

CONCLUSIONS DE L'AVOCAT GÉNÉRAL

M^{ME} JULIANE KOKOTT

présentées le 18 juillet 2007¹

I — Introduction

1. La présente affaire illustre le fait que le stockage de données à certaines fins suscite l'envie de les utiliser à plus large échelle. En Espagne, les fournisseurs d'accès à Internet sont tenus de stocker certaines données relatives aux utilisateurs individuels afin qu'elles puissent, le cas échéant, être utilisées dans le cadre d'une enquête pénale ou en vue de la sauvegarde de la sécurité publique et de la défense nationale. Or, une association de titulaires de droits d'auteur souhaite utiliser ces données afin d'identifier les utilisateurs qui enfreignent ces droits par l'échange de fichiers.
2. C'est la raison pour laquelle la juridiction de renvoi souhaite s'entendre préciser si le droit communautaire autorise, voire exige, la divulgation de données à caractère personnel relatives au trafic concernant l'utilisation d'Internet aux titulaires de droits de propriété intellectuelle. Elle part du principe que

diverses directives sur la protection de la propriété intellectuelle et sur la société de l'information confèrent aux titulaires de droits correspondants le droit d'exiger des fournisseurs de services électroniques qu'ils leur communiquent ces données lorsqu'elles sont de nature à démontrer une violation de droits protégés.

3. Je démontrerai toutefois dans les pages qui suivent que les dispositions du droit communautaire relatives à la protection des données dans le secteur des communications électroniques n'autorisent la transmission de données à caractère personnel relatives au trafic qu'aux autorités publiques compétentes, mais ne permettent pas une divulgation directe aux titulaires de droits d'auteur désireux de poursuivre civilement la violation de leurs droits.

II — Le cadre juridique

A — *Le cadre juridique communautaire*

4. Ce sont des dispositions relatives à la protection de la propriété intellectuelle et au

¹ — Langue originale: l'allemand.

commerce électronique ainsi, en particulier, que les dispositions sur la protection des données qui nous intéressent en l'espèce.

1. La protection de la propriété intellectuelle dans la société de l'information

5. Le premier instrument de protection de la propriété intellectuelle dans la société de l'information qu'il convient de nommer est la directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») ².

6. L'article 1^{er}, paragraphe 5, de la directive 2000/31 délimite le champ d'application de celle-ci. Aux termes du point b), la directive n'est pas applicable «aux questions relatives aux services de la société de l'information couvertes par les directives 95/46/CE et 97/66/CE» ³.

2 — JO L 178, p. 1.

3 — Il s'agit de 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 (JO L 281, p. 31), et de la directive 97/66/CE du Parlement européen et du Conseil, du 15 décembre 1997, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO 1998, L 24, p. 1).

7. L'article 15, paragraphe 2, de la directive 2000/31 dispose ce qui suit:

«Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.»

8. L'article 18, paragraphe 1, de la directive 2000/31 est rédigé dans les termes suivants:

«Les États membres veillent à ce que les recours juridictionnels disponibles dans le droit national portant sur les activités des services de la société de l'information permettent l'adoption rapide de mesures, y compris par voie de référé, visant à mettre un terme à toute violation alléguée et à prévenir toute nouvelle atteinte aux intérêts concernés.»

9. La directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information⁴, contient des règles particulières concernant la protection de la propriété intellectuelle dans le commerce électronique. Nous retiendrons en particulier l'article 8, intitulé «Sanctions et voies de recours»:

«1. Les États membres prévoient des sanctions et des voies de recours appropriées contre les atteintes aux droits et obligations prévus par la présente directive et prennent toutes les mesures nécessaires pour en garantir l'application. Ces sanctions sont efficaces, proportionnées et dissuasives.

2. Chaque État membre prend les mesures nécessaires pour faire en sorte que les titulaires de droits dont les intérêts sont lésés par une infraction commise sur son territoire puissent intenter une action en dommages-intérêts et/ou demander qu'une ordonnance sur requête soit rendue ainsi que, le cas échéant, demander la saisie du matériel concerné par l'infraction ainsi que des dispositifs, produits ou composants visés à l'article 6, paragraphe 2.

[...]

10. L'article 9 de la directive 2001/29 limite son champ d'application de la manière suivante:

«La présente directive n'affecte pas les dispositions concernant notamment les brevets, les marques, les dessins et modèles, les modèles d'utilité, les topographies des semi-conducteurs, les caractères typographiques, l'accès conditionnel, l'accès au câble des services de radiodiffusion, la protection des trésors nationaux, les exigences juridiques en matière de dépôt légal, le droit des ententes et de la concurrence déloyale, le secret des affaires, la sécurité, la confidentialité, la protection des données personnelles et le respect de la vie privée, l'accès aux documents publics et le droit des contrats.»

11. L'article 8 de la directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle⁵, prévoit un droit d'information particulier en faveur des titulaires de droits de propriété intellectuelle:

«1. Les États membres veillent à ce que, dans le cadre d'une action relative à une atteinte à un droit de propriété intellectuelle et en réponse à une demande justifiée et

4 — JO L 167, p. 10.

5 — JO L 157, p. 45. La version utilisée ici est la version corrigée publiée au JO L 195, p. 16.

proportionnée du requérant, les autorités judiciaires compétentes puissent ordonner que des informations sur l'origine et les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle soient fournies par le contrevenant et/ou toute autre personne qui:

3. Les paragraphes 1 et 2 s'appliquent sans préjudice d'autres dispositions législatives et réglementaires qui:

[...]

[...]

- c) a été trouvée en train de fournir, à l'échelle commerciale, des services utilisés dans des activités contrefaisantes,
- e) régissent la protection de la confidentialité des sources d'information ou le traitement des données à caractère personnel.»

[...]

12. Aux termes de son article 2, paragraphe 3, la directive 2004/48 n'affecte pas:

2. Les informations visées au paragraphe 1 comprennent, selon les cas:

- a) les noms et adresses des producteurs, fabricants, distributeurs, fournisseurs et autres détenteurs antérieurs des marchandises ou des services, ainsi que des grossistes destinataires et des détaillants;
- «a) les dispositions communautaires régissant le droit matériel de la propriété intellectuelle, la directive 95/46/CE, la directive 1999/93/CE et la directive 2000/31/CE en général et les articles 12 à 15 de cette dernière directive en particulier;

[...]

[...]»

2. Les dispositions relatives à la protection des données

13. La directive importante en matière de protection des données est 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)⁶.

14. Aux termes de son article 1^{er}, paragraphe 1, elle «harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté».

15. Aux termes de son article 1^{er}, paragraphe 2, les dispositions de cette directive précisent et complètent la directive 95/46⁷ aux fins énoncées au paragraphe 1.

16. L'article 2, sous b), de la directive 2002/58 définit la notion de données relatives au trafic comme étant «toutes les données traitées en vue de l'acheminement d'une communication par un réseau de télécommunications électroniques ou de sa facturation».

17. Le traitement des données relatives au trafic est soumis aux règles énoncées à l'article 6:

«1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5 du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période

6 — JO L 201, p. 37.

7 — Note sans objet: voir note 3.

au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

[...]

6. Les paragraphes 1, 2, 3 et 5 s'appliquent sans préjudice de la possibilité qu'ont les organes compétents de se faire communiquer des données relatives au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation.»

18. La réserve de l'article 15, paragraphe 1, de la directive 2002/58 évoquée à l'article 6, paragraphe 1, de celle-ci est rédigée dans les termes suivants:

«Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention,

la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.»

19. Cette réserve est expliquée dans le onzième considérant de la directive 2002/58:

«(11) À l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent,

la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.»

20. L'article 19 de la directive 2002/58 règle son rapport à la directive 97/66 qui l'a précédée:

«La directive 97/66/CE est abrogée avec effet à partir de la date visée à l'article 17, paragraphe 1.

Les références faites à la directive abrogée s'entendent comme étant faites à la présente directive.»

21. L'article 13, paragraphe 1, de la directive 95/46, auquel se réfère l'article 1^{er} de la directive 2002/58, dispose ce qui suit:

«Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

- a) la sûreté de l'État;
- b) la défense;
- c) la sécurité publique;
- d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;
- e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;

f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);

g) la protection de la personne concernée ou des droits et libertés d'autrui.»

22. Il convient en outre d'observer qu'un groupe indépendant de protection des personnes à l'égard du traitement des données à caractère personnel (ci-après le «groupe de protection des données») a été institué en application de l'article 29 de la directive 95/46⁸. Il est chargé de prendre position sur toute question relative au droit en matière de protection des données. Le contrôleur européen de la protection des données, mis en place en application de l'article 286 CE et du règlement (CE) n° 45/2001⁹, est chargé d'une mission analogue.

23. Enfin, la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données géné-

rées 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/CE¹⁰, intéresse elle aussi la présente affaire.

24. La directive 2006/24 oblige les États membres à conserver notamment les données relatives au trafic Internet et doit, conformément à son article 15, être transposée dans les ordres juridiques internes au plus tard le 15 septembre 2007. Elle autorise néanmoins les États membres à différer de 18 mois la conservation des données de communication concernant l'accès à l'Internet. Le Royaume d'Espagne n'a pas fait usage de cette faculté.

25. L'article 11 de la directive 2006/24 ajoute un paragraphe 1 bis à l'article 15 de la directive 2002/58:

«Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE [...] aux fins visées à l'article 1^{er}, paragraphe 1, de ladite directive.»

8 — Les documents du groupe de protection des données peuvent être consultés sous http://ec.europa.eu.justice_home/fsj/privacy/workinggroup/index_de.htm.

9 — Règlement 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 (JO 2001, L 8, p. 1).

10 — JO L 105, p. 54.

