

## I

*(Résolutions, recommandations et avis)*

## AVIS

## CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

### **Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données**

(2007/C 255/01)

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 <sup>(1)</sup>,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 <sup>(2)</sup>, et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

#### I. INTRODUCTION

1. La communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données <sup>(3)</sup> a été transmise au CEPD le 7 mars 2007. Celui-ci présente le présent avis conformément à l'article 41 du règlement (CE) n° 45/2001.

2. La communication rappelle l'importance de la directive 95/46/CE <sup>(4)</sup>, qui constitue une étape importante dans la protection des données à caractère personnel, et examine la directive et sa mise en œuvre en trois chapitres: le passé, la situation actuelle et l'avenir. Sa conclusion principale est qu'il n'y a pas lieu de modifier la directive, dont la mise en œuvre devrait encore être améliorée au moyen d'autres instruments, pour la plupart non contraignants.

3. Le présent avis du CEPD suit la structure de la communication. Plus important, le CEPD souscrit à la conclusion principale de la Commission selon laquelle la directive ne devrait pas être modifiée.

4. Néanmoins, le CEPD adopte cette position également pour des raisons pratiques. Les points de départ de son raisonnement sont les suivants:

— à court terme, il est plus opportun de se concentrer sur la mise en œuvre de la directive qui, comme la communication le montre, peut encore être améliorée considérablement,

— à plus long terme, des modifications de la directive semblent inévitables mais les principes essentiels demeureraient,

— il conviendrait de fixer dès à présent une date précise pour l'examen de la directive en vue de l'élaboration des propositions destinées à apporter les modifications susmentionnées, ce qui inciterait certainement à entamer dès aujourd'hui la réflexion sur les changements futurs.

<sup>(1)</sup> JOL 281 du 23.11.1995, p. 31.<sup>(2)</sup> JOL 8 du 12.1.2001, p. 1.<sup>(3)</sup> Ci-après dénommée «la communication».<sup>(4)</sup> Ci-après dénommée «la directive».

5. Ces éléments sont essentiels, car il ne faut pas perdre de vue que la directive s'inscrit dans un contexte dynamique. Premièrement, l'Union européenne évolue: la libre circulation d'informations entre les États membres — et entre les États membres et les pays tiers — a gagné en importance et deviendra une réalité encore plus cruciale. Deuxièmement, la société aussi évolue. La société de l'information se développe et s'apparente de plus en plus à une société de la surveillance<sup>(5)</sup>, rendant d'autant plus nécessaire une protection efficace des données à caractère personnel afin de tenir compte de ce nouveau contexte de manière tout à fait satisfaisante.

## II. PERSPECTIVES DE L'AVIS

6. Dans le cadre de l'examen de la communication, le CEPD se penchera notamment sur les aspects décrits ci-après qui présentent un intérêt au regard des évolutions évoquées plus haut:

- amélioration de la mise en œuvre de la directive proprement dite: comment rendre la protection des données plus efficace? Pour parvenir à cette amélioration, il faudra recourir à diverses mesures, allant d'une meilleure communication avec la société à une application plus stricte de la législation relative à la protection des données,
- interaction avec la technologie: les nouvelles évolutions technologiques, notamment dans les domaines de l'échange des données, des systèmes d'identification par radiofréquence (RFID), de la biométrie et des systèmes de gestion des identités, ont des répercussions évidentes sur les exigences liées à un cadre juridique efficace régissant la protection des données. La nécessité de prévoir une protection effective des données à caractère personnel d'une personne peut également entraîner l'imposition de limitations par rapport à l'utilisation de ces nouvelles technologies. L'interaction peut donc se résumer comme suit: la technologie influe sur la législation, qui à son tour a une incidence sur la technologie,
- respect de la vie privée à l'échelle mondiale et questions de compétence en rapport avec les frontières extérieures de l'Union européenne. Alors que la compétence du législateur communautaire se limite au territoire de l'Union européenne, la notion de frontières extérieures perd de sa pertinence en ce qui concerne les échanges de données. L'économie dépend de plus en plus des réseaux mondiaux et les sociétés établies dans l'Union européenne transfèrent de plus en plus leurs activités vers des pays tiers, y compris le traitement des données à caractère personnel. Par ailleurs, des affaires récentes, notamment celles relatives à SWIFT et aux données PNR, confirment le fait que d'autres juridictions montrent un intérêt pour des «données provenant de l'UE». D'une manière générale, le lieu physique d'une opération de traitement est désormais moins pertinent,
- protection des données et application de la législation: les menaces récentes, qu'elles soient ou non liées au terrorisme, auxquelles la société est exposée ont accru la possibilité (ou les demandes de pouvoir disposer d'une

telle possibilité), pour les services répressifs, de collecter, stocker et échanger des données à caractère personnel. Parfois, le secteur privé joue un rôle actif, comme en attestent des exemples récents. D'une part, la ligne de démarcation avec le troisième pilier du traité UE (dans lequel la directive ne s'applique pas) revêt une plus grande importance, d'autre part, elle devient plus floue. Dans certains cas, le risque existe même que des données à caractère personnel ne soient protégées ni par des instruments relevant du premier pilier ni par des instruments relevant du troisième pilier (le «vide juridique»),

- les conséquences, en tout état de cause pour la protection des données et l'application de la législation, de l'entrée en vigueur du traité modificatif, désormais prévue pour 2009.

## III. LE PASSÉ ET LA SITUATION ACTUELLE

7. Le premier rapport sur la mise en œuvre de la directive relative à la protection des données, publié le 15 mai 2003, contenait un programme de travail pour une meilleure mise en application de la directive sur la protection des données, lui-même assorti d'une liste de dix actions à mener en 2003 et 2004. La communication décrit la manière dont chacune de ces actions a été réalisée.
8. Sur la base de l'analyse des travaux menés dans le cadre du programme de travail précité, la communication dresse une évaluation positive des améliorations réalisées dans la mise en œuvre de la directive. L'évaluation de la Commission, telle qu'elle est résumée dans les titres du chapitre 2 («Situation actuelle») de la communication, dit en substance ceci: la mise en application s'est améliorée, même si certains États membres n'ont pas encore procédé à une mise en œuvre correcte; certaines disparités subsistent encore, mais elles s'expliquent pour la plupart par la marge d'appréciation laissée par la directive et, en tout état de cause, elles ne constituent pas un réel problème pour le marché intérieur. Les solutions juridiques énoncées dans la directive se sont pour l'essentiel avérées appropriées pour garantir le droit fondamental à la protection des données, tout en répondant aux évolutions technologiques et aux exigences imposées par la sauvegarde des intérêts publics.
9. Le CEPD souscrit aux grandes lignes de cette évaluation positive. Plus précisément, il reconnaît le travail considérable qui a été accompli dans le domaine des flux transfrontières de données: le constat d'une protection adéquate en ce qui concerne les pays tiers, les nouvelles clauses contractuelles types, l'adoption de règles d'entreprise contraignantes, la réflexion menée sur une interprétation plus uniforme de l'article 26, paragraphe 1, de la directive et l'amélioration constatée dans les notifications faites au titre de l'article 26, paragraphe 2, sont autant d'éléments qui contribuent à faciliter les transferts internationaux de données à caractère personnel. Toutefois, il ressort de la jurisprudence de la Cour de justice<sup>(6)</sup> qu'il reste encore du travail à accomplir dans ce domaine de la plus haute importance, afin de répondre aux évolutions tant dans le domaine technologique qu'en matière répressive.

