fournie de la nécessité de la conservation à des fins d'ordre public, étant donné que les analyses avaient révélé que la plus grande quantité des données relatives au trafic réclamées par les services répressifs datait de moins de six mois.

15. Selon le CEPD, les considérations susmentionnées du groupe de travail «Article 29» devraient servir de point de départ pour l'appréciation de la proposition. On ne peut toutefois se contenter de transposer à celle-ci le résultat de ces considérations; il faut tenir compte du caractère potentiellement évolutif de la situation. Selon le CEPD, les observations formulées ci-après pourraient être pertinentes aux fins de l'appréciation.

16. En premier lieu, certaines statistiques ont été produites pour montrer que, en pratique, l'ancienneté des données relatives au trafic réclamées par les services répressifs pouvait aller jusqu'à un an. La Commission et la présidence du Conseil accordent de l'importance à une étude réalisée par la police du Royaume-Uni ([2]) selon laquelle, bien que 85 % des données relatives au trafic réclamées par la police datent de moins de six mois, des données datant d'entre six mois et un an ont été utilisées dans des enquêtes complexes sur des infractions graves. Des exemples ont également été présentés. La durée de conservation figurant dans la proposition — un an pour les données téléphoniques — correspond à ces pratiques des services répressifs.

17. Le CEPD n'est pas convaincu que ces statistiques prouvent la nécessité de conserver jusqu'à un an les données relatives au trafic. Le fait que, dans certains cas, l'accès aux données relatives au trafic ou aux données de localisation ait aidé à élucider un crime ne signifie pas automatiquement que ces données soient (en général) nécessaires à des fins de maintien de l'ordre. On ne peut toutefois ignorer ces statistiques. Elles constituent au moins une tentative sérieuse visant à démontrer la nécessité de la conservation. Par ailleurs, les chiffres indiquent clairement qu'une période de conservation supérieure à un an n'est pas nécessaire compte tenu des pratiques actuelles des services répressifs.

18. En deuxième lieu, si la directive 2002/58/CE prévoit déjà la possibilité, pour les fournisseurs, de conserver des données relatives au trafic à des fins de facturation, cette possibilité n'est pas toujours utilisée, puisque, de plus en plus souvent, les données ne font l'objet d'absolument aucune conservation à des fins de facturation (cartes prépayées pour les

([1]) Voir également le point 3 du présent avis.

([2]) «Liberty and security, striking the right balance». Document de la présidence britannique de l'Union européenne daté du 7 septembre 2005.

communications de téléphonie mobile, abonnement forfaitaire, etc.). Dans ces cas — en pratique de plus en plus fréquents —, les données relatives au trafic et les données de localisation ne sont jamais stockées, mais effacées immédiatement après la communication. Il en va de même pour les appels qui n'aboutissent pas. Cela peut avoir une incidence sur l'efficacité de l'action des services répressifs.

19. Par ailleurs, cette évolution des services de télécommunications peut entraîner des perturbations dans le fonctionnement du marché intérieur, en raison notamment de l'adoption (imminente) de mesures législatives dans les États membres au titre de l'article 15 de la directive 2002/58/CE. À titre d'exemple, le gouvernement italien a récemment publié un décret obligeant les fournisseurs à stocker pendant quatre ans les données téléphoniques. Cette obligation aura un coût considérable dans certains États membres tels que l'Italie.

20. En troisième lieu, les méthodes de travail des services répressifs ont également évolué: les enquêtes proactives et le recours à l'assistance technique ont pris de l'importance. En conséquence, les autorités doivent pouvoir disposer d'outils adaptés et précis qui leur permettent d'accomplir leur mission dans le respect des principes de la protection des données. L'un des outils dont les autorités des États membres disposent habituellement est la conservation de données *a posteriori* ou le gel de données relatives aux communications, sur demande, dans le cas d'une enquête donnée. Il a été avancé que cet instrument qui, en soi, a moins de répercussions sur ces principes que l'instrument proposé à présent (la conservation des données) pouvait ne pas toujours être suffisant, en particulier pour localiser des personnes impliquées dans des actes de terrorisme ou d'autres infractions graves mais sans avoir été soupçonnées auparavant d'aucune activité terroriste. Cependant, d'autres éléments de preuve sont nécessaires pour déterminer si tel est réellement le cas.

21. En quatrième lieu, les craintes suscitées par les attentats terroristes ont pris de l'ampleur. Le CEPD partage l'avis, exprimé dans le cadre des propositions sur la conservation des données, selon lequel la sécurité physique est, en soi, primordiale. La société a besoin d'être protégée. C'est pourquoi les gouvernements ont l'obligation, en cas d'attaque contre la société, de montrer qu'ils tiennent bien compte de ce besoin de protection et d'examiner s'ils doivent y répondre en introduisant de nouvelles mesures législatives. Il va sans dire que le CEPD appuie sans réserve la mission des gouvernements — tant au niveau national qu'au niveau européen — qui consiste à protéger la société et à montrer qu'ils font le nécessaire pour assurer cette protection, notamment en adoptant de nouvelles mesures légitimes et efficaces sur la base des résultats de leur examen.