26. L'accès aux données conservées conformément à la directive 2006/24 est réglé à l'article 4:

«Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme.»

la Información y de Comercio Electrónico) du 11 juillet 2002:

«Article 12. Devoir de conservation des données relatives au trafic dans le domaine des communications électroniques

1. Les opérateurs de réseaux et services de communications électroniques, les fournisseurs d'accès à des réseaux de télécommunications et les fournisseurs de services de stockage de données conserveront les données de connexion et de trafic engendrées par les communications établies au cours de la prestation d'un service de la société de l'information pour une période maximale de 12 mois aux conditions établies par le présent article et par les règles adoptées en vue de sa mise en œuvre.

B — *Le cadre juridique espagnol*

27. La juridiction de renvoi limite l'exposé du cadre juridique national essentiellement à l'article 12, paragraphes 1 à 3, de la loi n° 34/2002 sur les services de la société de l'information et du commerce électronique (Ley 34/2002 de Servicios de la Sociedad de

2. [...] Les opérateurs de réseaux et services de communications électroniques et les fournisseurs de services visés par le présent article ne pourront utiliser les données conservées à des fins autres que celles qui sont indiquées au paragraphe suivant ou autres que celles que la loi autorise, et ils adopteront les mesures de sécurité appropriées afin d'éviter leur perte ou altération ainsi que tout accès non autorisé à ces données.

3. Les données seront conservées en vue de leur utilisation dans le cadre d'une enquête pénale ou en vue de la sauvegarde de la sécurité publique et de la défense nationale et seront mises à la disposition des juges ou tribunaux ou du ministère public qui en feront la demande. Ces données ne seront communiquées aux forces de l'ordre que conformément aux dispositions de la réglementation sur la protection des données personnelles.»

28. La juridiction de renvoi indique en outre que la violation de droit d'auteur n'est punissable en Espagne que lorsque les faits sont commis dans un but lucratif¹¹.

III — Le contexte technique, les faits et le litige au principal

29. La requérante au principal, Productores de Música de España (ci-après «Promusicae»), est une association sans but lucratif regroupant des producteurs et des éditeurs d'enregistrements musicaux et d'enregistrements audiovisuels, essentiellement musicaux. Elle a engagé un recours afin d'obtenir qu'il soit ordonné à un fournisseur de

services d'accès à l'Internet, la Telefónica de España SAU (ci-après «Telefónica»), de lui révéler l'identité et l'adresse de certains utilisateurs de l'Internet. Promusicae a identifié ces personnes au moyen de ce qu'il est convenu d'appeler leurs adresses IP et parce qu'elle connaît le jour et l'heure auxquels elles les ont utilisées.

30. L'adresse IP est un format d'adresse numérique, comparable à un numéro de téléphone, qui permet aux appareils connectés au réseau, tels que des serveurs Web, des serveurs de courrier électronique ou des ordinateurs personnels, de communiquer sur l'Internet. Ainsi, par exemple, le serveur sur lequel les pages de la Cour peuvent être consultées porte l'adresse IP 147.67.243.28¹². Lorsqu'un utilisateur consulte une page, l'adresse de l'ordinateur appelant est communiquée à l'ordinateur dans lequel la page est stockée, de sorte que les données peuvent être transférées d'un ordinateur à l'autre par le biais de l'Internet.

31. Des adresses IP fixes peuvent être attribuées à des utilisateurs privés pour leurs communications avec l'Internet, à la façon d'un raccordement au réseau téléphonique. Cette façon de procéder est néanmoins assez rare, car l'Internet est actuellement organisé de telle manière que seul un nombre limité

11 — Elle se réfère à ce sujet à la Circular 1/2006, du 5 mayo 2006, sobre los delitos contra la propiedad intelectual e industrial tras la reforma de la Ley Orgánica 15/2003, http://www.fiscal.es/csblob/CIRCULAR%201_2006.doc?blobcol=urldata&blobheader=application%2Fmsword&blobkey=id&blobtable=MungoBlobs&blobwhere=1109248064092&ssbinary=true, p. 37 et suiv., de la Fiscalía General del Estado (ministère public général de l'État).

12 — Selon www.dnsstuff.com.

d'adresses est mis à la disposition de chaque fournisseur d'accès¹³. C'est pourquoi ce sont généralement, comme en l'espèce, des adresses IP dynamiques qui sont utilisées, c'est-à-dire que le fournisseur d'accès attribue à ses clients pour chaque accès une adresse ad hoc qu'il puise dans son contingent d'adresses. Par sa nature même, cette adresse peut donc changer à chaque connexion.

32. Promusicae a indiqué qu'elle avait identifié toute une série d'adresses IP qui auraient été utilisées à des moments déterminés pour des échanges de fichiers musicaux «filesharing» dont les droits d'auteur et les droits d'exploitation appartiennent à ses associés.

33. Le «filesharing» est une forme d'échange de fichiers, par exemple de morceaux de musique ou de films. Les utilisateurs copient tout d'abord les fichiers sur leur ordinateur et les offrent ensuite à quiconque est connecté à eux via l'Internet et un programme déterminé, à savoir en l'espèce, Kazaa. Au cours d'une telle opération, c'est normalement¹⁴ l'adresse IP de celui qui offre

le fichier d'un autre à la consultation qui est utilisée et qui peut ainsi être identifiée.

34. Pour pouvoir engager une action à l'encontre de ces utilisateurs, Promusicae exige du fournisseur d'accès concerné, Telefónica, qu'il lui communique les coordonnées des utilisateurs auxquels les adresses IP qu'elle a identifiées ont été attribuées aux heures qu'elle indique. Telefónica est, en effet, en mesure d'identifier chaque connexion utilisée parce qu'elle conserve, même après la fin de celle-ci, les coordonnées de celui à qui elle a attribué une adresse IP déterminée ainsi que le moment de cette attribution.

35. La juridiction de renvoi a, dans une première décision, ordonné à Telefónica de fournir les informations souhaitées. Telefónica s'est néanmoins rebiffée au motif que l'article 12 de la loi n° 34/2002 lui interdit de fournir des renseignements au tribunal. Les opérateurs de réseaux et de services de communications électroniques ainsi que les fournisseurs de services ne peuvent livrer des informations sur les données que la loi leur impose de conserver que dans le cadre d'une enquête pénale ou en vue de la sauvegarde de la sécurité publique et de la défense nationale.

36. Si elle convient que cette interprétation puisse être correcte en droit espagnol, la juridiction de renvoi estime néanmoins que

13 — Voir, à ce sujet, communication de la Commission au Conseil et au Parlement européen — l'Internet nouvelle génération: priorités d'actions dans la migration vers le nouveau protocole Internet IPv6 [COM(2002) 96].

14 — Techniquement, il semble qu'il soit également possible d'occulter sa propre adresse IP. Les offres correspondantes sont néanmoins payantes ou très lentes, voire les deux. Voir contribution wikipedia anonyme P2P, http://en.wikipedia.org/wiki/Anonymous_p2p ainsi que, sans référence au «filesharing», document de travail WP 37 du groupe de protection des données du 21 novembre 2000, «L'espace privé dans l'Internet», p. 86 et suiv.

la disposition en cause serait alors incompatible avec le droit communautaire. C'est la raison pour laquelle elle a adressé la question préjudicielle suivante à la Cour:

«Le droit communautaire et, concrètement, l'article 15, paragraphe 2, et l'article 18 de la directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, l'article 8, paragraphes 1 et 2, de la directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, l'article 8 de la directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle et l'article 17, paragraphe 2, et l'article 47 de la charte des droits fondamentaux de l'Union européenne permettent-ils aux États membres de limiter au cadre d'une enquête criminelle ou aux impératifs de sauvegarde de la sécurité publique et de la défense nationale, et donc à l'exclusion des procédures civiles, l'obligation qui incombe aux opérateurs de réseaux et services de communications électroniques, aux fournisseurs d'accès à des réseaux de télécommunications et aux fournisseurs de services de stockage de données de conserver et de mettre à disposition les données de connexion et de trafic engendrées par les communications établies au cours de la prestation d'un service de la société de l'information?»

37. Ont participé à la procédure Promusicae, Telefónica, les gouvernements italien, slovène, finlandais et du Royaume-Uni ainsi que la Commission des Communautés européennes. Le groupe de protection des données¹⁵ ainsi que le contrôleur européen de la protection des données n'ont pas présenté d'observations, en particulier parce que l'article 23 du statut de la Cour ne prévoit pas leur intervention. Étant donné, cependant, qu'ils sont susceptibles d'apporter une contribution importante à la solution de questions relatives au droit de la protection des données, j'ai accordé une attention particulière aux prises de position qu'ils avaient publiées à propos de la question soulevée en l'espèce.

IV — Appréciation juridique

38. La Cour doit déterminer s'il est compatible avec les directives citées par la juridiction de renvoi de limiter l'obligation de communiquer les données relatives au trafic au cadre de poursuites judiciaires et d'autres procédures analogues, mais d'en exclure les procédures de droit civil.

39. La juridiction de renvoi estime qu'il y aurait une contradiction entre le droit

¹⁵ — Voir le point 22 plus haut.

espagnol et le droit communautaire, mais elle perd cependant de vue que la disposition de droit espagnol en cause est fondée sur l'article 15 de la directive 2002/58 et reprend très largement les termes de celui-ci. Cette directive contient des règles sur la protection des données dans le secteur des communications électroniques et complète ainsi la directive 95/46 au moyen de règles générales concernant la protection des données.