<sup>(5)</sup> Notamment l'arrêt de la Cour dans l'affaire Lindqvist (voir note de bas de page 15) et dans celle relative aux données PNR (voir note de bas de page 17).

<sup>(6)</sup> Voir le point 37 du présent avis.

10. La communication indique également que le respect de la directive et la sensibilisation à cet égard sont des éléments essentiels pour favoriser une meilleure mise en œuvre et que ces aspects pourraient être davantage exploités. Par ailleurs, l'échange des meilleures pratiques et l'harmonisation en matière de notifications et d'information constituent des précédents concluants en termes de réduction des formalités administratives et des coûts pour les entreprises.
11. En outre, l'analyse de la situation passée confirme qu'il est impossible de réaliser des améliorations sans y associer un large éventail de parties intéressées. La Commission, les autorités responsables de la protection des données et les États membres sont certes des acteurs incontournables dans la plupart des actions menées. Néanmoins, le rôle du secteur privé est de plus en plus important, notamment en ce qui concerne la promotion de l'autorégulation et des codes de conduite européens ou le développement des technologies renforçant la protection de la vie privée.

#### IV. L'AVENIR

##### A. La conclusion: ne pas modifier la directive maintenant

12. Plusieurs raisons étayent la conclusion de la Commission, à savoir que, dans les circonstances actuelles et à court terme, il n'y a pas lieu d'envisager de présenter une proposition visant à modifier la directive.
13. Fondamentalement, la Commission invoque deux raisons à l'appui de cette conclusion. Premièrement, le potentiel de la directive n'a pas été totalement exploité. Il est en effet encore possible d'améliorer sensiblement sa mise en œuvre dans les domaines de compétence des États membres. Deuxièmement, la Commission précise que, bien que la directive laisse une marge d'appréciation aux États membres, rien n'indique que les disparités constatées dans les limites de cette marge posent de réels problèmes pour le marché intérieur.
14. À la lumière de ces deux raisons, la Commission formule sa conclusion de la manière suivante: elle explique ce que la directive devrait faire, en veillant à inspirer confiance, pour ensuite indiquer que la directive constitue une référence, qu'elle est techniquement neutre et qu'elle continue à fournir des solutions concrètes et appropriées<sup>(7)</sup>.
15. Le CEPD accueille favorablement la manière dont cette conclusion est formulée mais il est d'avis qu'on pourrait encore la renforcer par deux aspects complémentaires:
- premièrement, la nature de la directive,
  - deuxièmement, la pratique législative de l'Union.

##### La nature de la directive

16. Le droit fondamental des personnes physiques à la protection de leurs données à caractère personnel est reconnu à l'article 8 de la Charte des droits fondamentaux de l'Union et énoncé, notamment, dans la convention n° 108 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. En substance, la directive constitue un cadre qui reprend les éléments principaux de la protection de ce droit fondamental en précisant et en amplifiant les droits et libertés figurant dans ladite convention<sup>(8)</sup>.

17. Un droit fondamental vise à protéger le citoyen en toutes circonstances dans une société démocratique. Il ne devrait pas être possible de modifier facilement les éléments principaux d'un droit de cette nature en fonction des évolutions de la société ou des préférences politiques des gouvernements en place. Ainsi, les suites de menaces que font peser les organisations terroristes sur la société peuvent être différentes dans certains cas si l'on considère que ces menaces pourraient justifier une plus grande ingérence dans un droit fondamental d'une personne, mais elles ne peuvent en aucun cas porter atteinte aux éléments essentiels du droit proprement dit, ni priver une personne de l'exercice de ce droit ou limiter celui-ci inconsiderément.
18. Un deuxième aspect de la directive consiste à envisager d'encourager la libre circulation des informations dans le marché intérieur. Cet objectif peut également être considéré comme fondamental dans un marché intérieur sans frontières et en constante évolution. L'harmonisation des dispositions essentielles des législations nationales est l'un des principaux moyens visant à assurer la mise en place et le fonctionnement de ce marché intérieur. Elle donne corps à la confiance mutuelle entre les États membres à l'égard de leurs systèmes juridiques nationaux respectifs. C'est donc aussi pour ces raisons que l'apport de modifications doit être dûment réfléchi. Celles-ci sont effet susceptibles d'affecter cette confiance mutuelle.
19. Un troisième élément caractérisant la directive est que celle-ci doit être considérée comme un cadre général sur lequel reposent des instruments juridiques particuliers. Il s'agit notamment des mesures visant à mettre en œuvre ce cadre général, ainsi que des cadres spécifiques concernant tel ou tel secteur. La directive sur la vie privée et les communications électroniques [2002/58/CE<sup>(9)</sup>] constitue un de ces cadres spécifiques. Dans la mesure du possible, les évolutions constatées dans la société devraient donner lieu à une modification des mesures de mise en œuvre ou des cadres juridiques spécifiques, pas du cadre général qui les régit.

##### La pratique législative de l'Union

20. Selon le CEPD, la conclusion selon laquelle il ne faut pas modifier la directive à l'heure actuelle est aussi la conséquence logique des principes généraux d'une bonne gestion et de la pratique suivie en matière législative. De nouvelles propositions législatives — qu'elles portent sur de nouveaux domaines de l'action communautaires ou modifient des textes existants — ne devraient être présentées que si leur caractère nécessaire et proportionné est suffisamment démontré, et aucune proposition ne devrait être présentée si le même résultat peut être atteint en recourant à d'autres instruments dont la portée est moins étendue.

<sup>(8)</sup> Considérant 11 de la directive.

<sup>(9)</sup> 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) (JO L 201 du 31.7.2002, p. 37).

21. En l'état actuel des choses, le caractère nécessaire et proportionné d'une modification de la directive n'est pas démontré. Le CEPD rappelle que la directive définit le cadre général régissant la protection des données conformément au droit communautaire. Elle doit garantir, d'une part, la protection des droits et libertés des personnes, notamment le droit à la protection de la vie privée, à l'égard du traitement des données à caractère personnel et, d'autre part, la libre circulation de ces données dans le marché intérieur.
22. Ce cadre général ne devrait pas être modifié avant qu'il n'ait été complètement mis en œuvre dans les États membres, à moins de disposer d'éléments indiquant clairement qu'il ne permettrait pas d'atteindre les objectifs de la directive. Le CEPD estime que la Commission a — compte tenu des circonstances actuelles — étayé de manière satisfaisante sa thèse selon laquelle le potentiel de la directive n'a pas été totalement exploité (voir le point III du présent avis). De même, rien ne permet d'affirmer que ses objectifs ne pourraient pas être atteints dans le cadre actuel.