22. Si le CEPD admet que la conjoncture a évolué, il n'est pas, à l'heure actuelle, convaincu de la nécessité, énoncée dans la proposition, de conserver des données relatives au trafic et des données de localisation à des fins répressives. Il souligne l'importance du principe de droit établi par la directive 2002/58/CE, selon lequel les données relatives au trafic doivent être effacées dès que leur stockage n'est plus nécessaire à des fins liées à la communication elle-même. En outre, les données statistiques fournies ne prouvent pas que le cadre juridique en vigueur n'offre pas les instruments nécessaires pour protéger la sécurité physique, ni que les États membres exercent pleinement les compétences qui leur ont été attribuées, en droit européen, pour coopérer dans les limites du cadre juridique en vigueur (mais sans les résultats nécessaires).

23. Toutefois, si le Parlement européen et le Conseil — après avoir soigneusement mis en balance les intérêts en jeu — parviennent à la conclusion que la nécessité de conserver les données relatives au trafic et les données de localisation est suffisamment démontrée, le CEPD estime que la conservation ne peut être justifiée en droit communautaire que pour autant que le principe de proportionnalité soit respecté et que des garanties suffisantes soient prévues, conformément au présent avis.

La proportionnalité

24. Le caractère proportionnel de la nouvelle mesure législative proposée dépend lui-même des dispositions de fond qu'elle comporte: apporte-t-elle une réponse pertinente et proportionnée aux besoins de la société?

25. Le premier élément à prendre en considération a trait à la pertinence de la proposition: peut-on s'attendre à ce qu'elle améliore la sécurité physique des habitants de l'Union européenne? L'une des raisons de douter de cette pertinence, souvent mentionnée dans les discussions publiques, tient au fait que les données relatives au trafic et les données de localisation ne sont pas toujours rattachées à une personne précise, de sorte que les informations sur un numéro de téléphone (ou une adresse IP) ne révèlent pas nécessairement l'identité d'une personne. Une autre raison — encore plus sérieuse — d'en douter est qu'on peut se demander si l'existence de bases de données gigantesques permet aux services répressifs de trouver facilement ce dont ils ont besoin dans un cas précis.

26. Le CEPD estime que la seule conservation des données relatives au trafic et des données de localisation n'est pas en soi une réponse pertinente ni efficace. Des mesures supplémentaires s'imposent pour permettre aux autorités d'avoir un accès ciblé et rapide aux données dont elles ont besoin dans un cas précis. La conservation des données n'est pertinente et efficace que dans la mesure où des moteurs de recherche efficaces existent.

27. Le second élément à prendre en compte a trait au caractère proportionné de la réponse. Pour être proportionnée, la proposition devrait:

— limiter les durées de conservation. Celles-ci doivent correspondre aux besoins établis des services répressifs,

— limiter la quantité de données à stocker. Cette quantité doit correspondre aux besoins établis des services répressifs, et il convient de veiller à ce qu'il soit impossible d'accéder aux données relatives au contenu,

— prévoir des mesures de sécurité satisfaisantes permettant de limiter l'accès aux données et leur utilisation ultérieure, de garantir la sécurité des données et de faire en sorte que les personnes concernées elles-mêmes puissent exercer leurs droits.

28. Le CEPD souligne l'importance de ces limitations strictes, qui doivent s'accompagner de garanties appropriées en vue d'un accès limité. Il estime que, compte tenu de l'importance des trois éléments mentionnés au point précédent, les États membres ne devraient pas — en ce qui concerne ces éléments — prendre de mesures nationales complémentaires compromettant la proportionnalité. Ce besoin d'harmonisation sera développé dans la section IV.

Mesures de sécurité satisfaisantes

29. La proposition aura pour effet de mettre à la disposition des fournisseurs des bases de données dans lesquelles un nombre considérable de données relatives au trafic et de données de localisation seront stockées.

30. En premier lieu, la proposition devra veiller à ce que ces données ne puissent être accessibles et utilisables ultérieurement que dans des circonstances bien précises et à des fins bien précises et d'un nombre limité.

31. En deuxième lieu, les bases de données devront être suffisamment protégées (sécurité des données). À cet effet, il faut veiller à ce que, au terme des périodes de conservation, les données soient efficacement effacées. Il ne doit y avoir aucun «vidage de données» ni exploitation de données. En bref, cela exige un degré élevé de sécurité des données ainsi que des mesures de sécurité techniques et d'organisation appropriées.

32. Il est d'autant plus important d'assurer un degré élevé de sécurité des données que la simple existence des données pourrait susciter le dépôt de demandes d'accès et d'utilisation par au moins trois groupes de parties prenantes:

— les fournisseurs eux-mêmes. Ils pourraient être tentés d'utiliser les données pour atteindre leurs propres objectifs commerciaux. Des garanties sont nécessaires pour empêcher la copie de ces fichiers,

— les services répressifs: la proposition leur offre un droit d'accès, mais uniquement dans des cas précis et conformément à la législation nationale (article 3, paragraphe 2, de la proposition). Aucun accès ne devrait être autorisé à des fins de fouille de données ou de recherche aléatoire d'informations. L'échange de données avec les services d'autres États membres devrait être clairement réglementé,

— les services de renseignement (responsables de la sûreté nationale).