40. Il s'agit dès lors de vérifier si, compte tenu des règles sur la protection des données, il est compatible avec les dispositions citées par la juridiction de renvoi d'interdire aux fournisseurs d'accès à l'Internet d'identifier les titulaires de certaines lignes d'abonnés de manière à permettre l'engagement de poursuites de droit civil pour violation des droits d'auteur.

d'obligations dans le chef d'un particulier¹⁷. Si le droit espagnol s'opposait d'une manière incontestable à toute diffusion des données en cause, l'interprétation de directives sollicitée par la juridiction de renvoi ne saurait pas davantage avoir pour effet d'obliger Telefónica à les communiquer. Compte tenu des informations dont dispose la Cour, il n'est cependant pas exclu que le droit espagnol puisse être interprété d'une manière conforme aux directives. Aussi longtemps que cette possibilité existe, une demande préjudicielle telle que celle qui a été adressée à la Cour en l'espèce ne peut pas être considérée comme n'étant pas indispensable à la juridiction de renvoi pour statuer au principal¹⁸.

B — *Sur la rapport des différentes directives entre elles*

A — *Sur la recevabilité de la demande*

41. On pourrait concevoir des doutes concernant la recevabilité de la demande préjudicielle et la nécessité pour la juridiction nationale d'obtenir une réponse à la question qu'elle a adressée à la Cour¹⁶. Une directive ne peut pas, par elle-même, créer

42. Certains participants consacrent leurs observations — presque exclusivement — à interpréter les directives citées par la juridiction de renvoi. Ce faisant, ils soulignent régulièrement la nécessité d'une protection effective contre les violations du droit d'auteur. La Commission, en revanche, observe à bon droit que les trois directives en question ne touchent pas au droit de la protection des données.

16 — Voir arrêts du 16 mars 2006, Poseidon Chartering (C-3/04, Rec. p. I-2505, point 14), et du 14 décembre 2006, Confederación Española de Empresarios de Estaciones de Servicios (C-217/05, Rec. p. I-11987, point 17), ainsi que les notes qu'ils contiennent respectivement.

17 — Arrêts du 5 octobre 2004, Pfeiffer e.a. (C-397/01 à C-403/01, Rec. p. I-8835, point 108), et du 3 mai 2005, Berlusconi e.a. (C-387/02, C-391/02 et C-403/02, Rec. p. I-3565, point 73).

18 — Voir arrêt du 16 juin 2005, Pupino (C-105/03, Rec. p. I-5285, points 31 et suiv., en particulier point 48).

43. Aux termes de l'article 1^{er}, paragraphe 5, sous b), de la directive 2000/31 sur le commerce électronique, celle-ci n'est pas applicable aux questions relatives aux services de la société de l'information couvertes par la directive 95/46 sur la protection des données et par la directive 97/66 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Cette directive a entre-temps été remplacée par la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

44. L'article 9 de la directive 2001/29 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information dispose expressément que la directive n'affecte pas, notamment, les dispositions concernant la protection des données personnelles et le respect de la vie privée.

45. Le rapport entre la directive 2004/48 relative au respect des droits de propriété intellectuelle et la protection des données est un peu moins clair. L'article 2, paragraphe 3, sous a), prévoit que cette directive n'affecte pas la directive 95/46. Promusicae en déduit que la directive 2002/58, qui n'est pas nommée dans cet article, ne serait pas applicable dans le champ d'application de la directive 2004/48.

46. Ce point de vue pourrait être compris en ce sens que, conformément au principe *lex posterior derogat legi priori*, la directive 2004/48 l'emporterait sur la directive 2002/58, mais pas sur la directive 95/46, qui est expressément soustraite de son champ d'application. Il convient cependant de rétorquer à Promusicae qu'aux termes de son article 1^{er}, paragraphe 1, la directive 2002/58 a pour objet de préciser et de compléter la directive 95/46, fonction que ne revendique pas la directive 2004/48. Au contraire, il résulte de son deuxième considérant que la protection de la propriété intellectuelle qu'elle instaure ne doit pas faire obstacle à la protection des données personnelles, y compris sur l'Internet. Il serait toutefois contradictoire de faire passer au second rang et sans compensation des dispositions ayant pour objet de préciser et de compléter des règles antérieures et qui concernent en particulier la protection des données sur l'Internet, protection à laquelle la protection de la propriété intellectuelle ne doit pas faire obstacle, alors que, par ailleurs, on continuerait à respecter les réglementations générales. Il serait bien plus logique d'étendre à la directive 2002/58 la réserve formulée en faveur de la directive 95/46.

47. En ce qui concerne le droit à l'information en cause ici que prévoit l'article 8, paragraphes 1 et 2, de la directive 2004/48, le fait que, conformément à l'article 8, paragraphe 3, sous e), il s'applique sans préjudice d'autres dispositions législatives et réglementaires qui régissent le traitement des données à caractère personnel milite également en faveur de cette solution. La proposition de la

Commission ne mettait pas encore explicitement l'accent sur la protection des données comme la directive le fait à nouveau; ce n'est qu'au cours des négociations au Conseil et au Parlement que cet accent a été introduit dans la directive¹⁹. La directive 2002/58 contient précisément de telles dispositions et n'est donc pas, à tout le moins, battue en brèche par le droit d'information litigieux prévu à l'article 8 de la directive 2004/48.

48. Il faut observer à titre complémentaire que l'accord TRIPs²⁰ n'exige pas, lui non plus, que la protection des données tienne la directive 2004/48 en échec. Promusicae expose à bon droit que les articles 41 et 42 de l'accord TRIPs exigent la protection effective de la propriété intellectuelle et souligne en particulier la nécessité de disposer de droits de recours juridictionnel. Un droit d'information n'est en tout cas prévu à l'article 47 de l'accord TRIPs que directement à l'encontre du contrevenant²¹. Les

États contractants peuvent introduire un tel droit, mais, conformément à l'article 47, ils ne sont pas tenus de le faire²². L'article 8 de la directive 2004/48 étend l'obligation d'information à des tiers, ce qui va même au-delà de cette faculté. Par conséquent, une telle extension peut être restreinte par la protection des données sans entrer en conflit avec l'accord TRIPs.

49. Toutes les trois directives citées par la juridiction de renvoi cèdent donc le pas aux directives sur la protection des données 95/46 et 2002/58. Contrairement à ce qu'ont fait valoir certains participants, cela ne signifie pas que la protection des données aurait la primauté sur les objectifs de ces directives. Il s'agit bien plutôt de créer un équilibre relatif entre ceux-ci et la protection des données dans le cadre des directives qui la consacrent.

19 — On comparera l'article 9, paragraphe 3, sous e), de la proposition de la Commission [COM(2003) 46] avec la disposition analogue du projet consolidé du Conseil du 19 décembre 2003 (document du Conseil 16289/03) et avec l'article 8, paragraphe 3, sous e), du projet remanié du Parlement (JO 2004, C 102 E, p. 242 et suiv.), qui a été repris tel quel par le Conseil.

20 — Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce, qui figure à l'annexe 1 C de l'accord instituant l'Organisation mondiale du commerce, approuvé au nom de la Communauté, pour ce qui concerne les matières relevant de ses compétences, dans la décision 94/800/CE du Conseil, du 22 décembre 1994 (JO L 336, p. 1). L'abréviation TRIPs correspond à Agreement on Trade-Related Aspects of Intellectual Property Rights.

21 — Dans sa version allemande, l'article 42, quatrième phrase, de l'accord TRIPs pourrait, certes, être (mal) entendu en ce sens qu'une protection juridictionnelle effective devrait prévoir un moyen d'identifier des renseignements confidentiels, alors que cette disposition doit au contraire permettre de protéger les informations confidentielles dans les procédures judiciaires lorsque cela est licite. Cela apparaît plus clairement dans les versions linguistiques à force probante (à savoir les versions anglaise, française et espagnole). Voir, également, dans le même sens Gervais, D., *The TRIPs Agreement, Drafting History and Analysis*, Londres, 2003, p. 291.

C — Sur la protection des données

50. La directive 2002/58, qui contient des dispositions sur la protection des données dans les communications électroniques, et la

22 — Telle était également la position du Conseil et de la Commission au cours de la procédure d'adoption de la directive 2004/48 (document du Conseil 6052/04 du 9 février 2004, p. 6 et suiv.).

directive 95/46, qui règle la protection des données d'une manière générale, sont importantes pour la solution du cas qui nous occupe. La Cour déduit en tout cas du principe de la protection des données, qui est un droit fondamental, des points de repère importants pour l'interprétation de ces dispositions de droit dérivé.

1. Sur l'obligation de respecter les droits fondamentaux dans la protection des données

51. La protection des données repose sur le droit fondamental à la vie privée, ainsi qu'il résulte en particulier de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la «CEDH»), qui a été signée à Rome le 4 novembre 1950²³. L'article 7 de la charte des droits fondamentaux de l'Union européenne²⁴ (ci-après la «charte»), qui a été proclamée à Nice le 7 décembre 2000, a confirmé ce droit fondamental. Son article 8 a mis un accent particulier sur le droit fondamental à la protection des données à caractère personnel, en rappelant des principes fondamentaux importants de la protection des données.

52. Conformément à cette disposition, la communication de données à caractère personnel à un tiers porte atteinte au droit au respect de la vie privée des intéressés, quelle que soit l'utilisation ultérieure des informations ainsi communiquées, et présente ainsi le caractère d'une ingérence au sens de l'article 8 de la CEDH²⁵.

53. Une telle ingérence méconnaît l'article 8 de la CEDH, sauf si elle est «prévue par la loi»²⁶. Conformément au principe de prévisibilité, une disposition qui permettrait une telle ingérence doit être formulée avec suffisamment de précision pour permettre à ses destinataires de régler leur conduite en fonction d'elle²⁷. L'exigence de prévisibilité a trouvé une expression particulière dans le droit de la protection des données qui impose que tout traitement de données soit lié à des fins déterminées, comme l'exige expressément l'article 8, paragraphe 2, de la charte. Cette obligation est concrétisée à l'article 6, paragraphe 1, sous b), de la directive 95/46, aux termes duquel les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

54. De surcroît, toute ingérence dans la vie privée — le traitement de données à

23 — Arrêt du 20 mai 2003, *Österreichischer Rundfunk e.a.* (C-465/00, C-138/01 et C-139/01, Rec. p. I-4989, points 73 et suiv.).