#### B. À plus long terme, des modifications semblent inévitables

23. Dans le futur, il faudra également veiller à ce que les principes de la protection des données garantissent une protection effective aux personnes physiques, compte tenu du contexte dynamique dans lequel la directive s'inscrit (voir le point 5 du présent avis) et des perspectives évoquées au point 6: amélioration de la mise en œuvre, interaction avec la technologie, respect de la vie privée à l'échelle mondiale et questions de compétence, protection des données et respect de la législation et le traité modificatif. Cette nécessité d'une application intégrale des principes relatifs à la protection des données fixe la norme pour les modifications futures de la directive. Le CEPD rappelle à nouveau que, à plus long terme, des modifications apparaissent inévitables.
24. Pour ce qui est de la teneur des mesures susceptibles d'être adoptées à l'avenir, le CEPD fournit déjà à ce stade quelques éléments qu'il juge indispensables dans tout système futur de protection des données au sein de l'Union européenne, à savoir:
- il n'est pas nécessaire d'élaborer de nouveaux principes; en revanche, il faut de toute évidence prévoir d'autres arrangements administratifs qui, d'une part, soient efficaces et adaptés à une société fonctionnant en réseau et, d'autre part, permettent de réduire au maximum les coûts administratifs,
  - le champ d'application étendu de la législation relative à la protection des données ne devrait pas être modifié. Il devrait s'appliquer à toutes les utilisations des données à caractère personnel et ne pas être limité aux données sensibles ni, de quelque autre manière, à des intérêts particuliers ou à des risques spécifiques. En d'autres termes, le CEPD rejette une approche «de minimis» en ce qui concerne le champ d'application de la protection des données. Cela garantit que les personnes concernées pourront exercer leurs droits quelle que soit la situation,
  - la législation relative à la protection des données devrait continuer à couvrir un large éventail de situations, tout en permettant d'adopter une approche équilibrée dans des cas concrets, compte tenu d'autres intérêts (publics ou privés) justifiés ainsi que de la nécessité de limiter au minimum les conséquences d'un point de vue bureaucratique. Les autorités chargées de la protection des données devraient également avoir la possibilité de définir des priorités et de mettre l'accent sur des domaines ou des questions revêtant une importance particulière ou présentant des risques spécifiques,
  - le système devrait s'appliquer intégralement à l'utilisation des données à caractère personnel à des fins répressives, tout en sachant que des mesures complémentaires appropriées peuvent s'avérer nécessaires pour répondre à des problèmes particuliers dans ce domaine,
  - il conviendrait de prévoir des arrangements appropriés en ce qui concerne les échanges de données avec les pays tiers en s'inspirant, dans la mesure du possible, des normes mondiales applicables à la protection des données.
25. La communication mentionne — en relation avec les défis posés par les nouvelles technologies — l'examen en cours de la directive 2002/58/CE et la nécessité éventuelle d'adopter des règles plus spécifiques permettant d'apporter une solution aux problèmes de protection des données suscités par les nouvelles technologies comme Internet ou la RFID<sup>(10)</sup>. Le CEPD se réjouit de cet examen et des mesures envisagées, bien qu'il estime que celles-ci ne devraient pas seulement concerner les progrès technologiques, mais prendre aussi en considération le contexte dynamique dans sa globalité et, dans une perspective à long terme, englober également la directive 95/46/CE. Par ailleurs, une action plus ciblée s'impose à cet égard. Malheureusement, la communication manque de précision:
- aucun calendrier n'est défini pour la réalisation des différentes actions mentionnées au chapitre 3 de la communication,
  - le délai pour la présentation ultérieure d'un rapport sur l'application de la directive n'est pas précisé. L'article 33 de la directive demande à la Commission de faire rapport «périodiquement» sans non plus préciser cette périodicité,
  - il n'existe pas de mandat: la communication ne permet pas de mesurer le degré de réalisation des actions prévues. Le texte fait simplement référence au programme de travail présenté en 2003,
  - aucune indication n'est fournie quant à la manière de procéder à plus long terme.
- Le CEPD suggère que la Commission précise ces différents éléments.

<sup>(10)</sup> Page 11 de la communication.

## V. PERSPECTIVES QUANT AUX MODIFICATIONS FUTURES

### A. Une mise en œuvre complète

26. Toute modification future doit être précédée d'une mise en œuvre intégrale des dispositions actuelles de la directive. Une mise en œuvre complète signifie d'abord que les prescriptions légales énoncées dans la directive doivent être respectées. La communication indique <sup>(11)</sup> que certains États membres n'ont pas incorporé dans leur législation un certain nombre de dispositions importantes de la directive et mentionne à cet égard, notamment, les dispositions relatives à l'indépendance des autorités de contrôle. Il incombe à la Commission de contrôler le respect de ces dispositions et, lorsqu'elle le juge approprié, de faire usage des pouvoirs qui lui sont conférés en vertu de l'article 226 du traité CE.

27. La communication envisage une communication interprétative pour certaines dispositions, notamment celles qui peuvent éventuellement donner lieu à des procédures formelles d'infraction au titre de l'article 226 du traité CE.

28. Par ailleurs, la directive prévoit d'autres mécanismes qui visent à améliorer la mise en œuvre. Plus précisément, les missions du Groupe de l'article 29, énumérées à l'article 30 de la directive, ont été définies à cette fin: elles ont pour objectif de renforcer la mise en œuvre dans les États membres afin de parvenir à un niveau élevé et harmonisé de protection des données, au-delà de ce qui est strictement nécessaire pour respecter les obligations imposées par la directive. Dans l'exercice de ce rôle, ce groupe a élaboré au fil des années un grand nombre d'avis et d'autres documents.

29. Selon le CEPD, une mise en œuvre complète de la directive comprend les deux éléments suivants:

— il convient de veiller à ce que les États membres respectent intégralement les obligations qui leur incombent en vertu du droit européen. Cela signifie que les dispositions de la directive devraient être transposées dans les législations nationales, mais aussi, dans la pratique, que les objectifs définis par la directive soient atteints,

— il conviendrait de recourir pleinement à d'autres instruments, non contraignants, susceptibles de contribuer à un degré élevé et harmonisé de protection des données.

Le CEPD souligne qu'il convient de faire une distinction nette entre ces deux éléments, compte tenu des conséquences différentes sur le plan juridique et des compétences qui y sont liées. Concrètement, la Commission devrait être pleinement compétente pour le premier élément, tandis que le groupe susmentionné devrait être l'acteur principal en ce qui concerne le deuxième aspect.

30. Une autre distinction, plus précise, qu'il convient également de faire a trait aux instruments disponibles pour parvenir à une meilleure mise en œuvre de la directive. Citons notamment:

— les mesures d'exécution. Ces mesures — adoptées par la Commission dans le cadre de la procédure de comité — sont prévues au chapitre IV de la directive relatif au

transfert de données à caractère personnel vers des pays tiers (voir l'article 25, paragraphe 6, et l'article 26, paragraphe 3),

— une législation sectorielle,

— les procédures d'infraction en vertu de l'article 226 du traité CE,

— les communications interprétatives. Ce type de communication pourrait se concentrer sur les dispositions susceptibles de donner à lieu à des procédures d'infraction ou servir principalement de texte de référence pour la protection des données dans la pratique (voir également les points 57 à 62) <sup>(12)</sup>,

— autres communications. Citons, par exemple, la communication de la Commission au Parlement et au Conseil relative aux technologies renforçant la protection de la vie privée,

— encouragement des meilleures pratiques. Cet instrument peut être utilisé dans divers domaines, notamment la simplification administrative, les audits, le contrôle de l'application et les sanctions, etc. (voir également les points 63 à 67).

31. Le CEPD suggère à la Commission d'indiquer clairement comment elle utilisera ces différents outils lorsqu'elle élaborera ses mesures sur la base de la communication à l'examen. À cet égard, elle devrait également établir une distinction nette entre ce qui relève de ses propres compétences et ce qui relève des compétences du groupe. En dehors de cela, il va sans dire qu'une bonne coopération entre la Commission et le groupe est, en toutes circonstances, une condition pour réussir.