33. En ce qui concerne l'accès des services de renseignement aux données, le CEPD note que, conformément à l'article 33 du traité UE et à l'article 64 du traité CE, les interventions dans des domaines relevant des premier et troisième piliers ne portent pas atteinte à l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure. Selon le CEPD, il résulte de ces dispositions que l'Union européenne n'est pas compétente pour contrôler l'accès des services de sécurité ou du renseignement aux données conservées par les fournisseurs. En d'autres termes, le droit de l'Union européenne n'a d'incidence ni sur l'accès de ces services aux données relatives au trafic et aux données de localisation conservées par les fournisseurs ni sur l'utilisation ultérieure des informations obtenues par ces services. Il s'agit d'un élément à prendre en compte dans l'appréciation de la proposition. C'est aux États membres qu'il devrait incomber de prendre les mesures nécessaires pour réglementer l'accès des services de renseignement aux données en question.

34. En troisième lieu, les effets décrits aux points précédents ont des répercussions potentielles sur la personne concernée. Il faut prévoir des garanties supplémentaires pour s'assurer que celle-ci puisse exercer simplement et rapidement les droits que lui confère son «statut» de personne concernée. Le CEPD souligne la nécessité d'un contrôle effectif sur l'accès et l'utilisation ultérieure, exercé de préférence par les autorités judiciaires des États membres. Les garanties devraient également s'appliquer en cas d'accès aux données relatives au trafic et d'utilisation ultérieure de ces données par les autorités d'autres États membres.

35. Dans ce contexte, le CEPD renvoie à des initiatives pour un nouveau cadre juridique sur la protection des données qui soit applicable à l'action des services répressifs (pour ce qui relève du troisième pilier du traité UE). Selon le CEPD, ce cadre juridique exige des garanties supplémentaires et ne saurait se limiter à une réaffirmation des principes généraux de la protection des données prévus pour le premier pilier ([1]).

36. En quatrième lieu, il existe un lien direct entre le caractère approprié et le coût des mesures de sécurité. Une loi satisfaisante sur la conservation des données doit par conséquent comporter des dispositions incitant les fournisseurs à investir dans l'infrastructure technique. Ils pourraient par exemple être indemnisés pour les frais supplémentaires induits par des mesures de sécurité appropriées.

37. En résumé, les mesures de sécurité devraient, pour être satisfaisantes:

— limiter l'accès aux données et leur utilisation ultérieure,

— prévoir des mesures de sécurité techniques et d'organisation suffisantes pour protéger les bases de données. Il s'agit notamment d'effacer correctement les données au

([1]) Voir, à cet égard, le document de synthèse sur les services répressifs et l'échange d'informations au sein de l'UE, adopté lors de la conférence de printemps des autorités européennes de protection des données, qui s'est tenue à Cracovie les 25 et 26 avril 2005.

terme du délai de conservation et d'accuser réception des demandes d'accès et d'utilisation émanant de différents groupes de parties prenantes,

— garantir l'exercice des droits des personnes concernées, sans se contenter de réaffirmer les principes généraux de la protection des données,

— prévoir des dispositions incitant les fournisseurs à investir dans l'infrastructure technique.

III. La base juridique et le projet de décision-cadre

38. La proposition a pour fondement le traité CE, en particulier son article 95; aux termes de son article 1er, elle a pour objectif d'harmoniser les obligations des fournisseurs en matière de traitement et de conservation des données relatives au trafic et des données de localisation. Elle prévoit que les données portant sur des infractions pénales ne sont transmises qu'aux autorités nationales compétentes, dans des cas précis, mais elle laisse aux États membres le soin de définir plus précisément la finalité visée ainsi que l'accès aux données et leur utilisation ultérieure, sous réserve des garanties prévues par le cadre communautaire en vigueur en matière de protection des données.

39. À cet égard, la proposition a un champ d'application plus restreint que le projet de décision-cadre, qui est fondé sur l'article 31, paragraphe 1, point c), du traité UE et qui comporte des dispositions supplémentaires sur «l'accès aux données retenues» et sur les demandes d'accès adressées par d'autres États membres. L'exposé des motifs explique cette limitation du champ d'application de la proposition: l'accès des services répressifs concernés aux informations et l'échange de ces informations entre ces services sont des questions qui ne relèvent pas du champ d'application du traité CE.

40. Le CEPD n'est pas convaincu par cette affirmation figurant dans l'exposé des motifs. Une intervention de la Communauté fondée sur l'article 95 du traité CE (marché intérieur) doit avoir pour objet principal l'élimination des entraves aux échanges commerciaux. Selon la jurisprudence de la Cour de justice, pareille intervention doit vraiment être de nature à contribuer à l'élimination de ce type d'entrave. Le législateur communautaire doit en outre, lors de son intervention, respecter les droits fondamentaux (article 6, paragraphe 2, du traité UE; voir la section II du présent avis). C'est pourquoi l'instauration, au niveau communautaire, de règles sur la conservation des données dans l'intérêt du marché intérieur peut imposer de traiter, également au niveau de la Communauté européenne, du respect des droits fondamentaux: si le législateur communautaire ne pouvait instaurer de règles sur l'accès aux données et leur utilisation, il ne pourrait s'acquitter de l'obligation qui lui est faite à l'article 6 du traité UE, puisque ces règles sont indispensables pour garantir une conservation des données dans le strict respect des droits fondamentaux. En d'autres termes, les règles relatives à l'accès aux données, ainsi qu'à leur utilisation et à leur échange, sont, selon le CEPD, indissociables de l'obligation proprement dite de conserver les données.