24 — JO C 364, p. 1.

25 — Arrêt *Österreichischer Rundfunk e.a.* (déjà cité à la note 23, point 74).

26 — *Ibidem*, point 76.

27 — *Ibidem*, point 77; la Cour s'y réfère à la jurisprudence de la Cour européenne des droits de l'homme.

caractère personnel — doit répondre à l'exigence de proportionnalité par rapport aux objectifs poursuivis²⁸. Il faut ainsi qu'un besoin social impérieux soit en cause et que la mesure prise soit proportionnée au but légitime recherché²⁹.

55. Le but légitime poursuivi en l'espèce est la protection des droits fondamentaux des titulaires de droits d'auteur, et notamment la protection de la propriété ainsi que le droit à une protection juridique effective. Il est de jurisprudence constante que ces deux droits fondamentaux font partie des principes généraux du droit communautaire³⁰, ce qui a été confirmé par les articles 17 et 47 de la charte. L'article 17, paragraphe 2, de la charte souligne ainsi que la propriété intellectuelle relève elle aussi du domaine de protection du droit fondamental à la propriété³¹.

56. C'est au législateur communautaire qu'il appartient en tout premier lieu d'établir un

équilibre entre les positions concernées en matière de droits fondamentaux ainsi qu'à la Cour lorsqu'elle interprète le droit communautaire. Les États membres sont néanmoins, eux aussi, tenus d'en tenir compte lorsqu'ils épuisent leur compétence réglementaire résiduelle dans le cadre de la transposition de directives. De surcroît, les pouvoirs publics et les juridictions des États membres ne doivent pas seulement interpréter leur droit national d'une manière conforme aux directives sur la protection des données, mais également veiller à ne pas se fonder sur une interprétation de ces directives qui entre en conflit avec les droits fondamentaux protégés par l'ordre juridique communautaire ou avec les autres principes généraux du droit communautaire³².

2. Sur l'applicabilité des directives sur la protection des données

57. Le droit dérivé concrétise les exigences préalables en matière de droits fondamentaux pour la protection des données et les élargit sur un point qui est également déterminant pour la solution de la présente affaire. Les directives, en effet, ne prévoient pas seulement une obligation des autorités nationales de garantir la protection des

28 — Ibidem, point 80.

29 — Ibidem, point 83, la Cour s'y réfère à la jurisprudence de la Cour européenne des droits de l'homme.

30 — Voir, en ce qui concerne le droit de propriété, notamment arrêts du 11 juillet 1989, *Schräder* (265/87, Rec. p. 2237, point 15); du 28 avril 1998, *Metronome Musik* (C-200/96, Rec. p. I-1953, point 21), et du 6 décembre 2005, *ABNA e.a.* (C-453/03, C-11/04, C-12/04 et C-194/04, Rec. p. I-10423, point 87). En ce qui concerne la protection juridique effective, voir arrêts du 15 mai 1986, *Johnston* (222/84, Rec. p. 1651, points 18 et 19); du 15 octobre 1987, *Heylens e.a.* (222/86, Rec. p. 4097, point 14); du 25 juillet 2002, *Unión de Pequeños Agricultores/Conseil* (C-50/00 P, Rec. p. I-6677, point 39), et du 13 mars 2007, *Unibet* (C-432/05, Rec. p. I-2271, point 37).

31 — Voir, déjà en ce sens, arrêt *Metronome Musik* (déjà cité à la note 30, points 21 et 26) ainsi que, tout récemment, l'arrêt que la Cour européenne des droits de l'homme a rendu le 11 janvier 2007 dans l'affaire *Anheuser-Busch Inc. c. Portugal* (plainte 73049/01, §72).

32 — Voir arrêt du 6 novembre 2003, *Lindqvist* (C-101/01, Rec. p. I-12971, point 83).

données, mais elles l'étendent en même temps aux particuliers, pour autant qu'il ne s'agisse pas d'un traitement effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques, comme le veut l'article 3, paragraphe 2, deuxième tiret, de la directive 95/46³³. La Communauté réalise et concrétise ainsi un but de protection résultant du droit fondamental à la protection des données³⁴.

58. Les actions de droit civil que Promusicae souhaite engager pour violation du droit d'auteur et le traitement des données de connexion par Telefónica ne sauraient être considérés comme des activités exclusivement personnelles ou domestiques, comme le montre également, en ce qui concerne le traitement de données de connexion, l'existence de la directive 2002/58, qui ne prévoit pas d'exception pour les activités personnelles ou domestiques, mais part de l'idée que le traitement de données à caractère personnel par des fournisseurs de services de communications électroniques est en principe soumis aux exigences de la protection des données. C'est ainsi que l'échange de pareilles données entre entreprises privées n'est pas exclu du champ d'application des règles qu'elle comporte. Il convient, par consé-

quent, de vérifier si les autres conditions d'application du droit de la protection des données sont réunies en l'espèce.

59. Aux termes de son article 3, paragraphe 1, la directive 2002/58 s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté. Conformément à l'article 2 de la directive 2002/58, ces notions sont définies dans la directive 95/46 ou dans la directive 2002/21/CE³⁵.

60. La fourniture d'accès à l'Internet est un service de communications électroniques accessible au public au sens de l'article 2, sous c), de la directive 2002/21, c'est-à-dire un service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

61. Communiquer à quels utilisateurs certaines adresses IP ont été attribuées à des moments précis implique la communication de données à caractère personnel au sens de

33 — Ibidem, points 46 et suiv.

34 — En ce qui concerne le secret des communications téléphoniques, le Bundesverfassungsgericht présuppose même une obligation de protection correspondante à charge de l'État dans ses arrêts du 9 octobre 2002 [1 BvR 1611/96 et 1 BvR 805/98, BVerfGE 106, 28 (37), point 21 de la version figurant à l'adresse www.bundesverfassungsgericht.de] et du 27 octobre 2006 [12 BvR 1811/99, Multimedia und Recht 2007, 308, point 13, de la version figurant à l'adresse www.bundesverfassungsgericht.de]. Il n'y a cependant pas lieu de trancher dans la présente affaire la question de savoir si les obligations relevant du droit de la protection des données des personnes privées reposent en droit communautaire également sur une obligation de protection impérative de la Communauté.

35 — Directive du Parlement européen et du Conseil, du 7 mars 2002, relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre») (JO L 108, p. 33).

l'article 2, sous a), de la directive 95/46, à savoir la divulgation d'informations sur des personnes physiques identifiées ou identifiables³⁶. Grâce à ces données, les opérations réalisées pourront être reliées au titulaire de la connexion en utilisant l'adresse IP correspondante.

l'acheminement d'une communication par un réseau de communications électroniques.

62. La communication de pareilles données est expressément citée comme exemple d'un traitement de données à caractère personnel à l'article 2, sous b), de la directive 95/46, c'est-à-dire comme exemple d'une opération effectuée ou non à l'aide de procédés automatisés.

63. En même temps, les adresses IP des utilisateurs, à tout le moins celles qui leur sont attribuées provisoirement, sont des données relatives au trafic au sens de l'article 2, sous b), de la directive 2002/58, à savoir des données traitées en vue de

3. Sur les interdictions de traitement applicables

64. Conformément à l'article 5, paragraphe 1, de la directive 2002/58, la confidentialité des communications s'étend également aux données relatives au trafic y afférentes. Les États membres doivent, en particulier, interdire à toute autre personne que les utilisateurs de stocker ces données sans le consentement des utilisateurs concernés, sauf lorsque cette personne y est légalement autorisée conformément à l'article 15, paragraphe 1.

65. L'article 6, paragraphe 1, de la directive 2002/58 indique clairement, en ce qui concerne les données relatives au trafic stockées par les exploitants de réseaux de communications, que ces données relatives au trafic concernant les abonnés et les utilisateurs traités et stockés par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, sans préjudice des paragraphes 2, 3 et 5 de cet article ainsi que de l'article 15, paragraphe 1.

36 — Dans la mesure où les titulaires des adresses IP peuvent être identifiés en raison du fait que le fournisseur d'accès à l'Internet a enregistré l'attribution qui leur en avait été faite, il s'agit d'ailleurs déjà, lorsque Promusicae intercepte les adresses IP, du traitement de données à caractère personnel, c'est-à-dire d'une opération qui doit être conforme aux exigences du droit de la protection des données; voir l'arrêt du Rechtbank d'Utrecht du 12 juillet 2005, Brein (194741/KGZA 05-462, annexe 5 aux observations de Promusicae, points 4.24 et suiv.), le document de travail WP 104 du groupe de travail sur la protection des données du 18 janvier 2005, document intitulé «Les questions de protection des données liées aux droits de propriété intellectuelle», p. 4, ainsi que, en ce qui concerne le droit français, les décisions (délibérations) de la commission nationale de l'informatique et des libertés (CNIL) 2005-235 du 18 octobre 2005 et 2006-294 du 21 décembre 2006 (à consulter sur <http://www.legifrance.gouv.fr/WAspad/RechercheExperteCnil.jsp>). Dans le registre des opérations de traitement déclarées de l'Agencia Española de Protección de Datos, <https://www.agpd.es/index.php?idSeccion=100> se trouve une déclaration correspondante de Promusicae.

66. Aussi bien le stockage que la communication de données à caractère personnel relatives au trafic concernant l'utilisation de l'Internet doivent dès lors être foncièrement interdits.

4. Sur les exceptions aux interdictions de traitement

67. Ces interdictions de traitement connaissent néanmoins un certain nombre d'exceptions, qui sont énoncées aux articles 6 et 15 de la directive 2002/58.

a) Sur les exceptions prévues à l'article 6, paragraphes 2, 3 et 5, de la directive 2002/58

68. Les paragraphes 2, 3 et 5 de l'article 6 de la directive 2002/58, que le paragraphe 1 du même article désigne expressément comme étant des exceptions, ne sont pas une base appropriée qui permettrait d'enfreindre l'interdiction de traitement faite par ce paragraphe 1 en communiquant à Promusicæ les données qu'elle sollicite.