### B. Interaction avec la technologie

32. À la base, les dispositions de la directive sont formulées de manière techniquement neutre. La communication établit un lien entre l'accent mis sur cette neutralité technologique et un certain nombre d'évolutions dans ce domaine, notamment l'Internet, l'accès à des services fournis dans des pays tiers, la RFID et l'association à la reconnaissance automatique de données constituées par des sons ou des images. Elle fait une distinction entre deux types de mesures: d'une part, la fourniture d'orientations plus précises quant à l'application des principes relatifs à la protection des données dans un environnement technologique en évolution, le groupe et sa Task Force Internet <sup>(13)</sup> jouant à cet égard un rôle important, d'autre part, une législation sectorielle qui pourrait être proposée par la Commission elle-même.

33. Le CEPD accueille favorablement cette approche, qui constitue une première étape importante. Cependant, à plus long terme, d'autres mesures, plus fondamentales, pourraient s'avérer nécessaires. La communication à l'examen pourrait servir de point de départ à une telle approche envisagée à long terme, pour laquelle le CEPD suggère de lancer la discussion, en guise de suite à donner à la communication. Les points évoqués ci-après peuvent éventuellement faire partie de cette approche.

<sup>(12)</sup> Voir, par exemple, l'avis n° 4/2007 du groupe sur le concept de données à caractère personnel (référence WP 136), adopté le 20 juin 2007.

<sup>(13)</sup> La Task Force Internet est un sous-groupe du Groupe de l'article 29.

<sup>(11)</sup> Page 6 de la communication, troisième paragraphe.

34. Premièrement, l'interaction avec les technologies est la suivante: d'une part, les nouvelles technologies qui se développent peuvent nécessiter de modifier le cadre légal régissant la protection des données; d'autre part, la nécessité de protéger de manière effective les données à caractère personnel des personnes peut exiger d'imposer de nouvelles limitations ou de définir des garanties appropriées quant à l'utilisation de certaines technologies, ce qui constitue une conséquence bien plus étendue. Toutefois, on pourrait également s'appuyer sur les nouvelles technologies et y avoir recours de manière efficace afin de renforcer la protection de la vie privée.
35. Deuxièmement, certaines limitations particulières pourraient s'avérer nécessaires si les nouvelles technologies sont utilisées par les instances gouvernementales dans l'exercice de leurs fonctions publiques. Les discussions sur l'interopérabilité et l'accès aux données qui ont actuellement lieu dans le domaine de la liberté, de la sécurité et de la justice, en relation avec la mise en œuvre du programme de La Haye, l'illustrent bien <sup>(14)</sup>.
36. Troisièmement, l'utilisation de matériel biométrique tel que le matériel ADN (mais ce n'est qu'un exemple) est de plus en plus répandue. Les questions particulières que soulève l'utilisation des données à caractère personnel extraites de ce type de matériel pourraient avoir des conséquences pour la législation relative à la protection des données.
37. Quatrièmement, force est de constater que la société elle-même évolue et qu'elle s'apparente de plus en plus à une société de la surveillance <sup>(15)</sup>. Cette évolution doit faire l'objet d'un débat de fond, dans le cadre duquel pourraient être abordées des questions essentielles consistant à savoir si cette évolution est inévitable, si le législateur européen doit intervenir dans cette évolution en vue de la limiter, si et comment il pourrait arrêter des mesures efficaces, etc.
39. Le CEPD regrette qu'une place plus importante n'ait pas été accordée à cet aspect dans la communication.
40. Actuellement, le chapitre IV de la directive (articles 25 et 26) prévoit un régime particulier applicable aux transferts de données vers des pays tiers, qui s'ajoute aux règles générales relatives à la protection des données. Ce régime s'est constitué au fil des ans, l'objectif étant de trouver un juste équilibre entre la protection des personnes dont les données doivent être transférées vers des pays tiers et, entre autres, les impératifs liés au commerce international et à la réalité des réseaux mondiaux de télécommunications. La Commission et le groupe <sup>(16)</sup>, mais aussi, par exemple, la Chambre de commerce internationale, ont consenti beaucoup d'efforts pour que ce système fonctionne, par l'adoption de décisions en matière d'adéquation, de clauses contractuelles types, de règles d'entreprise contraignantes, etc.
41. L'arrêt rendu par la Cour de justice dans l'affaire *Lindqvist* <sup>(17)</sup> revêt une importance particulière pour l'applicabilité de ce système à Internet. La Cour, après avoir souligné le caractère ubiquitaire des informations qui se trouvent sur Internet, a jugé que l'inscription de données sur une page Internet, même si celles-ci sont ainsi rendues accessibles aux personnes de pays tiers possédant les moyens techniques d'y accéder, ne saurait en soi être considérée comme un transfert vers un pays tiers.
42. Ce système, qui est une conséquence logique et nécessaire des limitations territoriales de l'Union européenne, ne peut offrir une protection complète au citoyen européen dans une société fonctionnant en réseau, où les frontières physiques perdent de leur importance (voir les exemples mentionnés au point 6 du présent avis): si les informations qui se trouvent sur Internet ont un caractère ubiquitaire, ce n'est pas le cas de la compétence du législateur européen.
43. Le défi consistera à trouver des solutions pratiques qui concilient la nécessité de protéger les citoyens européens concernés et les limitations territoriales de l'Union européenne et de ses États membres. Le CEPD — dans ses observations sur la communication de la Commission intitulée «Une stratégie relative à la dimension externe de l'espace de liberté, de sécurité et de justice» — a déjà encouragé la Commission à jouer un rôle moteur afin de renforcer la protection des données à caractère personnel au niveau international en soutenant les approches bilatérales et multilatérales avec les pays tiers ainsi que la coopération avec d'autres organisations internationales <sup>(18)</sup>.

### C. Respect de la vie privée à l'échelle mondiale et compétences

38. Les notions de respect de la vie privée à l'échelle mondiale et de compétence occupent une place limitée dans la communication. La seule intention évoquée à cet égard est que la Commission continuera à exercer son contrôle et à contribuer aux débats dans les enceintes internationales, afin de veiller à la cohérence des engagements pris par les États membres avec les obligations que leur impose la directive. En dehors de cela, la communication énumère un certain nombre d'actions réalisées en vue de simplifier les obligations en matière de transferts internationaux (voir le point III du présent avis).

<sup>(14)</sup> Voir, par exemple, les observations du CEPD en date du 10 mars 2006 relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes (publiées sur le site web du CEPD).

<sup>(15)</sup> Voir le rapport intitulé «Report on the Surveillance Society» (rapport sur la société de la surveillance), élaboré par le *Surveillance Studies Network* à l'intention du Commissaire du Royaume-Uni à l'information et présenté lors de la 28<sup>ème</sup> Conférence internationale des Commissaires à la protection des données et à la vie privée qui a eu lieu à Londres les 2 et 3 novembre 2006 [voir le site: [www.privacyconference2006.co.uk](http://www.privacyconference2006.co.uk) (rubrique «Documents»)].

<sup>(16)</sup> Voir, par exemple, le document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005 (WP 114); le document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les «règles d'entreprise contraignantes», adopté le 14 avril 2005 (WP 107), et l'avis 8/2003 relatif au projet de clauses contractuelles types présenté par un groupe d'associations professionnelles («le contrat type alternatif»), adopté le 17 décembre 2003 (WP 84).