41. Le CEPD convient que l'institution des autorités compétentes relève de la responsabilité des États membres. Il en va de même pour l'organisation de la répression et de la protection judiciaire. Cependant, un acte communautaire peut imposer aux États membres des conditions applicables à la désignation des autorités compétentes, au contrôle juridictionnel ou à l'accès des citoyens à la justice. C'est grâce à ces dispositions qu'existent, au niveau national, des mécanismes appropriés garantissant la pleine efficacité de l'acte, et notamment sa stricte conformité avec la législation relative à la protection des données.

42. Le CEPD soulève un autre point lié à la base juridique. Il appartient au législateur communautaire de choisir la base juridique qui convient et, en conséquence, la procédure législative appropriée. Certes, ce choix dépasse les limites de la mission du CEPD. Toutefois, compte tenu des questions fondamentales et primordiales qui se posent en l'occurrence, le CEPD exprime en l'espèce une préférence marquée pour la procédure de codécision: seule cette procédure constitue un processus transparent de prise de décision, auquel participent pleinement les trois institutions concernées et dans lequel les principes qui fondent l'Union sont pleinement respectés.

IV. Le besoin d'harmonisation

43. La proposition de directive harmonise les types de données à conserver, leurs durées de conservation, ainsi que les finalités pour lesquelles elles peuvent être transmises aux autorités compétentes. La proposition vise l'harmonisation pleine et entière de ces éléments. Elle est, à cet égard, d'une nature fondamentalement différente de celle du projet de décision-cadre, qui prévoit des règles minimales.

44. Le CEPD souligne la nécessité d'une harmonisation pleine et entière de ces éléments, eu égard au fonctionnement du marché intérieur, aux besoins du maintien de l'ordre et — dernier point, mais non le moindre — à la CEDH et aux principes de la protection des données.

45. En ce qui concerne le fonctionnement du marché intérieur, l'harmonisation des obligations en matière de conservation des données justifie le choix de la base juridique de la proposition (article 95 du traité CE). Permettre l'existence de différences fondamentales entre les législations des différents États membres ne supprimerait certes pas les perturbations qui existent déjà dans le fonctionnement du marché intérieur des communications électroniques et qui sont dues notamment à l'adoption (imminente) de mesures législatives dans les États membres au titre de l'article 15 de la directive 2002/58/CE (voir le point 19 du présent avis).

46. Ce qui précède est d'autant plus important qu'un nombre considérable de communications électroniques relève de la compétence de plusieurs États membres. On peut citer, à titre d'exemple, les appels téléphoniques transfrontières, l'itinérance (*roaming*), le franchissement de frontières *pendant* des communications par téléphonie mobile et le recours à un fournisseur dans un État membre autre que le pays de résidence de l'intéressé.

47. De plus, l'absence d'harmonisation, dans ce contexte, irait à l'encontre des besoins du maintien de l'ordre, puisque les autorités compétentes doivent satisfaire à des obligations légales différentes. L'échange d'informations entre les autorités des États membres pourrait s'en trouver entravé.

48. Enfin, le CEPD souligne — en renvoyant à la responsabilité qui lui incombe aux termes de l'article 41 du règlement (CE) nº 45/2001 — que l'harmonisation pleine et entière des principaux éléments figurant dans la proposition est indispensable au respect de la CEDH et des principes de la protection des données. Toute mesure législative obligeant à conserver des données relatives au trafic et des données de localisation doit, pour être acceptable du point de vue de la protection des données et satisfaire aux critères de la nécessité et de la proportionnalité, limiter clairement la quantité de données à conserver, leurs durées de conservation ainsi que (les finalités de) l'accès aux données et (de) leur utilisation ultérieure.

V. Observations sur les articles de la proposition

Article 3: obligation de conservation de données

49. L'article 3 est la disposition clé de la proposition. L'article 3, paragraphe 1, introduit l'obligation de conserver des données relatives au trafic et des données de localisation, tandis que l'article 3, paragraphe 2, met en œuvre le principe de limitation de l'objet du traitement. Cette disposition énonce trois limitations importantes. Les données conservées peuvent uniquement être transmises:

— aux autorités nationales compétentes,

— dans des cas précis,

— à des fins de prévention, de recherche, de détection et de poursuite des infractions pénales graves, comme les actes terroristes et la criminalité organisée.

L'article 3, paragraphe 2, renvoie à la législation nationale des États membres pour la description détaillée d'autres limitations.

50. Le CEPD accueille favorablement l'article 3, paragraphe 2, qui constitue selon lui une disposition importante, mais considère que les limitations ne sont pas suffisamment précises, que l'accès et l'utilisation ultérieure devraient faire l'objet de dispositions explicites dans la directive et que des garanties supplémentaires s'imposent. Comme il a été indiqué dans la section III du présent avis, le CEPD n'est pas convaincu que l'absence de dispositions (précises) sur l'accès aux données relatives au trafic et aux données de localisation et sur leur utilisation ultérieure soit une conséquence inévitable du choix de la base juridique de la proposition (article 95 du traité CE), ce qui le conduit à formuler les observations qui suivent.