69. L'article 6, paragraphe 2, de la directive 2002/58 autorise à titre de dérogation le

traitement des données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion. Il paraît déjà douteux que cette exception permette d'enregistrer les coordonnées des utilisateurs auxquels une adresse IP dynamique a été attribuée et à quel moment elle l'a été. Il n'est normalement pas nécessaire de disposer de pareilles informations pour pouvoir calculer les redevances dues au fournisseur d'accès. Les procédures habituelles de facturation sont fondées sur la durée de la connexion sur le fournisseur d'accès ou sur le volume d'échange de données produit par l'utilisateur, sans préjudice des hypothèses dans lesquelles le contrat entre l'abonné et celui-ci prévoit une utilisation illimitée de l'accès pour un montant forfaitaire. Or, s'il n'est pas nécessaire d'utiliser l'adresse IP pour établir les factures, il n'est donc pas licite de l'enregistrer³⁷.

70. Indépendamment de cela, l'article 6, paragraphe 2, n'est en tout cas pas une base appropriée autorisant à communiquer des données relatives au trafic à des tiers souhaitant tenter une action à l'encontre de l'utilisateur pour certaines opérations qu'il a réalisées en utilisant cette adresse IP. De telles poursuites ne présentent aucun rapport avec l'établissement de factures ou le paiement d'interconnexions.

37 — Voir, en ce sens, point 2.8. de la position du groupe de protection des données à propos du stockage des données relatives au trafic à des fins de facturation, WP 69 du 29 janvier 2003.

71. La dérogation prévue à l'article 6, paragraphe 3, de la directive 2002/58 n'est pas davantage pertinente. Elle n'autorise le fournisseur d'accès à utiliser les données pour commercialiser ses services de communications électroniques ou fournir des services à valeur ajoutée qu'à la condition qu'il obtienne préalablement l'autorisation de l'utilisateur.

72. Enfin, Promusicae ne peut pas davantage se prévaloir de l'article 6, paragraphe 5, de la directive 2002/58, qui autorise des tiers agissant sous l'autorité des fournisseurs de réseaux publics à utiliser des données relatives au trafic à certaines fins, en particulier lorsqu'il s'agit de détecter les fraudes. Le vingt-neuvième considérant de la directive précise, à ce sujet, que les pratiques frauduleuses en question consistent à utiliser le service de communications électroniques sans le payer. Or, Promusicae n'agit pas sous l'autorité de Telefónica et la violation de droits d'auteur n'est pas une pratique frauduleuse au sens de cette disposition.

b) Sur l'article 6, paragraphe 6, de la directive 2002/58

73. Promusicae considère que l'article 6, paragraphe 6, de la directive 2002/58 autorise la communication et l'utilisation de données relatives au trafic lorsqu'il s'agit d'engager les actions de droit civil permet-

tant d'obtenir le respect des droits d'auteur. Aux termes de cette disposition, les organes compétents peuvent se faire communiquer des données relatives au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation.

74. Promusicae ne peut pas s'autoriser de cette disposition pour obtenir la communication de données relatives au trafic au simple motif déjà qu'elle n'est pas un organe compétent pour le règlement de litiges. On ne voit guère non plus en quoi il serait nécessaire de communiquer les données relatives au trafic litigieuses à la juridiction de renvoi pour lui permettre de régler le litige qui oppose Promusicae à Telefónica. Pour trancher la question de savoir si Telefónica a le droit et est tenue de communiquer ces données à Promusicae, cette juridiction n'a pas besoin d'en avoir connaissance.

75. Le fait que Promusicae exige la communication des données relatives au trafic pour pouvoir engager des poursuites contre les utilisateurs indéliçats n'est pas davantage un motif d'autoriser leur communication sur la base de l'article 6, paragraphe 6, de la directive 2002/58.

76. Il serait incompatible avec la prévisibilité qui doit être assurée en cas de justification légale d'ingérences dans la vie privée ou

d'atteintes à la protection des données d'interpréter l'article 6, paragraphe 6, de la directive 2002/58 en ce sens que le but d'utiliser des données relatives au trafic en vue d'engager des poursuites légales autorise, à lui seul, leur communication à la partie adverse parce qu'une telle interprétation n'est pas suffisamment étayée par le libellé de cette disposition et ajouterait une nouvelle dérogation, pratiquement illimitée, à celles qui sont prévues à l'article 6, paragraphes 2, 3 et 5, ainsi qu'à l'article 15, paragraphe 1, dérogations qui sont expressément visées et délimitées de manière relativement claire par l'article 6, paragraphe 1³⁸. Le libellé de l'article 6 n'indique pas à l'utilisateur de services de communications électroniques la nouvelle dérogation qui s'ajouterait ainsi.

77. Cette exception irait en outre très loin et ne pourrait dès lors pas être considérée comme proportionnée par rapport aux objectifs poursuivis. L'utilisateur devrait en principe toujours — et pas seulement en cas de violation de droits d'auteur — s'attendre à ce que les données relatives à ses connexions soient communiquées à des tiers qui, pour quelque motif que ce soit, entendraient engager des poursuites à son encontre. Il est exclu que des litiges de cet ordre soient fondés sur un besoin social impérieux au sens de l'article 8 de la CEDH tel qu'il a été interprété par la Cour³⁹.

78. Si l'on analyse les motifs pour lesquels l'article 6 de la directive 2002/58 autorise le stockage des données relatives au trafic, il se dégage de ceux-ci un argument encore plus convaincant en faveur d'une restriction de la divulgation de ces données. Selon l'article 6, paragraphe 1, sous b), de la directive 95/46, seuls les motifs de stockage prévus justifient leur divulgation. Dans le cas des données relatives au trafic, ces motifs sont, conformément à l'article 6 de la directive 2002/58, la gestion du réseau de communications, l'établissement des factures et, lorsque l'utilisateur y consent, la commercialisation des services ou la fourniture de services à valeur ajoutée ou encore — ce qui va plus loin — le traitement de ces données sous l'autorité des fournisseurs en vue de répondre aux demandes de la clientèle ou de détecter des fraudes au sens évoqué plus haut⁴⁰. La solution des conflits n'est pas un motif autonome de stockage de données relatives au trafic, mais permet uniquement aux organes compétents d'en prendre connaissance. Il ne peut donc s'agir que de litiges qui ont trait aux motifs pour lesquels des données peuvent être stockées⁴¹. Constituer des preuves en vue d'éventuelles poursuites légales engagées par des tiers n'est cependant pas un motif de stockage susceptible d'être reconnu.

79. Dans ces conditions, la communication à Promusicae des données relatives au trafic

38 — Voir les conclusions que j'ai présentées le 29 janvier 2004 dans l'affaire Commission/Pays-Bas (arrêt du 24 juin 2004, C-350/02, Rec. p. I-6213), point 71, à propos de l'interprétation de l'article 6, paragraphe 4, de la directive 97/66.

39 — Voir le point 54 plus haut avec les notes y afférentes.

40 — Voir le point 72 plus haut.

41 — Dans cette mesure-là, l'exposé que j'ai fait dans un autre contexte à propos du «polymorphisme des litiges» dans les conclusions que j'ai présentées dans l'affaire Commission/Pays-Bas (citées à la note 38, point 81) ne doit pas être interprété de manière excessive.

qu'elle sollicite ne peut pas être fondée sur l'article 6, paragraphe 6, de la directive 2002/58.

sécurité publique et de la défense nationale. La loi précise formellement qu'elles ne peuvent pas être communiquées à d'autres fins.

c) Sur l'article 15, paragraphe 1, de la directive 2002/58

80. L'article 15, paragraphe 1, de la directive 2002/58 permet, lui aussi, de restreindre les droits résultant de l'article 6, paragraphe 1. Aux termes de l'article 13, paragraphe 1, de la directive 95/46, une telle limitation doit être nécessaire à la sauvegarde de la sûreté de l'État, à la défense nationale, à la sécurité publique ainsi qu'à la prévention, à la recherche, à la détection et à la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques dans une société démocratique, et elle doit en outre être appropriée et proportionnée.

81. Le Royaume d'Espagne s'est autorisé de ces dispositions dérogatoires pour imposer aux fournisseurs d'accès, à l'article 12, paragraphe 1, de la loi n° 34/2002, l'obligation de conserver les données relatives au trafic et aux connexions. La divulgation de celles-ci est cependant expressément limitée au cadre des enquêtes pénales, de la protection de la

82. L'on peut légitimement douter qu'il soit compatible avec les droits fondamentaux⁴² de stocker les données relatives au trafic de tous les utilisateurs, c'est-à-dire, en somme, de les conserver en vue d'une utilisation ultérieure, même en l'absence de tout soupçon concret⁴³. Étant donné que la réglementation espagnole est en tout cas compatible avec le libellé de l'article 15, paragraphe 1, de la directive 2002/58, le stockage préventif peut être présumé conforme, du moins pour les besoins de la présente espèce⁴⁴. Par contre, se référer ainsi aux droits fondamentaux irait au-delà du cadre fixé par la présente demande préjudicielle, qui ne concerne pas la validité de l'article 15, paragraphe 1. Par conséquent, il est permis de supposer que le stockage est licite, du moins aux fins de la présente

42 — Voir la position 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 [COM(2005) 438 final, JO 2005, C 298, p. 1], ainsi que les positions du groupe de protection des données du 21 octobre 2005, 4/2005 sur la proposition de directive et du 25 mars 2006, 3/2006 sur la directive 2006/24.