<sup>(17)</sup> Arrêt de la Cour du 6 novembre 2003 dans l'affaire C-101/01, Recueil 2003, p. I-12971, points 56 à 71.

<sup>(18)</sup> Voir la lettre adressée en date du 28 novembre 2005 au directeur général de la direction générale «Justice, liberté et sécurité» de la Commission européenne concernant la communication intitulée «Une stratégie relative à la dimension externe de l'espace de liberté, de sécurité et de justice» (*Letter to the Director General of the European Commission's Justice, Freedom and Security department on the Communication on «A Strategy on the External Dimension of the Area of Freedom, Security and Justice»*) (disponible sur le site web du CEPD).

44. Ces solutions pratiques sont notamment les suivantes:

- perfectionnement du cadre mondial pour la protection des données. Des normes plus généralement reconnues, telles que les lignes directrices de l'OCDE relatives à la protection des données (1980) et les lignes directrices de l'ONU, pourraient servir de base,
- perfectionnement du régime particulier applicable aux transferts de données vers des pays tiers, prévu au chapitre IV de la directive (articles 25 et 26),
- conclusion d'accords internationaux en matière de compétence ou d'accords similaires avec les pays tiers,
- élaboration de mécanismes visant à assurer le respect des normes à l'échelle mondiale, notamment le recours à des règles d'entreprise contraignantes par les sociétés multinationales, quel que soit le lieu où elles traitent des données à caractère personnel.

45. Aucune de ces solutions n'est nouvelle. Néanmoins, il est nécessaire de se représenter clairement comment utiliser ces méthodes le plus efficacement possible et comment faire en sorte que les normes relatives à la protection des données — celles qualifiées de droits fondamentaux dans l'Union européenne — soient également effectives dans une société fonctionnant en réseau à l'échelle mondiale. Le CEPD invite la Commission à commencer à réfléchir à ce projet mobilisateur, avec le plus grand nombre de parties prenantes intéressées.

#### D. Respect de la législation

46. La communication accorde une attention toute particulière aux exigences imposées par les intérêts publics, notamment en matière de sécurité. Elle explique l'article 3, paragraphe 2, de la directive et l'interprétation qu'en donne la Cour de justice dans son arrêt PNR <sup>(19)</sup>, ainsi que l'article 13, notamment en liaison avec la jurisprudence de la Cour européenne des droits de l'homme. La communication souligne par ailleurs que, lorsque la Commission concilie des mesures visant à assurer la sécurité et des droits fondamentaux non négociables, elle veille à ce que les données à caractère personnel soient protégées comme cela est garanti par l'article 8 de la convention européenne des droits de l'homme. Ce principe s'applique aussi au dialogue transatlantique avec les États-Unis d'Amérique.

47. Le CEPD estime qu'il est important que la Commission rappelle avec autant de clarté l'obligation qui incombe à l'Union, conformément à l'article 6 du traité UE, de respecter les droits fondamentaux tels qu'ils sont garantis par la convention européenne des Droits de l'Homme. Ce rappel est d'autant plus important que le Conseil européen a désormais décidé que, en vertu du *traité modificatif*, la Charte des droits fondamentaux de l'Union européenne

devrait être juridiquement contraignante. L'article 8 de ladite charte définit le droit de toute personne à la protection des données à caractère personnel la concernant.

48. Chacun sait que les demandes formulées par les services répressifs en vue de pouvoir utiliser plus largement les données à caractère personnel aux fins de la lutte contre la criminalité — sans parler de la lutte contre le terrorisme — risquent de réduire le niveau de protection offert au citoyen, même en deçà du niveau garanti par l'article 8 de la convention européenne des droits de l'homme et la convention n° 108 du Conseil de l'Europe <sup>(20)</sup>. Ces préoccupations constituent un point principal du troisième avis du CEPD, publié le 27 avril 2007, 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.

49. Dans ce contexte, il est essentiel de prendre pour base, aux fins de la protection du citoyen, la norme définie par la directive, également en relation avec les demandes exprimées par les services répressifs. La convention européenne des droits de l'homme et la convention n° 108 prévoient un niveau minimum de protection, mais n'offrent pas la précision nécessaire. De surcroît, il a fallu adopter des mesures complémentaires pour garantir une protection appropriée du citoyen. Cette nécessité a été l'un des principaux facteurs qui ont conduit à l'adoption de la directive en 1995 <sup>(21)</sup>.

50. De même, il importe de garantir de manière effective ce niveau de protection dans toutes les situations où des données à caractère personnel sont traitées à des fins répressives. Bien que la communication ne porte pas sur le traitement des données dans le troisième pilier, c'est fort à propos qu'elle aborde le cas où des données collectées (et traitées) à des fins commerciales sont utilisées dans un but répressif, une situation qui tend à se généraliser étant donné que les services de police font de plus en plus souvent appel aux informations détenues par des tiers. La directive 2006/24/CE <sup>(22)</sup> est la meilleure illustration de cette tendance: cette directive fait obligation aux fournisseurs de communications électroniques de conserver (pendant une plus longue période) les données qu'ils ont collectées (et stockées) à des fins commerciales, pour les besoins des services répressifs. Selon le CEPD, il convient de veiller pleinement à ce que les données à caractère personnel collectées et traitées dans le cadre du champ d'application de la directive soient dûment protégées lorsqu'elles sont utilisées à des fins liées à l'intérêt public, et notamment aux fins de sécurité ou de lutte contre le terrorisme. Dans certains cas cependant, ces finalités peuvent aller au-delà du champ d'application de la directive.

<sup>(19)</sup> Arrêt de la Cour du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04, *Parlement européen/Conseil et Commission*, Recueil 2006, p. I-4721.

<sup>(20)</sup> 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.

<sup>(21)</sup> Le CEPD a fait état du manque de précision de la convention n° 108 dans un certain nombre d'avis en relation avec la nécessité d'adopter une décision-cadre du Conseil.

<sup>(22)</sup> 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).

51. Les observations qui précèdent conduisent le CEPD à faire les suggestions suivantes à la Commission:

- il faut poursuivre la réflexion sur les implications, pour la protection des données, de la participation de sociétés privées aux activités des services répressifs, afin de veiller à ce que les principes de la directive 95/46/CE s'appliquent pleinement aux situations évoquées ci-dessus et qu'aucune lacune n'affecte le droit fondamental du citoyen à la protection des données. En particulier, il convient de veiller à ce que les données à caractère personnel collectées dans le cadre du champ d'application de la directive soient protégées de manière appropriée et systématique, également lorsqu'elles sont traitées ultérieurement pour la sauvegarde d'intérêts publics, que ce soit dans les limites du champ d'application de la directive ou au-delà,
- en tout état de cause, cette réflexion devrait inclure les lacunes du cadre juridique actuel, à savoir les cas où la limite entre le premier et le troisième piliers n'est pas clairement établie ou même les situations susceptibles de se présenter où il n'existe aucune base appropriée pour adopter un instrument juridique relatif à la protection des données <sup>(23)</sup>,
- l'article 13 de la directive, qui permet de prévoir des exceptions et limitations aux principes régissant la protection des données, lorsque cela est nécessaire notamment pour la sauvegarde d'intérêts publics, devrait être interprété de manière à maintenir son effet utile en tant qu'interface et garantie essentielles pour les données à caractère personnel collectées dans le cadre du champ d'application de la directive, conformément à l'arrêt rendu par la Cour de justice dans l'affaire *Österreichischer Rundfunk* <sup>(24)</sup> et à la jurisprudence de la Cour européenne des droits de l'homme,
- il convient d'examiner la possibilité de proposer des textes législatifs visant à harmoniser les conditions et garanties applicables aux exceptions prévues à l'article 13.