51. En premier lieu, il n'est pas précisé que d'autres parties prenantes, comme le fournisseur lui-même, n'ont pas accès aux données. Conformément à l'article 6 de la directive 2002/58/CE, les fournisseurs ne peuvent traiter des données relatives au trafic que jusqu'à la fin de la période au cours de laquelle les données sont conservées à des fins de facturation. Selon le CEPD, rien ne justifie que les fournisseurs ou toute autre partie intéressée bénéficient d'un accès autre que celui prévu par la directive 2002/58/CE, et dans les conditions fixées par celle-ci.

52. Le CEPD recommande d'ajouter au texte une disposition garantissant que personne en dehors des autorités compétentes n'ait accès aux données. Cette disposition pourrait être formulée comme suit: «l'accès aux données et leur traitement ne sont autorisés que pour la finalité visée à l'article 3, paragraphe 2» ou «les fournisseurs garantissent de façon effective que l'accès est uniquement accordé aux autorités compétentes».

53. En deuxième lieu, la limitation à des cas précis semble interdire l'accès ordinaire pour des opérations de recherche aléatoire d'informations ou des activités de fouille de données. Le texte de la proposition devrait néanmoins préciser que des données ne peuvent être transmises que si cela s'avère nécessaire en considération d'une infraction pénale particulière.

54. En troisième lieu, le CEPD se félicite que la finalité de l'accès soit limitée aux infractions pénales graves, comme les actes terroristes et la criminalité organisée; dans d'autres cas moins graves, il serait malaisé de respecter le critère de proportionnalité en accordant un accès aux données relatives au trafic et aux données de localisation. Toutefois, le CEPD se demande si cette limitation est suffisamment précise, en particulier pour les cas où l'accès serait demandé en considération d'une infraction pénale grave autre qu'un acte de terrorisme ou de criminalité organisée. La pratique ne sera pas la même dans tous les États membres. Le CEPD a souligné, dans la section IV du présent avis, la nécessité d'une harmonisation pleine et entière des principaux éléments qui figurent dans la proposition. Il recommande en conséquence de limiter la disposition en question à *certaines* infractions pénales graves.

55. En quatrième lieu, contrairement au projet de décision-cadre, la proposition ne comporte pas de disposition concernant l'accès. Selon le CEPD, la directive ne devrait pas passer sous silence l'accès aux données et leur utilisation ultérieure, qui font partie intégrante du sujet traité (voir la section III du présent avis).

56. Le CEPD recommande d'ajouter à la proposition un ou plusieurs articles concernant l'accès des autorités compétentes aux données relatives au trafic et aux données de localisation et à l'utilisation ultérieure de ces données. L'objectif de ces articles devrait être de veiller à ce que les données ne soient utilisées que pour les finalités mentionnées à l'article 3, paragraphe 2, que les autorités garantissent la qualité, la confidentialité et la sécurité des données qu'elles ont obtenues et que les données soient effacées lorsqu'elles ne sont plus

nécessaires aux fins de la prévention, de la recherche, de la détection et de la poursuite de l'infraction pénale en question. Il devrait en outre être précisé que, dans des cas précis, l'accès devrait être soumis à un contrôle juridictionnel dans les États membres.

57. En cinquième lieu, la proposition n'entoure pas la protection des données de garanties supplémentaires. Les considérants renvoient simplement aux garanties prévues par la législation en vigueur, plus précisément par la directive 95/46/CE et la directive 2002/58/CE. Le CEPD ne souscrit pas à cette approche de la protection des données, qu'il juge restrictive au regard de l'importance particulière qu'il convient d'accorder aux garanties (supplémentaires) (voir la section II du présent avis).

58. Par conséquent, le CEPD recommande d'inclure une partie sur la protection des données. Cette partie pourrait comporter les recommandations qui précèdent au sujet de l'article 3, paragraphe 2, ainsi que d'autres dispositions relatives à la protection des données, telles que celles qui portent sur l'exercice de ses droits par la personne concernée (voir la section II du présent avis), sur la qualité et la sécurité des données, ainsi que sur les données relatives au trafic et les données de localisation relatives à des personnes non soupçonnées d'avoir commis une infraction pénale.

Article 4: catégories de données à conserver

59. D'une manière générale, le CEPD approuve l'article et l'annexe, et ce en raison:

— de la technique législative choisie, qui comprend un descriptif fonctionnel dans le dispositif de la directive et des détails techniques en annexe, ce qui est suffisamment souple pour répondre de manière appropriée à l'évolution technologique, tout en offrant au citoyen une garantie de sécurité juridique,

— de la distinction établie entre données de télécommunications et données internet, même si cette distinction tend à perdre de l'importance sur le plan technologique. Cette distinction est néanmoins importante du point de vue de la protection des données, car, sur l'internet, la frontière entre données relatives au contenu et données relatives au trafic n'est pas nettement définie (voir, par exemple, l'article 1er, paragraphe 2, de la directive, d'où il ressort que les informations consultées sur l'internet constituent des données relatives au contenu),

— du degré d'harmonisation: la proposition envisage un degré élevé d'harmonisation, avec une liste exhaustive des catégories de données à conserver (contrairement au projet de décision-cadre qui contient une liste minimale, les États membres disposant d'une grande marge d'appréciation pour ajouter des données). Du point de vue de la protection des données, il est essentiel de procéder à une harmonisation pleine et entière (voir la section IV).