43 — Le Bundesverfassungsgericht estime que de telles ingérences dans la vie privée sont particulièrement graves, parce que l'individu ne présente aucune caractéristique justifiant une telle ingérence et parce que, bien qu'il se comporte de manière légale, il peut être intimidé en raison des risques d'utilisation abusive et en raison du sentiment d'être surveillé; voir arrêt du 4 avril 2006 sur les méthodes de recherche par recoupement à l'aide de banques de données [1 BvR 518/02, *Neue Juristische Wochenschrift* 2006, 1939 (1944), point 117 de la version disponible sur www.bundesverfassungsgericht.de].

44 — Voir arrêt du 11 novembre 1997, Eurotunnel e.a. (C-408/95, Rec. p. I-6315, points 33 et suiv.).

procédure. Il conviendra peut-être un jour de réexaminer cette question à propos de la directive 2006/24, qui introduit une obligation de stockage dans le droit communautaire⁴⁵. Dans l'hypothèse où la Cour estimerait néanmoins utile d'examiner la compatibilité du stockage à titre de question préliminaire dans la présente affaire déjà, il serait alors certainement nécessaire d'ordonner la réouverture de la procédure orale afin de permettre aux parties de présenter leurs observations sur ce point conformément à l'article 23 du statut de la Cour.

83. Si l'on va au fond des choses, la question qui se pose ici est cependant celle de savoir si l'article 15, paragraphe 1, de la directive 2002/58 permet de fournir à Promusicae les données dont elle demande la communication — et qui ont été stockées, car, dans l'hypothèse où le droit de la protection des données autoriserait une telle communication, il faudrait encore vérifier si les directives citées par la juridiction de renvoi — et la propriété des titulaires de droits d'auteur qui est protégée dans ce cadre — exigent que l'on fasse usage de cette possibilité. En pareil cas, les juridictions espagnoles seraient tenues d'utiliser les éventuelles marges d'interprétation disponibles en vue de permettre cette communication⁴⁶.

45 — L'Irlande a engagé contre le Conseil et le Parlement un recours qui est toujours pendant devant la Cour (affaire C-301/06, communication au JO 2006, C 237, p. 5). Elle demande l'annulation de la directive 2006/24, au motif qu'elle serait fondée sur une base juridique incorrecte. Pour le surplus, le recours ne porte pas sur la question de savoir si le stockage des données est compatible avec les droits fondamentaux.

46 — Voir arrêt Lindqvist (déjà cité à la note 32, point 87).

84. L'article 15, paragraphe 1, de la directive 2002/58 énonce expressément des motifs de dérogation de deux types, à savoir, d'une part, parmi les quatre premiers cas qu'il prévoit, la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense nationale et la sécurité publique ainsi que la prévention, la recherche, la détection et la poursuite d'infractions pénales et, d'autre part, la prévention, la recherche, la détection et la poursuite d'utilisations non autorisées du système de communications électroniques. De surcroît, l'article 15, paragraphe 1, de la directive 2002/58 renvoie à l'article 13, paragraphe 1, de la directive 95/46, qui contient d'autres motifs de dérogation.

Sur l'article 15, paragraphe 1, de la directive 2002/58 lu en combinaison avec l'article 13, paragraphe 1, sous g), de la directive 95/46

85. Une première base permettant de divulguer les données en cause pourrait résulter des dispositions combinées de l'article 15, paragraphe 1, de la directive 2002/58 et de l'article 13, paragraphe 1, sous g), de la directive 95/46. L'article 13, paragraphe 1, sous g), de la directive 95/46 permet de communiquer des données à caractère personnel lorsqu'il s'agit de protéger des droits et des libertés d'autrui. Contrairement à d'autres motifs d'exception qui figurent à l'article 13, paragraphe 1, de la directive 95/46, l'article 15, paragraphe 1, de la

directive 2002/58 ne reprend certes pas ces motifs expressément, mais il autorise, dans sa version allemande, certaines restrictions «conformément à l'article 13, paragraphe 1, de la directive 95/46».

86. Si l'on examine ce passage de la version allemande isolément, il pourrait être interprété comme un renvoi à *tous* les motifs d'exception qui figurent à l'article 13, paragraphe 1, de la directive 95/46⁴⁷. Le fait que l'article 15, paragraphe 1, de la directive 2002/58 énonce lui-même des motifs de dérogation qui autorisent une limitation «conformément à l'article 13, paragraphe 1, de la directive 95/46» s'oppose néanmoins déjà à une telle interprétation. Ces motifs ne correspondent que partiellement à ceux qui sont énoncés à l'article 13, paragraphe 1, de la directive 95/46 et ne contiennent pas l'exception en faveur de la protection des droits d'autrui qui figure au point g) de celui-ci. C'est pourquoi les motifs énoncés à l'article 13, paragraphe 1, de la directive 95/46 ne valent dans le domaine des communications électroniques que dans la mesure où ils sont expressément repris à l'article 15, paragraphe 1, de la directive 2002/58.

87. Cette réglementation résulte plus clairement des versions linguistiques autres que de

la version allemande. À l'ambiguïté du «gemäß» allemand, elles ont préféré une forme telle que «comme le prévoit l'article 13, paragraphe 1, de la directive 95/46»⁴⁸. Une telle rédaction repose sur une décision délibérée qui a été prise au cours du processus législatif. En effet, lors de la première adoption de cette réglementation — il s'agissait alors de la directive 97/66 —, le Conseil a, comme l'indique la Commission, renoncé à reprendre globalement les motifs dérogatoires énumérés à l'article 13, paragraphe 1, de la directive 95/46 et a opté plutôt pour la réglementation différenciée qui nous est parvenue aujourd'hui⁴⁹.

88. La spécialité de l'article 15, paragraphe 1, de la directive 2002/58 par rapport à l'article 13, paragraphe 1, de la directive 95/46 milite également en faveur d'une telle solution⁵⁰. Ce dernier s'applique à toutes les données à caractère personnel, indépendamment du point de savoir dans quel contexte elles sont recueillies. Il garde ainsi une portée relativement générale puisqu'il peut s'appliquer à de nombreuses situations très différentes⁵¹. Le premier de ces deux articles, en

47 — C'est ainsi que, dans «Auskunftsansprüche gegenüber Internetzugangspornidern 'vor' dem 2. Korb und 'nach' der Enforcement-Richtlinie der EU», *Multimedia und Recht* 2004, p. 514 (517 et suiv.), Christian Cychowski considère que la transposition allemande de cette règle dérogatoire permet de communiquer aux titulaires de droits d'auteur les données relatives au trafic de quiconque aurait violé ces droits.

48 — C'est ainsi que l'on peut lire dans la version française «comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE», dans la version anglaise «as referred to in Article 13(1) of Directive 95/46/CE» et dans la version espagnole «a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE», chaque fois après une énumération des différents motifs de justification licites.

49 — Voir note 6 des observations de la Commission.

50 — Sieber, U., et Höfiger, F. M., «Drittauskunftsansprüche nach §101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen», *Multimedia und Recht* 2004, p. 575 (582), et Spindler, G., et Dorschel, J., «Auskunftsansprüche gegen Internet-Service-Provider», *Computer und Recht* 2005, p. 38 (45 et suiv.).

51 — Voir, en ce sens, arrêt Lindqvist (déjà cité à la note 32, point 83).

revanche, vise concrètement les données à caractère personnel qui sont réunies dans le cadre des communications électroniques et repose dès lors sur une estimation comparativement précise de l'intensité avec laquelle une communication de données à caractère personnel relatives au trafic porte atteinte au droit fondamental à la protection des données.

89. Par conséquent, la protection des droits et des libertés d'autrui que prévoit l'article 13, paragraphe 1, sous g), de la directive 95/46 ne peut pas justifier la communication de données à caractère personnel relatives au trafic.

Sur l'usage non autorisé du système de communications électroniques

90. Par ailleurs, il faut examiner si l'utilisation non autorisée du système de communications électroniques, qui est le cinquième cas prévu à l'article 15, paragraphe 1, de la directive 2002/58, peut justifier une communication des données à caractère personnel.

91. La notion d'utilisation non autorisée du système de communications électroniques permet en substance deux interprétations en ce qui concerne le type de comportement couvert, à savoir l'utilisation à des fins

illicites ou l'utilisation non conforme au système. S'il est évident que la violation des droits d'auteur est une fin illicite, elle peut néanmoins être commise au moyen d'une utilisation du système conforme à sa destination, à savoir le chargement de données en provenance d'autres ordinateurs connectés à l'Internet. Il n'est pas nécessaire, pour se rendre coupable d'une telle violation, de manipuler le système de communications — d'une manière incompatible avec lui — en se procurant, par exemple, les mots de passe d'ordinateurs appartenant à autrui ou en lui déclinant une fausse identité⁵².

92. Selon la Commission, l'article 15, paragraphe 1, de la directive 2002/58 vise l'utilisation non conforme au système qui met en danger son intégrité ou sa sécurité, comme le démontrerait également l'historique de cette disposition, puisque cette notion a été introduite dans la directive 97/66 afin de garantir l'utilisation correcte de la fréquence.

93. Cette interprétation stricte de la notion d'utilisation non autorisée correspond à la confidentialité des communications qui est protégée par l'article 5 de la direc-

52 — Les actes décrits comme des infractions pénales punissables par la décision-cadre 2005/222/JAI du Conseil, du 24 février 2005, relative aux attaques visant les systèmes d'information (JO L 69, p. 67) seront généralement constitutifs d'une utilisation non conforme au système.

tive 2002/58. Il n'est généralement possible de constater que le système a été utilisé à des fins illicites qu'en surveillant le contenu des communications.

94. S'il est vrai que l'article 15, paragraphe 1, permet également de déroger à la confidentialité des communications, il est tout aussi exact que les autres motifs d'exception expressément énoncés seraient superflus et largement privés de leur effet utile puisque les atteintes à la sécurité nationale, à la défense nationale ou à la sécurité publique sont généralement assorties d'une intention illicite, comme le sont les infractions pénales commises au moyen de systèmes de communications électroniques.