#### E. La situation éventuelle dans le cadre du traité modificatif

52. Dans sa communication, la Commission aborde l'impact — considérable — du traité constitutionnel dans le domaine de la protection des données. De fait, le traité — désormais le traité modificatif — aura une importance capitale à cet égard: il marquera la fin de la structure en piliers, la disposition relative à la protection des données (actuellement l'article 286 du traité CE) sera précisée et la Charte des droits fondamentaux de l'Union, qui comprend à son article 8 une disposition relative à la protection des données, deviendra un instrument contraignant.
53. Le mandat de la Conférence intergouvernementale (CIG) attache une attention particulière à la protection des données. En substance, le point 19 f) dit trois choses: premièrement, les règles générales relatives à la protection des données seront sans préjudice des règles particulières adoptées dans le cadre du titre relatif à la PESC (l'actuel

deuxième pilier); deuxièmement, une déclaration sur la protection des données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale (l'actuel troisième pilier) sera adoptée et, troisièmement, des mentions spécifiques sur la position de certains États membres seront adoptées dans les protocoles pertinents (ce point concerne principalement la position particulière du Royaume-Uni concernant la coopération policière et judiciaire en matière pénale).

54. Le deuxième aspect (la déclaration) devra faire l'objet d'une clarification au sein de la CIG. Les conséquences de la fin de la structure en piliers et l'applicabilité éventuelle de la directive à la coopération policière et judiciaire en matière pénale doivent être dûment examinées, de manière à assurer l'application la plus large possible des principes relatifs à la protection des données énoncés dans la directive. Il n'est pas opportun de s'attarder ici sur la question. Le CEPD a présenté des suggestions concernant la déclaration en question dans une lettre adressée à la présidence de la CIG <sup>(25)</sup>.

## VI. INSTRUMENTS POUR UNE MEILLEURE MISE EN ŒUVRE

### A. Observations générales

55. La communication fait référence à une série d'instruments et d'actions susceptibles de contribuer à une meilleure mise en œuvre de la directive à l'avenir. Le CEPD souhaite formuler des observations à cet égard, tout en envisageant également d'autres mesures complémentaires qui ne sont pas mentionnées dans la communication.

### B. Législation sectorielle

56. Dans certains cas, l'adoption de mesures législatives spécifiques au niveau de l'UE peut s'avérer nécessaire. Plus précisément, une législation sectorielle peut être utile pour adapter les principes de la directive aux questions soulevées par certaines technologies, comme cela a été le cas pour les directives relatives à la protection de la vie privée dans le secteur des télécommunications. Il convient d'examiner avec soin le recours à une législation spécifique dans des domaines tels que l'utilisation des technologies RFID.

### C. Procédure d'infraction

57. L'instrument le plus puissant mentionné dans la communication est la procédure d'infraction. Le texte met en évidence un domaine de préoccupation en particulier, à savoir l'indépendance des autorités nationales chargées de la protection des données et leurs pouvoirs, mais n'évoque qu'en termes généraux d'autres domaines. Le CEPD convient que la procédure d'infraction est un instrument essentiel et inévitable si un État membre n'assure pas une mise en œuvre complète de la directive, notamment compte tenu du fait qu'il s'est presque écoulé neuf ans depuis l'expiration du délai imparti à cette fin et que le dialogue structuré prévu dans le programme de travail a déjà eu lieu. Toutefois, à ce jour, la Cour de justice n'a encore été saisie d'aucune affaire d'infraction concernant la directive 95/46.

<sup>(23)</sup> Il s'agit de la question du «vide juridique», sur laquelle le CEPD s'est penché à plusieurs reprises, principalement en relation avec l'arrêt PNR (voir, par exemple, le rapport annuel 2006, p. 47).

<sup>(24)</sup> Arrêt de la Cour du 20 mai 2003 dans les affaires jointes C-465/00, C-138/01 et C-139/01, Recueil 2003, p. I-4989.

<sup>(25)</sup> Voir la lettre adressée en date 23 juillet 2007 par le CEPD à la présidence de la CIG concernant la protection des données dans le cadre du traité modificatif (disponible sur le site web du CEPD).

58. Il ne fait aucun doute qu'une analyse comparée des situations dans lesquelles on soupçonne une transposition incorrecte ou incomplète <sup>(26)</sup> ainsi qu'une communication interprétative peuvent renforcer la cohérence du rôle joué par la Commission en tant que gardienne des traités. Néanmoins, l'élaboration de ces instruments, qui peut prendre un certain temps et nécessiter un effort important, ne devrait pas retarder les procédures d'infraction dans les domaines pour lesquels la Commission a déjà clairement recensé une transposition ou une application incorrectes.

59. Par conséquent, le CEPD encourage la Commission à veiller à une meilleure mise en œuvre de la directive en recourant, lorsque cela est nécessaire, à la procédure d'infraction. À cet égard, le CEPD fera usage des compétences qui lui ont été attribuées afin d'intervenir, le cas échéant, devant la Cour de justice dans des procédures d'infraction relatives à la mise en œuvre de la directive 95/46 ou d'autres instruments juridiques dans le domaine de la protection des données à caractère personnel.

#### D. Communication interprétative

60. La communication fait également référence à une communication interprétative, dans laquelle la Commission précisera l'interprétation qu'elle fait de certaines dispositions de la directive dont la mise en œuvre est jugée problématique et qui peuvent donc conduire à l'ouverture d'une procédure d'infraction. Le CEPD se réjouit du fait que, à cet égard, la Commission tiendra compte des travaux menés par le groupe en ce qui concerne l'interprétation des dispositions. Il est en effet essentiel que la position du groupe soit dûment prise en considération lors de la rédaction future de la communication interprétative et que celui-ci soit consulté de manière appropriée afin de tenir compte de son expérience quant à l'application de la directive au niveau national.

61. Par ailleurs, le CEPD rappelle qu'il se tient à la disposition de la Commission pour la conseiller sur toute question relative à la protection des données à caractère personnel. Cela s'applique également aux instruments, notamment les communications de la Commission, qui n'ont pas de force contraignante, mais qui ont néanmoins pour objectif de définir les grandes orientations suivies par la Commission dans le domaine de la protection des données à caractère personnel. Pour ce qui est de la communication interprétative proprement dite, il conviendrait, afin que ce rôle consultatif soit efficace, que la consultation du CEPD ait lieu avant que le texte soit adopté <sup>(27)</sup>. Le rôle consultatif du Groupe de l'article 29 et du CEPD apportera une valeur ajoutée à cette communication, tout en préservant l'indépendance de la Commission quant à la décision que celle-ci prend de manière autonome de lancer formellement une procédure d'infraction relative à la mise en œuvre de la directive.

<sup>(26)</sup> Communication, p. 6.

<sup>(27)</sup> Voir le document stratégique intitulé «Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes», qui peut être consulté sur le site web du CEPD (point 5.2 du document).