60. Le CEPD recommande les modifications suivantes:

— le second alinéa de l'article 4 devrait comporter des critères plus concrets garantissant l'exclusion des données relatives au contenu. Il conviendrait d'ajouter la phrase suivante: «l'annexe ne peut inclure des données indiquant le contenu d'une communication»,

— l'article 5 offre la possibilité d'une révision de l'annexe par une directive de la Commission («procédure de comité»). De l'avis du CEPD, il serait préférable que les révisions de l'annexe ayant une incidence significative sur la protection des données soient opérées par voie de directive, selon la procédure de codécision ([1]).

Article 7: durées de conservation

61. Le CEPD se félicite du fait que les durées de conservation prévues dans la proposition soient sensiblement inférieures à celles qui sont prévues dans le projet de décision-cadre:

— tout en rappelant les doutes émis dans le présent avis quant aux éléments établissant la nécessité de conserver jusqu'à un an les données relatives au trafic, il convient de noter que la durée d'un an correspond aux pratiques des services répressifs, *telles qu'elles ressortent* des données statistiques fournies par la Commission et la présidence du Conseil,

— ces données statistiques montrent également que, sauf dans des cas exceptionnels, une plus longue durée de conservation des données ne correspond pas aux pratiques des services répressifs,

— une durée plus courte de six mois pour les données relatives à des communications électroniques utilisant uniquement ou principalement le protocole internet est importante du point de vue de la protection des données, car la conservation de communications internet entraîne la constitution de vastes bases de données (données qui ne sont généralement pas conservées à des fins de facturation), la frontière avec les données relatives au contenu n'est pas nettement définie et la conservation des données pendant plus de six mois ne correspond pas aux pratiques des services répressifs.

62. Il devrait être précisé dans le texte que:

— les durées de conservation de six mois et un an respectivement sont des durées maximales,

([1]) Voir, à cet égard, l'avis du CEPD du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (point 3.12).

— les données sont effacées au terme du délai de conservation. Le texte devrait en outre préciser par quel moyen l'effacement devrait être effectué. Selon le CEPD, un fournisseur doit effacer les données par des procédés automatisés, au moins quotidiennement.

Article 8: conditions à observer pour le stockage des données conservées

63. Cet article est étroitement lié à l'article 3, paragraphe 2, et comporte une disposition importante qui peut garantir, dans des cas précis, la limitation de l'accès aux seules données expressément nécessaires. L'article 8 et l'article 3, paragraphe 2, présupposent que les données demandées sont transmises par les fournisseurs aux autorités et que celles-ci n'ont pas directement accès aux bases de données. Le CEPD recommande de formuler explicitement ce sous-entendu.

64. La disposition devrait être plus précise et indiquer que:

— les données demandées sont transmises par les fournisseurs aux autorités (voir le point 63),

— les fournisseurs doivent installer l'architecture technique nécessaire, y compris les moteurs de recherche, pour faciliter l'accès ciblé aux données indiquées,

— les fournisseurs doivent veiller à ce que seuls ceux de leurs employés qui exercent des responsabilités techniques précises aient accès aux bases de données pour des raisons techniques et à ce que ces employés soient conscients du caractère sensible des données et soumis, dans l'exercice de leurs fonctions, à de strictes règles internes de confidentialité,

— la transmission des données ne doit pas seulement avoir lieu sans délai, mais également sans que soient révélées des données relatives au trafic ou des données de localisation autres que celles qui sont nécessaires aux fins de la demande.

Article 9: statistiques

65. L'obligation faite aux fournisseurs de transmettre annuellement des statistiques aide les institutions communautaires à contrôler l'efficacité de la mise en œuvre et de l'application de la proposition. Des informations pertinentes sont nécessaires.

66. Selon le CEPD, cette obligation met en œuvre le principe de transparence. Le citoyen européen est en droit de savoir si la conservation des données est efficace. C'est pourquoi le fournisseur devrait de surcroît avoir l'obligation de tenir des fichiers journaux et de procéder à des audits (internes) systématiques, afin de permettre aux autorités nationales chargées de la protection des données de contrôler en pratique l'application des règles relatives à la protection des données ([1]). Il conviendrait de modifier la proposition dans ce sens.

Article 10: coûts

67. Comme il a été indiqué dans la section II, il existe un lien direct entre le caractère approprié et le coût des mesures de sécurité ou, en d'autres termes, entre la sécurité et le coût. Le CEPD estime donc que l'article 10 — qui prévoit le remboursement aux fournisseurs des surcoûts qu'ils justifient avoir supportés — constitue une disposition importante susceptible d'inciter les fournisseurs à investir dans l'infrastructure technique.