95. Par ailleurs, une exception d'interprétation large en faveur de la communication à des fins illicites pourrait s'avérer assez imprévisible dans son application, de sorte qu'une telle exception viderait largement le droit à la protection des données à caractère personnel de son contenu.

96. Non seulement le nombre des opérations de communication illicites au regard du droit pénal est relativement élevé, mais, de surcroît, la communication peut également entrer en conflit avec des obligations résultant de certaines relations juridiques et que le droit pénal ne sanctionne pas, comme, par exemple, des obligations découlant de la relation de travail ou des obligations familiales. Le fournisseur du service de communication électronique pourrait même réprimer la consultation de certains sites ou la propagation de leur contenu. Il serait ainsi à peine possible de délimiter, parmi ces relations juridiques, celles qui pourraient permettre le stockage et la divulgation de données relatives au trafic ou peut-être même de contenus de communications. C'est la raison pour laquelle ce motif de restriction pris dans une acception large ne serait pas compatible avec l'exigence de prévisibilité.

97. À cela s'ajoute le fait qu'une interprétation large réduirait à peu de choses la protection des données à caractère personnel, tout comme, d'ailleurs, la protection de la confidentialité des communications. Pour pouvoir vérifier efficacement si les systèmes de communications électroniques sont utilisés à des fins illicites, il faudrait enregistrer l'ensemble des communications et les analyser en profondeur afin de contrôler leurs contenus. Le citoyen «de verre» serait ainsi une réalité.

98. C'est la raison pour laquelle il convient de préférer l'interprétation proposée par la Commission. Par conséquent, la notion d'utilisation non autorisée du système de communications électroniques ne vise que

l'utilisation non conforme au système, mais n'englobe pas l'utilisation à des fins illicites.

Sur les motifs d'exception des quatre premiers cas visés à l'article 15, paragraphe 1, de la directive 2002/58>

99. Il ne reste donc plus, comme base permettant de justifier la communication des données de connexion, que les quatre premiers cas énoncés à l'article 15, paragraphe 1, de la directive 2002/58, en particulier la prévention, la recherche, la détection et la poursuite d'infractions pénales ainsi que la sauvegarde de la sécurité publique.

100. Ces quatre premiers cas prévus à l'article 15, paragraphe 1, sont explicités dans le onzième considérant de l'exposé des motifs de la directive 2002/58, aux termes duquel celle-ci ne s'applique pas aux domaines qui ne sont pas régis par le droit communautaire, de sorte qu'elle ne modifie pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles qui sont visées à l'article 15, paragraphe 1, nécessaires à la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal.

101. La Cour a déjà précisé que les activités en cause sont des activités propres aux États et aux autorités étatiques⁵³. Si les autorités étatiques peuvent contraindre des opérateurs privés à leur apporter leur soutien⁵⁴, les poursuites que ceux-ci pourraient engager de leur propre chef à l'encontre de violations du droit ne relèvent plus de ces exceptions. Pour cette simple raison déjà, les quatre premiers cas visés à l'article 15, paragraphe 1, de la directive 2002/58 n'autorisent à communiquer des données de connexion qu'aux autorités publiques, mais pas directement à Promusicæ⁵⁵.

102. Il est également fort peu probable qu'il soit possible, en l'espèce, de communiquer des données à caractère personnel à des autorités étatiques en application du quatrième cas prévu à l'article 15, paragraphe 1, de la directive 2002/58, c'est-à-dire en vue

53 — Arrêt Lindqvist (déjà cité à la note 32, point 43).

54 — Arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, Rec. p. I-4721, point 58).

55 — Selon les indications fournies par Promusicæ, le résultat auquel on parvient ainsi pour le troisième et le quatrième cas prévus à l'article 15, paragraphe 1, de la directive 2002/58 correspond à la situation juridique en France, en Italie et en Belgique, où la législation permettrait aux autorités publiques compétentes d'exiger que les données à caractère personnel relatives au trafic leur soient communiquées. Dans son document de travail WP 104 (déjà cité à la note 35, p. 4), le groupe de protection des données va encore plus loin et limite aux autorités pénales la possibilité de communiquer des données à caractère personnel: «sur la base du principe de compatibilité et en conformité avec le principe de confidentialité établi dans les directives 2002/58/CE et 95/46/CE, les données détenues par les fournisseurs d'accès à Internet pour des finalités spécifiques, incluant principalement la prestation d'un service de télécommunication, ne peuvent pas être transférées à des tiers, tels que les détenteurs de droits, hormis, dans des circonstances définies prévues par la loi, à des autorités judiciaires publiques».

d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales. Comme la Commission l'explique à bon droit, une telle communication présuppose-rail que les violations du droit d'auteur alléguées par Promusicae doivent en même temps être considérées comme des infractions pénales.

103. Une sanction pénale n'est pas exclue en droit communautaire dès lors que, comme on peut le voir également à l'article 8, paragraphe 1, de la directive 2001/29 et à l'article 16 de la directive 2004/48, c'est au législateur national qu'il appartient de décider si et sous quelle forme des violations du droit d'auteur doivent être sanctionnées. Il lui est donc loisible de punir l'éventuelle violation de droits d'auteur qui serait commise grâce à l'échange de fichiers. Selon les indications fournies par la juridiction de renvoi, le caractère punissable de tels actes en Espagne présuppose néanmoins que le contrevenant ait agi dans un but de lucre⁵⁶. Or, aucun élément permettant de conclure à de telles visées lucratives n'a encore été exposé jusqu'à présent.

104. Il nous faut encore examiner le troisième cas prévu parmi les exceptions énu-

mérées à l'article 15, paragraphe 1, de la directive 2002/58, à savoir la sauvegarde de la sécurité publique. Conformément à la jurisprudence relative aux libertés fondamentales, l'ordre public et la sécurité publique ne peuvent être invoqués qu'en cas de menace réelle et suffisamment grave, affectant un intérêt fondamental de la société⁵⁷.

105. La protection des droits d'auteur est un intérêt social dont la Communauté, notamment, a itérativement souligné l'importance. C'est la raison pour laquelle cet objectif peut être reconnu comme un intérêt fondamental de la société, même lorsque l'intérêt du titulaire du droit n'est pas de nature foncièrement publique, mais bien de nature privée. Le «filesharing» illégal compromet d'ailleurs effectivement la protection des droits d'auteur.

106. Toutefois, il n'est en tout cas pas certain que le partage de fichiers entre personnes privées, en particulier lorsque celles-ci agissent sans but lucratif, compromette la protection des droits d'auteur d'une manière à ce point grave qu'elle justifierait l'application de cette exception. La mesure dans laquelle le partage de fichiers entre personnes privées entraîne un véritable

57 — Voir, par exemple, arrêts du 29 avril 2004, Orfanopoulos et Oliveri (C-482/01 et C-493/01, Rec. p. I-5257, point 66), à propos de la libre circulation, et du 14 mars 2000, Église de scientologie (C-54/99, Rec. p. I-1335, point 17), à propos de la libre circulation des capitaux.

56 — Voir le point 28 plus haut.

préjudice demeure, en effet, une question controversée⁵⁸.

107. Sans préjudice d'un contrôle par la Cour, c'est au législateur qu'il conviendrait de laisser le soin d'apprécier si tel est le cas. En particulier, lorsque les États membres frappent d'une sanction pénale la violation de droits d'auteur par l'échange de fichiers entre particuliers, ils portent une appréciation de ce type, mais, en pareil cas, le quatrième cas prévu à l'article 15, paragraphe 1, de la directive 2002/58 s'applique, de sorte qu'il n'est pas nécessaire d'invoquer la sécurité publique.

108. Le caractère punissable serait, sans doute, un indice important d'une menace suffisamment grave pour la protection des droits d'auteur, mais le droit pénal n'est pas nécessairement la seule forme sous laquelle le législateur peut exprimer sa réprobation. Il peut bien mieux mettre en œuvre son jugement de valeur en prévoyant d'abord la communication de données à caractère personnel relatives au trafic uniquement en vue de permettre des poursuites civiles, à condition, bien entendu, que la protection des données ne s'en trouve pas restreinte en raison de l'éventuelle violation de droits d'auteur dans des cas bénins.

109. Conformément au principe de prévisibilité et au principe du droit de la protection des données conformément auxquels toute mesure doit être conforme à l'objectif poursuivi, une telle réglementation doit exprimer de manière suffisamment claire que les fournisseurs d'accès à l'Internet enregistrent et communiquent les données à caractère personnel relatives au trafic également en vue de protéger les droits d'auteur. Dès lors que cet enregistrement et cette communication reposent sur la troisième possibilité prévue à l'article 15, paragraphe 1, de la directive 2002/58, il faudrait également tenir compte du fait que la protection de la sécurité publique est une mission des autorités étatiques et que, partant, les données relatives au trafic ne peuvent pas être révélées aux titulaires privés de droits sans une participation de ces autorités, par exemple les juridictions ou les autorités de contrôle chargées de l'application du droit de la protection des données.

110. En tout cas, le *législateur communautaire* n'a encore à ce jour pris aucune décision correspondante qui limiterait la protection des données de manière à permettre de poursuivre les violations du droit d'auteur. En particulier, les directives citées par la juridiction de renvoi ne sont pas pertinentes en la matière puisque, comme je l'ai déjà dit⁵⁹, elles ne touchent pas à la protection des données. Cela vaut, en

58 — Voir le rapport DSTI/ICCP/IE(2004)12/FINAL du 13 décembre 2005 (<http://www.oecd.org/dataoecd/13/2/34995041.pdf>, p. 76 et suiv.) au groupe de travail sur l'économie de l'information de l'Organisation de coopération et de développement économiques (OCDE).