62. Le CEPD se réjouit du fait que la communication susmentionnée n'abordera qu'un nombre restreint d'articles, ce qui permettra de se concentrer sur les questions plus sensibles. À cet égard, il attire l'attention de la Commission sur les questions suivantes, qui méritent qu'on y accorde une attention particulière dans la communication interprétative:

- le concept de données à caractère personnel <sup>(28)</sup>,
- la définition du rôle du responsable du traitement ou du sous-traitant,
- la détermination de la loi applicable,
- le principe de limitation de la finalité et les utilisations incompatibles,
- les motifs juridiques justifiant le traitement, notamment en ce qui concerne le consentement sans équivoque et l'équilibre des intérêts.

#### E. Autres instruments non contraignants

63. D'autres instruments non contraignants devraient renforcer, dans une optique prévoyante, le respect des principes relatifs à la protection des données, en particulier dans les environnements liés aux nouvelles technologies. De telles mesures devraient être fondées sur la notion de «*privacy by design*» (prise en compte du respect de la vie privée lors de la conception), de sorte que l'architecture des nouvelles technologies soit conçue et réalisée en tenant dûment compte des principes relatifs à la protection des données. La promotion des produits technologiques respectant la vie privée devrait être un élément capital dans un contexte où l'informatique omniprésente se développe rapidement.

64. La nécessité d'élargir l'éventail des parties prenantes à l'application effective de la législation relative à la protection des données est étroitement liée à ce qui précède. D'une part, le CEPD soutient résolument le rôle fondamental joué par les autorités chargées de la protection des données pour veiller au respect des principes de la directive en exerçant pleinement leurs compétences ainsi qu'en recourant aux possibilités de coordination au sein du Groupe de l'article 29. Une application plus effective de la directive est également un des objectifs de l'initiative de Londres.

65. D'autre part, le CEPD souligne qu'il est souhaitable d'encourager le respect des principes relatifs à la protection des données dans le secteur privé, au moyen de l'autorégulation et de la concurrence. Les entreprises devraient être encouragées à mettre en application ces principes et à entrer en concurrence afin de proposer des produits et des services respectant la vie privée, de manière à étendre leur position sur le marché en répondant mieux aux attentes des consommateurs soucieux du respect de leur vie privée. Les labels de protection de la vie privée constituent à cet égard un bon exemple. Ceux-ci pourraient accompagner les produits et services ayant fait l'objet d'une procédure de certification <sup>(29)</sup>.

<sup>(28)</sup> Cet aspect a également été examiné dans l'avis n° 4/2007 du groupe cité à la note de bas de page 10.

<sup>(29)</sup> Il convient de mentionner le projet EuroPriSe lancé par l'autorité chargée de la protection des données du Land de Schleswig-Holstein dans le cadre du programme eTEN de la Commission européenne.

66. Le CEPD souhaiterait également attirer l'attention de la Commission sur d'autres instruments qui, bien qu'ils ne soient pas mentionnés dans la communication, pourraient contribuer à une meilleure mise en œuvre de la directive. Ces instruments susceptibles d'aider les autorités chargées de la protection des données à assurer une meilleure application de la législation pertinente sont notamment les suivants:

- l'élaboration de critères,
- la promotion et l'échange des meilleures pratiques,
- la réalisation d'audits par des tiers portant sur le respect de la vie privée.

#### F. Autres instruments dans une perspective à plus long terme

67. Enfin, le CEPD songe à d'autres instruments, qui ne sont pas mentionnés dans la communication mais qui pourraient être envisagés dans la perspective d'une modification future de la directive ou inclus dans d'autres textes législatifs horizontaux. Citons notamment:

- les recours collectifs, qui permettraient à des groupes de citoyens de saisir la justice dans des affaires relatives à la protection des données à caractère personnel, pourraient constituer un instrument très efficace pour faciliter la mise en application de la directive,
- les recours formés par des personnes morales, notamment les associations de consommateurs et les organisations syndicales, dont les activités visent à protéger les intérêts de certaines catégories de personnes, pourraient avoir un effet similaire,
- l'obligation, pour les responsables du traitement, de signaler aux personnes concernées les infractions en matière de sécurité constituerait non seulement une garantie extrêmement utile, mais permettrait aussi de sensibiliser davantage les citoyens à cette question,
- les dispositions facilitant l'utilisation des labels de protection de la vie privée ou la réalisation d'audits par des tiers (voir les points 65 et 66 ci-dessus) dans un contexte transnational.

#### G. Mieux définir les compétences des acteurs institutionnels, en particulier du Groupe de l'article 29

68. Différents acteurs institutionnels ont des compétences liées à la mise en œuvre de la directive. Ainsi, conformément à l'article 28, les autorités de contrôle des États membres sont chargées de surveiller l'application des dispositions nationales visant à transposer la directive dans les États membres. L'article 29 institue le groupe réunissant les autorités de contrôle, dont la mission est définie à l'article 30, tandis qu'un comité, prévu à l'article 31, composé des représentants des gouvernements des États membres, assiste la Commission pour ce qui est des mesures d'exécution adoptées au niveau de la Communauté (procédure de comité).

69. La nécessité de mieux définir les compétences des différents acteurs concerne en particulier le groupe (ou ses activités). L'article 30, paragraphe 1, énumère quatre tâches qui lui incombent et qui consistent, en résumé, à examiner la mise

en œuvre de la directive au niveau national en vue d'en assurer l'homogénéité et à donner des avis sur les évolutions à l'échelle communautaire: niveau de protection, propositions législatives et codes de conduite. Cette liste met en évidence les compétences assumées par le groupe dans le domaine de la protection des données, qui sont par ailleurs illustrées par les documents que celui-ci a élaborés au fil des ans.

70. Aux termes de la communication, le groupe «représente un élément clé pour assurer une application meilleure et plus cohérente». Le CEPD souscrit pleinement à cette affirmation, mais juge également nécessaire de préciser certains éléments particuliers des compétences concernées.

71. Premièrement, la communication demande instamment d'améliorer la contribution du groupe, en ce sens que les autorités nationales devraient s'efforcer d'adapter leurs pratiques nationales afin de les aligner sur la ligne commune arrêtée<sup>(30)</sup>. Le CEPD se réjouit de l'intention exprimée dans cette déclaration mais il met en garde contre une confusion des compétences. C'est à la Commission qu'il appartient, en vertu de l'article 211 du traité CE, de contrôler le respect de la législation dans les États membres, y compris par les autorités de contrôle. Le groupe, en tant qu'organe consultatif indépendant, ne peut être tenu responsable de la mise en application de ses avis par les autorités nationales.

72. Deuxièmement, la Commission ne doit pas oublier qu'elle joue plusieurs rôles au sein du groupe, étant donné qu'elle ne fait pas seulement partie de ce groupe mais qu'elle en assure également le secrétariat. Dans l'exercice de ce deuxième rôle, elle doit apporter son concours au groupe de manière à ce que celui-ci puisse accomplir sa mission de manière indépendante. Concrètement, cela signifie deux choses: la Commission doit fournir les ressources nécessaires, tandis que le secrétariat doit fonctionner sous les ordres du groupe et de son président pour ce qui est du contenu et de la portée des activités du groupe ainsi que de la nature de sa contribution. De manière plus générale, les activités menées par la Commission pour l'accomplissement de ses autres missions conformément au droit communautaire ne devraient pas avoir d'incidence sur les services qu'elle met à disposition pour assurer le secrétariat du groupe.

73. Troisièmement, bien que le groupe ait toute latitude pour fixer ses priorités, la Commission pourrait indiquer ce qu'elle attend de lui et comment, selon elle, les ressources disponibles pourraient être utilisées de la manière la plus efficace.