68. D'après les estimations de l'analyse d'impact que la Commission a transmise au CEPD, le coût de la conservation des données est considérable. Pour un grand fournisseur de réseaux et de services, ce coût pourrait dépasser les 150 millions EUR pour une durée de conservation de douze mois, avec un coût annuel de fonctionnement avoisinant les 50 millions EUR ([2]). Aucun chiffre n'est toutefois fourni sur le coût des mesures de sécurité supplémentaires telles que les coûteux moteurs de recherche (voir l'observation relative à l'article 6) ni sur les conséquences financières (estimées) du remboursement intégral des surcoûts supportés par les fournisseurs.

69. Selon le CEPD, il est nécessaire de disposer de données chiffrées plus précises pour être en mesure de juger la proposition dans son intégralité. Le CEPD suggère de préciser dans l'exposé des motifs les conséquences financières de la proposition.

70. En ce qui concerne le contenu même de l'article 10, le lien entre le caractère approprié des mesures de sécurité et leur coût devrait être explicité dans le libellé de cette disposition. De plus, la proposition devrait fixer, pour les mesures de sécurité que les fournisseurs doivent prendre, des normes minimales conditionnant leur remboursement par un État membre. Selon le CEPD, l'établissement de ces normes ne

([1]) Voir, à cet égard, l'avis du CEPD du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (point 3.9).

([2]) La Commission cite les chiffres de l'ETNO (Association européenne des exploitants de réseaux de télécommunications) ainsi qu'un rapport du député européen Alvaro sur le projet de décision-cadre.

devrait pas être totalement laissé à l'appréciation des États membres. En effet, le degré d'harmonisation visé par la directive pourrait s'en trouver affecté. De plus, il faut tenir compte du fait que les États membres supportent les conséquences financières du remboursement.

Article 11: modification de la directive 2002/58/CE

71. Il convient de clarifier le lien entre la proposition et l'article 15, paragraphe 1, de la directive 2002/58/CE, étant donné que la proposition vide la disposition précitée d'une grande partie de sa substance. Il conviendrait de supprimer les références aux articles 6 et 9 de la directive 2002/58/CE qui figurent à l'article 15, paragraphe 1 (de la même directive), ou du moins de les modifier, afin de bien montrer que les États membres ne sont plus compétents pour adopter des textes législatifs ayant trait à des infractions pénales, en complément de ce qui est prévu par la présente proposition. Toute ambiguïté doit être levée sur les compétences que conservent les États membres — par exemple à l'égard de la conservation de données pour des finalités liées à des infractions pénales «sans caractère de gravité».

Article 12: évaluation

72. Le CEPD se félicite que la proposition comporte un article prévoyant que la directive soit évaluée au plus tard trois ans après son entrée en vigueur. Les doutes qui subsistent quant à la nécessité et à la proportionnalité de la proposition rendent cette évaluation encore plus importante.

73. Dans cette optique, le CEPD recommande de prévoir une obligation encore plus stricte, comportant les éléments suivants:

— l'évaluation devrait comprendre une analyse de l'efficacité de la mise en œuvre de la directive, du point de vue de l'action des services répressifs, ainsi qu'une analyse de l'impact sur les droits fondamentaux de la personne concernée. La Commission devrait y faire figurer tout élément d'appréciation susceptible d'avoir une incidence sur l'évaluation,

— l'évaluation devrait avoir lieu à intervalles réguliers (au moins tous les deux ans),

— la Commission devrait être tenue, le cas échéant, de soumettre des propositions de modification de la proposition (comme le prévoit l'article 18 de la directive 2002/58/CE).

VI. **Conclusions**

Conditions préalables

74. Pour le CEPD, il est essentiel que la proposition respecte les droits fondamentaux. Une mesure législative qui porterait atteinte à la protection garantie par le droit communautaire et, plus particulièrement, par la jurisprudence de la Cour de justice et de la Cour européenne des droits de l'homme est non seulement inacceptable, mais également illégale.

75. La nécessité et la proportionnalité de l'obligation de conserver des données — dans son intégralité — doivent être démontrées.

76. En ce qui concerne la nécessité: si le CEPD admet que la conjoncture a évolué, il n'est pas, à l'heure actuelle, convaincu de la nécessité, énoncée dans la proposition, de conserver des données relatives au trafic et des données de localisation à des fins répressives.

77. Le CEPD expose néanmoins, dans le présent avis, son point de vue sur la proportionnalité de la proposition. Il estime en premier lieu que la seule conservation des données relatives au trafic et des données de localisation n'est pas en soi une réponse pertinente ni efficace. Des mesures supplémentaires s'imposent pour permettre aux autorités d'avoir un accès ciblé et rapide aux données dont elles ont besoin dans un cas précis. En second lieu, la proposition devrait:

— limiter les durées de conservation. Celles-ci doivent correspondre aux besoins des services répressifs,

— limiter la quantité de données à stocker. Cette quantité doit correspondre aux besoins des services répressifs et garantir l'impossibilité d'accéder aux données relatives au contenu,

— prévoir des mesures de sécurité satisfaisantes.

Appréciation générale

78. Le CEPD souligne l'importance du fait que le texte actuel de la proposition prévoit une harmonisation pleine et entière des principaux éléments figurant dans la proposition, en particulier les types de données à conserver, les durées pendant lesquelles il convient de les conserver ainsi que (les finalités de) l'accès aux données et (de) leur utilisation ultérieure.