59 — Voir les points 41 et suivants plus haut.

particulier, pour le droit d'information prévu à l'article 8 de la directive 2004/48, dont les termes pourraient également couvrir la révélation de l'identité d'utilisateurs de l'Internet. Selon son paragraphe 3, sous e), cette disposition s'applique sans préjudice d'autres dispositions législatives et réglementaires qui régissent le traitement des données à caractère personnel.

111. Il ne serait donc pas conforme au principe de prévisibilité de déduire de ces directives une disposition finaliste d'enregistrement des données relatives au trafic qui n'y figure pas, alors que l'article 6, paragraphe 1, sous b), de la directive 95/46 impose que toute collecte de données soit liée à des fins déterminées⁶⁰. Les directives ne contiennent pas davantage la moindre indication concernant une participation d'autorités étatiques à la communication de données à caractère personnel à des titulaires privés de droits.

112. Cependant, dans l'état actuel du droit communautaire, les troisième et quatrième cas prévus à l'article 15, paragraphe 1, de la directive 2002/58 permettent, en tout cas, aux *États membres* de disposer que des données à caractère personnel relatives au

trafic soient communiquées à des autorités étatiques de manière à permettre de poursuivre les violations des droits d'auteur par le partage de fichiers aussi bien en application des règles du droit pénal qu'en application des règles du droit civil. Les États membres ne sont cependant pas tenus de le faire.

113. Par rapport à la communication directe de données à caractère personnel relatives au trafic aux titulaires de droits lésés, une telle solution serait plus modérée dans la constellation qui nous occupe en l'espèce et garantirait, en même temps, que la communication demeure dans de justes proportions par rapport aux positions juridiques protégées.

114. L'implication d'autorités étatiques est une solution plus modérée parce que, contrairement aux particuliers, elles sont directement tenues par les droits fondamentaux. Elles doivent, en particulier, respecter les garanties de procédure. De surcroît, elles tiennent généralement compte également de circonstances qui exonèrent l'utilisateur accusé d'avoir enfreint des droits d'auteur.

115. C'est ainsi que le fait que des droits d'auteur aient été enfreints à un moment

60 — Voir le point 53 plus haut.

déterminé sous une adresse IP ne permet pas encore d'affirmer de manière incontestable que c'est le titulaire de la connexion auquel cette adresse aurait été attribuée à ce moment-là qui se serait rendu coupable de ces actes. Au contraire, il est également possible que d'autres personnes aient utilisé sa connexion ou son ordinateur, ce qui peut même avoir été le cas sans qu'il en ait eu connaissance, par exemple, lorsqu'il utilise un réseau local insuffisamment sécurisé pour éviter les liaisons par câble⁶¹ ou lorsque son ordinateur a été «piraté» par des tiers sur l'Internet.

116. Contrairement aux autorités étatiques, les titulaires de droits d'auteur n'auront aucun intérêt à tenir compte de pareilles circonstances ou à les élucider.

117. Impliquer les autorités étatiques permet également de mieux garantir le caractère

proportionné de la communication de données à caractère personnel relatives au trafic.

118. Le législateur ne prévoira leur intervention que dans les cas où il soupçonne de manière suffisamment fondée l'existence d'une violation du droit. Il dispose en cela d'un large pouvoir d'appréciation et d'aménagement. Si l'article 8, paragraphe 1, de la directive 2001/29 et l'article 16 de la directive 2004/48 disposent que les sanctions doivent être appropriées, efficaces, proportionnées et dissuasives, il n'en faut pas moins tenir compte également de l'importance de la violation des droits d'auteur qui aurait été commise.

119. Par conséquent, la possibilité de communiquer des données à caractère personnel relatives au trafic peut être limitée à des cas particulièrement graves, comme, par exemple, aux actes commis dans un but lucratif, c'est-à-dire à une utilisation illégale d'œuvres protégées qui porte lourdement atteinte à leur utilisation économique par le titulaire du droit. Le neuvième considérant de l'exposé des motifs de la directive 2004/48 montre, lui aussi, que les mesures visant à protéger les droits d'auteur contre les atteintes dont ils peuvent faire l'objet sur l'Internet doivent précisément viser les atteintes graves. S'il mentionne la distribu-

61 — Voir document de travail de l'International Working Group on Data Protection in Telecommunications du 15 avril 2004 sur les risques potentiels des réseaux sans fil, document qui peut être consulté en anglais et en allemand sous <http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm>. Selon Dörhöfer, S., *Empirische Untersuchungen zur WLAN-Sicherheit mittels Wardriving*, <https://pil-old.informatik.uni-mannheim.de.8443/pub/research/theses/diplomarbeit-2006-doe-rhoefer-pdf>, p. 98, pratiquement 23 % de tous les réseaux n'étaient absolument pas sécurisés en Allemagne au moment de l'enquête et 60 % environ l'étaient insuffisamment. Sur les méthodes de partage, voir Tews, E., Weinmann, R.-P., et Pyskin, A., *Breaking 104 bit WEP in less than 60 seconds*, <http://eprint.iacr.org/2007/120.pdf>.

tion de produits piratés sur l'Internet, comme le gouvernement du Royaume-Uni le fait observer à bon escient, il la situe néanmoins dans le contexte de la criminalité organisée.

ou ne soient tout simplement pas disponibles.

120. Les droits fondamentaux à la propriété et à une protection juridique effective ne mettent pas en cause cette appréciation du caractère proportionné. Les droits fondamentaux imposent certainement de donner aux titulaires de droits d'auteur la possibilité de se défendre en justice contre les violations de ceux-ci. Contrairement à l'affaire *Moldovan e.a. c. Roumanie*⁶², citée par *Promusicae*, la présente affaire ne porte pas sur la question de savoir si une voie de recours est ouverte ou non, mais bien sur les moyens qui sont mis à la disposition des titulaires de droits pour leur permettre de démontrer l'existence d'une violation.

121. Dans cette mesure-là, l'obligation de protéger les titulaires de droits d'auteur qui incombe à l'État n'est pas telle qu'elle lui imposerait de mettre à leur disposition des moyens illimités lui permettant d'élucider les violations de ceux-ci. Au contraire, rien ne s'oppose à ce que certains droits d'investigation soient réservés aux autorités publiques

5. Sur la directive 2006/24

122. La directive 2006/24 ne permet pas d'aboutir à un résultat différent dans la présente espèce. S'il est vrai que, conformément à celle-ci, l'article 15, paragraphe 1, de la directive 2002/58 ne s'applique pas aux données stockées en application de la directive 2006/24, les données qui sont au cœur du présent litige n'ont pas été enregistrées conformément à la nouvelle directive. Comme *Promusicae* l'explique d'ailleurs, la directive n'est donc pas applicable *ratione temporis*.

123. Même si la directive 2006/24 pouvait s'appliquer, elle ne permettrait pas de communiquer directement des données à caractère personnel relatives au trafic à *Promusicae*. Conformément à son article 1^{er}, la conservation des données vise uniquement à permettre la recherche, la détection et la poursuite d'infractions graves. Par conséquent, ces données ne peuvent, conformément à l'article 4, être communiquées qu'aux autorités compétentes.

62 — Arrêt de la Cour européenne des droits de l'homme du 12 juillet 2005 (plaintes 41138/98 et 64320/01, § 118 et suiv.).

124. Pour autant que la directive 2006/24 soit susceptible de fournir une quelconque indication pour la solution qu'il convient de retenir en l'espèce, nous y puiserons le jugement de valeur que le législateur communautaire y a exprimé, à savoir que, jusqu'à présent, seule la grande criminalité exige une conservation à l'échelle communautaire des données relatives au trafic et à leur utilisation.

il lui faudra modifier les dispositions relatives à la protection des données. Néanmoins, le législateur n'a à ce jour encore rien entrepris de semblable. Au contraire, lorsqu'il a adopté les directives 2000/31, 2001/29 et 2004/48, il a maintenu en vigueur les règles de protection des données sans y apporter de modification. De même, lorsqu'il a adopté les directives 2002/58 et 2006/24 plus spécifiques à ce domaine, il n'a pas jugé devoir introduire des restrictions de la protection des données en faveur de la protection de la propriété intellectuelle.

6. Conclusion sur la protection des données

125. Ainsi donc, il est, à la lumière de la directive 2002/58, compatible avec le droit communautaire, et en particulier avec la directive 2000/31, la directive 2001/29 et la directive 2004/48, que des États membres excluent la communication de données à caractère personnel relatives au trafic lorsqu'elle est sollicitée en vue de permettre d'engager des poursuites de droit civil à l'encontre de violations du droit d'auteur.

127. La directive 2006/24 pourrait, au contraire, avoir pour effet de renforcer la protection des données en droit communautaire en ce qui concerne les litiges relatifs à des violations du droit d'auteur. En effet, même dans les procédures d'enquête pénale, la question se pose de savoir dans quelle mesure il y est compatible avec le droit fondamental à la protection des données que garantit le droit communautaire de permettre aux titulaires dont les droits ont été lésés de prendre connaissance des résultats de l'enquête lorsque ceux-ci reposent sur l'évaluation de données relatives au trafic qui ont été conservées au sens de la directive 2006/24. Jusqu'à présent, cette question n'a pas été abordée par le droit communautaire, puisque les directives concernant la protection des données ne s'appliquent pas aux poursuites pénales⁶³.

126. Le jour où la Communauté jugera nécessaire de mettre en place une protection plus étendue des titulaires de droits d'auteur,

63 — Voir arrêt Parlement/Conseil et Commission (déjà cité à la note 54, point 58).

V — Conclusion

128. Eu égard aux observations qui précèdent, je propose à la Cour de répondre comme suit à la question préjudicielle:

«Il est compatible avec le droit communautaire que des États membres excluent la communication de données à caractère personnel relatives au trafic lorsque celle-ci est sollicitée en vue de permettre la poursuite de violations du droit d'auteur en droit civil.»