74. Quatrièmement, le CEPD regrette que la communication ne donne pas d'indications précises quant à la répartition des rôles entre la Commission et le groupe. Il invite la Commission à présenter au groupe un document comportant de telles indications. Le CEPD suggère d'y inclure les questions suivantes:

- la Commission pourrait demander au groupe de travailler sur un certain nombre de questions concrètes et précises. Les demandes de la Commission devraient être fondées sur une stratégie claire exposant le mandat et les priorités du groupe,

<sup>(30)</sup> Voir la page 11 de la communication.

- le groupe définit, de manière précise, ses propres priorités dans un programme de travail,
- éventuellement, la Commission et le groupe pourraient définir leurs arrangements au moyen d'un protocole d'accord,
- il est essentiel que le groupe soit pleinement associé à l'interprétation de la directive et qu'il contribue aux discussions susceptibles de déboucher sur l'apport de modifications à la directive.

## VII. CONCLUSIONS

75. Le CEPD souscrit à la conclusion principale de la Commission selon laquelle la directive ne devrait pas être modifiée à court terme. On pourrait néanmoins renforcer cette conclusion en s'appuyant également sur la nature de la directive et la pratique législative de l'Union.
76. Les points de départ du raisonnement suivi par le CEPD sont les suivants:
- à court terme, il est plus opportun de se concentrer sur les améliorations à apporter à la mise en œuvre de la directive,
  - à plus long terme, des modifications de la directive semblent inévitables,
  - il conviendrait de fixer dès à présent une date précise pour l'examen de la directive en vue de l'élaboration des propositions destinées à apporter les modifications susmentionnées, ce qui inciterait certainement à entamer dès aujourd'hui la réflexion sur les changements futurs.
77. Les principaux aspects des modifications futures sont notamment les suivants:
- il n'est pas nécessaire d'élaborer de nouveaux principes mais il faut de toute évidence prévoir d'autres arrangements administratifs,
  - le champ d'application étendu de la législation relative à la protection des données, applicable à toutes les utilisations des données à caractère personnel, ne devrait pas être modifié,
  - la législation relative à la protection des données devrait permettre d'adopter une approche équilibrée dans des cas concrets et aussi donner la possibilité aux autorités chargées de la protection des données de définir des priorités,
  - le système devrait s'appliquer intégralement à l'utilisation des données à caractère personnel à des fins répressives, tout en sachant que des mesures complémentaires appropriées peuvent s'avérer nécessaires pour répondre à des problèmes particuliers dans ce domaine.
78. Le CEPD suggère que la Commission précise les éléments suivants: un calendrier pour la réalisation des actions mentionnées au chapitre 3 de la communication, un délai pour la présentation ultérieure d'un rapport sur l'application de la directive, un mandat permettant de mesurer le degré de réalisation des actions prévues et la manière de procéder à plus long terme.

79. Le CEPD accueille favorablement l'approche relative aux technologies, qui constitue une première étape importante, et suggère de lancer la discussion sur une approche à long terme, notamment un débat fondamental sur le développement d'une société de la surveillance. Il se réjouit également de l'examen en cours de la directive 2002/58/CE et de la nécessité éventuelle d'adopter des règles plus spécifiques permettant d'apporter une solution aux problèmes de protection des données suscités par les nouvelles technologies comme Internet ou la RFID. Ces mesures devraient prendre en considération le contexte dynamique dans sa globalité et, dans une perspective à long terme, englober également la directive 95/46/CE.

80. Le CEPD regrette que les notions de respect de la vie privée à l'échelle mondiale et de compétence occupent une place limitée dans la communication et il demande que soient mises en place des solutions pratiques conciliant la nécessité de protéger les citoyens européens concernés et les limitations territoriales de l'Union européenne et de ses États membres, notamment: le renforcement du cadre mondial pour la protection des données, le perfectionnement du régime particulier applicable aux transferts de données vers des pays tiers, la conclusion d'accords internationaux en matière de compétence ou d'accords similaires avec les pays tiers et l'élaboration de mécanismes visant à assurer le respect des normes à l'échelle mondiale, notamment le recours à des règles d'entreprise contraignantes par les sociétés multinationales.

Le CEPD invite la Commission à commencer à réfléchir à ce projet mobilisateur, avec le plus grand nombre de parties prenantes intéressées.

81. Pour ce qui est de l'application de la législation, le CEPD fait les suggestions suivantes à la Commission:
- se pencher davantage sur les implications de la participation de sociétés privées aux activités des services répressifs,
  - maintenir l'effet utile de l'article 13 de la directive, éventuellement en proposant des textes législatifs visant à harmoniser les conditions et garanties applicables aux exceptions prévues par cet article.
82. Une mise en œuvre complète de la directive signifie: 1) qu'il faut veiller à ce que les États membres respectent intégralement les obligations qui leur incombent en vertu du droit européen; et 2) qu'il conviendrait de recourir pleinement à d'autres instruments, non contraignants, susceptibles de contribuer à un degré élevé et harmonisé de protection des données. Le CEPD demande à la Commission d'indiquer clairement comment elle entend utiliser ces différents instruments et quelle distinction elle fait entre ses propres compétences et celles du Groupe de l'article 29.
83. En ce qui concerne les instruments susmentionnés:
- dans certains cas, l'adoption de mesures législatives spécifiques au niveau de l'UE peut s'avérer nécessaire,
  - la Commission est encouragée à veiller à une meilleure mise en œuvre de la directive en recourant à la procédure d'infraction,

- la Commission est invitée à recourir à une communication interprétative — tout en respectant le rôle consultatif tant du groupe que du CEPD — pour les questions suivantes: le concept de données à caractère personnel, la définition du rôle du responsable du traitement ou du sous-traitant, la détermination de la loi applicable, le principe de limitation de la finalité et les utilisations incompatibles, et les motifs juridiques justifiant le traitement, notamment en ce qui concerne le consentement sans équivoque et l'équilibre des intérêts,
  - les instruments non contraignants englobent ceux fondés sur la notion de «privacy by design» (prise en compte du respect de la vie privée lors de la conception),
  - également à plus long terme: les recours collectifs, les recours formés par des personnes morales dont les activités visent à protéger les intérêts de certaines catégories de personnes, l'obligation, pour les responsables du traitement, de signaler aux personnes concernées les infractions en matière de sécurité et les dispositions facilitant l'utilisation des labels de protection de la vie privée ou la réalisation d'audits par des tiers dans un contexte transnational.
84. Le CEPD invite la Commission à présenter au groupe un document donnant des indications précises quant à la répartition des rôles entre la Commission et le groupe, et d'y inclure notamment les questions suivantes:
- demandes adressées par la Commission pour que le groupe travaille sur un certain nombre de questions concrètes et précises, sur la base d'une stratégie claire exposant le mandat et les priorités du groupe,
  - possibilité de définir des arrangements dans un protocole d'accord,
  - pleine participation du groupe à l'interprétation de la directive et aux discussions susceptibles de déboucher sur l'apport de modifications à la directive.
85. Les conséquences du traité modificatif doivent être dûment examinées, de manière à assurer l'application la plus large possible des principes relatifs à la protection des données énoncés dans la directive. Le CEPD a présenté des suggestions à cet égard dans une lettre adressée à la présidence de la CIG.
- Fait à Bruxelles, le 25 juillet 2007.
- Peter HUSTINX  
*Contrôleur européen de la protection des données*