79. Sur certains points, des éclaircissements sont nécessaires, par exemple pour garantir l'effacement approprié des données au terme de la période de conservation et prévenir efficacement l'accès aux données et leur utilisation par différents groupes de parties prenantes.

80. Le CEPD estime qu'il est essentiel de prendre les mesures suivantes pour que la proposition soit acceptable du point de vue de la protection des données:

— ajouter à la proposition des dispositions portant spécifiquement sur l'accès aux données relatives au trafic et aux données de localisation par les autorités compétentes et sur l'utilisation ultérieure de ces données, en tant que partie intégrante et indissociable du sujet traité,

— ajouter à la proposition des garanties supplémentaires pour la protection des données (sans se contenter d'une simple référence aux garanties prévues par la législation en vigueur, plus précisément par les directives 95/46/CE et 2002/58/CE), notamment pour garantir l'exercice des droits des personnes concernées,

— ajouter à la proposition de nouvelles dispositions incitant les fournisseurs à investir dans une infrastructure technique appropriée, en particulier des incitations financières. Cette infrastructure ne peut être appropriée que s'il existe des moteurs de recherche efficaces.

Recommandations de modifications de la proposition

81. En ce qui concerne l'article 3, paragraphe 2:

— ajouter une disposition garantissant que personne en dehors des autorités compétentes n'ait accès aux données. Cette disposition pourrait être formulée comme suit: «l'accès aux données et leur traitement ne sont autorisés que pour la finalité visée à l'article 3, paragraphe 2» ou «les fournisseurs garantissent de façon effective que l'accès est uniquement accordé aux autorités compétentes»,

— préciser que des données ne peuvent être transmises que si cela s'avère nécessaire en considération d'une infraction pénale particulière,

— limiter la disposition en question à *certaines* infractions pénales graves,

— ajouter à la proposition un ou plusieurs articles concernant l'accès des autorités compétentes aux données relatives au trafic et aux données de localisation et à l'utilisation ultérieure de ces données, et introduire une disposition prévoyant que, dans certains cas précis, l'accès devrait être soumis à un contrôle juridictionnel dans les États membres,

— inclure une partie sur la protection des données.

82. En ce qui concerne les articles 4 et 5:

— ajouter au second alinéa de l'article 4 la phrase suivante: «l'annexe ne peut inclure des données indiquant le contenu d'une communication»,

— préciser qu'il serait préférable que les révisions de l'annexe ayant une incidence significative sur la protection des données soient opérées par voie de directive, selon la procédure de codécision.

83. En ce qui concerne l'article 7, il conviendrait de préciser dans le texte que:

— les durées de conservation de six mois et un an respectivement sont des durées maximales,

— les données sont effacées au terme du délai de conservation. Le texte devrait en outre préciser par quel moyen l'effacement devrait être effectué, à savoir par le fournisseur, par des procédés automatisés, et au moins quotidiennement.

84. En ce qui concerne l'article 8, il conviendrait de préciser dans le texte que:

— les données demandées sont transmises par les fournisseurs aux autorités,

— les fournisseurs doivent installer l'architecture technique nécessaire, y compris les moteurs de recherche, pour faciliter l'accès ciblé aux données indiquées,

— les fournisseurs doivent veiller à ce que seuls ceux de leurs employés qui exercent des responsabilités techniques précises aient accès aux bases de données pour des raisons techniques et à ce que ces employés soient conscients du caractère sensible des données et soumis, dans l'exercice de leurs fonctions, à de strictes règles internes de confidentialité,

— la transmission des données ne doit pas seulement avoir lieu sans délai, mais également sans que soient révélées des données relatives au trafic ou des données de localisation autres que celles qui sont nécessaires aux fins de la demande.

85. En ce qui concerne l'article 9:

— ajouter une disposition obligeant le fournisseur à tenir des fichiers journaux et à procéder à des audits (internes) systématiques, afin de permettre aux autorités nationales chargées de la protection des données de contrôler en pratique l'application des règles relatives à la protection des données.

86. En ce qui concerne l'article 10:

— expliciter dans le libellé de cette disposition le lien entre le caractère approprié des mesures de sécurité et leur coût,

— prévoir, pour les mesures de sécurité que les fournisseurs doivent prendre, des normes minimales conditionnant leur remboursement par un État membre,

— préciser dans l'exposé des motifs les conséquences financières de la proposition.

87. En ce qui concerne l'article 11:

— modifier l'article 15, paragraphe 1, de la directive 2002/58/CE en supprimant les références aux articles 6 et 9 (de la même directive), ou du moins en modifiant, afin de bien montrer que les États membres ne sont plus compétents pour adopter des textes législatifs ayant trait à des infractions pénales, en complément de ce qui est prévu par la présente proposition.

88. En ce qui concerne l'article 12, modifier les dispositions relatives à l'évaluation:

— l'évaluation devrait comprendre une analyse de l'efficacité de la mise en œuvre de la directive,

— elle devrait avoir lieu à intervalles réguliers (au moins tous les deux ans),

— la Commission devrait être tenue, le cas échéant, de soumettre des propositions de modification de la proposition (comme le prévoit l'article 18 de la directive 2002/58/CE).

Fait à Bruxelles, le 26 septembre 2005.

Peter HUSTINX

Contrôleur européen de la protection des données