H/Inf (2008) 9

Lignes directrices visant à aider les fournisseurs de services Internet

développées par le Conseil de L'Europe en coopération avec l'Association européenne des fournisseurs de services Internet (EuroISPA)

H/Inf (2008) 9

Lignes directrices visant à aider les fournisseurs de services Internet

développées par le Conseil d'Europe en coopération avec l'Association européenne des fournisseurs de services Internet (EuroISPA)

Direction générale
des droits de l'Homme et des affaires juridiques
Conseil de l'Europe
2008

Direction générale des droits de l'Homme et des affaires juridiques
Conseil de l'Europe
F-67075 Strasbourg Cedex

1re impression, juillet 2008
Imprimé dans les ateliers du Conseil de l'Europe

Ces lignes directrices, développées par le Conseil de l'Europe en coopération étroite avec l'Association européenne des fournisseurs de services Internet (EuroISPA), établissent des points de repère à l'intention des fournisseurs de services Internet (FSI). Tout en reconnaissant l'importance du rôle que jouent les FSI en tant que fournisseurs d'accès à Internet, de courrier électronique ou d'information, elles attirent également l'attention sur la nécessité de protéger les utilisateurs, et notamment leurs droits à la vie privée et à la liberté d'expression. À cet égard, les lignes directrices soulignent l'importance pour les fournisseurs en ligne d'être conscients de l'impact de leurs activités sur les droits de l'Homme.

Pour toute information complémentaire sur les activités du Conseil de l'Europe et de l'EuroISPA, voir : www.coe.int • www.euroispa.org

Table des matières

Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les Etats de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire.

Article 10 de la Convention européenne des Droits de l'Homme

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

Article 8 de la Convention européenne des Droits de l'Homme

Comprendre le rôle et la place des fournisseurs de services Internet pour la promotion et le respect des droits de l'homme

1. En fournissant les infrastructures et les services de base permettant aux utilisateurs d'accéder à Internet et de l'utiliser et ainsi d'exercer leurs droits à bénéficier de la société d'information, les fournisseurs de services Internet (FSI) offrent des prestations à forte valeur de service public pour la société.

2. Les FSI sont donc exceptionnellement bien placés et bien dotés pour promouvoir et protéger les droits de l'homme et les libertés fondamentales. En outre, la prestation de services Internet devient une condition préalable à la généralisation de la démocratie participative. Les FSI ont aussi un rôle important pour les Etats qui se sont engagés à protéger et à promouvoir ces droits et ces libertés dans le cadre de leurs engagements de droit international.

3. Les FSI fournissent à leurs utilisateurs une gamme de services variés, qu'il s'agisse de l'accès à Internet ou d'autres services de la société de l'information (applications, contenus et/ou hébergement). Les lignes directrices tiennent compte du fait que tous les FSI n'assument pas le même rôle ni les mêmes responsabilités à l'égard des utilisateurs selon le type de prestation fournie et la catégorie de clients concernée.

4. Les fournisseurs d'accès facilitent l'entrée sur l'Internet et, ainsi à l'accès à un éventail varié d'informations, de cultures et de langues ; c'est avec eux que s'établi souvent le premier contact ainsi que la confiance des utilisateurs. Leur rôle est une condition préalable à la jouissance, par les utilisateurs, des avantages de la société de l'information, notamment par la recherche et la diffusion d'informations ou d'idées, par la création et par l'accès à des connaissances et à l'éducation.

5. On peut considérer que les fournisseurs d'accès, notamment ceux qui s'adressent aux particuliers et aux familles, peuvent participer à une mission de service public en favorisant les droits de leurs clients à bénéficier de la société de l'information. Ce faisant, ils leur permettent de mieux exercer leurs droits et leurs libertés et d'en jouir davantage.

6. Ces fournisseurs d'accès et particulièrement les hébergeurs, ont aussi la possibilité d'agir sur les droits et les libertés dans la mesure où ils peuvent mettre en application des décisions et des actions concernant l'accessibilité aux services (par exemple, ils peuvent supprimer des contenus, les bloquer ou les filtrer).

7. Enfin, les FSI ont accès à une quantité variable d'informations (contenus et/ou données sur le trafic) qui souligne l'importance de leur rôle et de leur position au regard des droits et des libertés des utilisateurs. D'une manière générale, ils ne devraient pas être tenus de surveiller activement les contenus et les données de trafic ; cependant dans certains cas déterminés légalement et expressément notifiés, un FSI peut devoir aider à la surveillance de certains contenus ou informations ou fournir à un tiers des renseignements sur un utilisateur. De tels cas peuvent avoir des conséquences sur la liberté d'expression ou le droit au respect de la vie privée.

8. Globalement, les FSI, et notamment les hébergeurs et les fournisseurs de contenus, ont potentiellement un rôle considérable à jouer dans la promotion des opportunités et des avantages qu'offre la société de l'information. Cela doit être souligné et communiqué aux utilisateurs, aux Etats et surtout aux FSI eux-mêmes.

9. Dans cette optique, les FSI sont encouragés non seulement à prendre acte des lignes directrices qui suivent, à les examiner et à s'efforcer de les respecter mais aussi à y faire référence sur leurs sites web et dans leurs contrats d'utilisation.

10. Ils sont également incités à veiller à ce que leurs employés clés soient sensibilisés à ces lignes directrices et à leurs enjeux, en coopération avec les associations de FSI et les Etats membres et, si nécessaire, avec l'assistance des experts du Conseil de l'Europe.

11. Les associations de FSI peuvent jouer un rôle important en assumant la responsabilité collective de la sensibilisation et de l'information sur les questions qui y sont abordées. Elles sont encouragées à les promouvoir activement auprès de leurs membres, par exemple, par des références ou en les intégrant dans leurs propres codes de conduite et en offrant le soutient d'expertises.

12. Pour ce qui est de l'information à mettre à la disposition des clients, les FSI peuvent en confier la tâche aux associations de FSI, en particulier dans le cas de petites entreprises et quand ces informations ne sont pas spécifiques aux fournisseurs (comme sur les risques présentés par Internet). De plus, les associations peuvent participer à l'harmonisation de l'information des utilisateurs et rassembler les connaissances sur les problèmes abordés dans les lignes directrices. Elles peuvent aussi permettre la coopération et les échanges entre structures existantes dans le domaine de la sécurité sur Internet comme le programme Un Internet Plus Sûr.

13. Ces lignes directrices n'excluent en rien les obligations applicables aux FSI et à leurs activités au regard du droit national, européen ou international et doivent au contraire être prises en compte dans le cadre de ces obligations.

Portée des lignes directrices

14. Les lignes directrices qui suivent sont présentées en plusieurs chapitres selon les rôles respectifs des FSI. Le premier chapitre s'applique aux fournisseurs d'accès Internet (prestataires de services d'accès Internet dédiés ou à la demande). Le deuxième concerne les fournisseurs d'autres services propres à la société de l'information tels que services d'hébergement, fournisseurs de contenus et fournisseurs d'applications. Le troisième chapitre s'applique aux tous les FSI.

15. Elles ne s'appliquent pas aux fournisseurs de seul transit.

Lignes directrices pratiques

Lignes directrices à l'intention des fournisseurs de services Internet (FSI) fournissant des services d'accès

• 16. Veillez à ce que vos clients aient accès à l'information sur les risques potentiels que peut présenter Internet pour leurs droits, leur sécurité et le respect de leur vie privée, ainsi que sur ce que vous faites pour les aider à écarter ces risques. Fournissez des informations sur les outils et les logiciels disponibles à utiliser pour une meilleure protection. Si vous élaborez cette information vous-mêmes, veillez à ce qu'elle soit la plus précise, accessible et à jour possible. Si vous ne le faites pas vous-même, proposez à vos clients des liens à des sources d'informations adéquates, en particulier vers les associations de FSI ou vers des réseaux spécialisés dans la sécurité sur Internet. Des informations pourraient être disponibles sur les risques suivants :

16.1. Contenus illicites ou préjudiciables, risques pour les enfants

• Offrez des informations ou des liens vers l'information sur les risques de tomber sur des contenus illicites sur Internet ou de contribuer à leur diffusion ainsi que sur les risques que des enfants soient exposés à des contenus ou des comportements préjudiciables quand ils surfent sur Internet. Il peut s'agir de contenus ou des comportements qui peuvent nuire au bien-être physique, affectif et psychologique des enfants, tels que la pornographie en ligne, la représentation et la glorification de la violence sur autrui ou sur soi-même, les propos humiliants, discriminatoires ou racistes ou l'apologie de tels propos, la sollicitation (l'approche), l'intimidation, la persécution et d'autres formes de harcèlement . Bien qu'on ne puisse pas vous demander quels contenus sont illicites ou dommageables, il serait utile que l'information que vous offrirez contienne :

– des explications sur ce que vous faites pour lutter contre de tels contenus et comportements, en particulier en collaboration avec des « hotlines » spécialisées (par exemple, Inhope) ;

– des conseils sur comment se protéger contre les risques de trouver des contenus et des comportements illicites ou préjudiciables (par exemple, grâce à des liens vers des informations pertinentes sur des sites web de sécurité de l'Internet) ;

– des renseignements sur les outils logiciels disponibles destinés à protéger les utilisateurs, leur fonctionnement et la manière de les adapter aux besoins de chacun.

• Donnez des informations ou des liens vers des informations sur ce que vos clients peuvent faire pour protéger leurs enfants lorsqu'ils utilisent Internet. Signalez les sites web dont les contenus sont adaptés aux enfants et les ressources disponibles en ligne en matière de sécurité, telles que le Manuel de Maîtrise de l'Internet du Conseil de l'Europe (www.coe.int/Internet-literacy), ou le jeu en ligne *Through the Wild Web Woods*, qui permet d'apprendre à surfer en toute sécurité sur Internet (www.wildwebwoods.org) ou encore les sites web du réseau d sécurité de l'Internet (www.saferInternet.org).

16.2. Risques sur la sécurité

• Si nécessaire, expliquez les mesures que vous prenez pour protéger vos clients contre les risques sur leur sécurité. Ces risques peuvent concerner l'intégrité des données (virus, vers, chevaux de Troie, etc.), la confidentialité (par exemple, lors de transactions en ligne), la sécurité des réseaux ou d'autres risques (par exemple, le phishing).

• Sensibilisez vos clients à des information supplémentaires – ou offrez-leur les liens pertinents – sur les moyens techniques d'assurer leur sécurité sur Internet.

16.3. Risques concernant le respect de la vie privée

• Informez vos clients (ou proposez-leur les liens nécessaires) sur les risques éventuels d'atteinte à leur vie privée lorsqu'ils utilisent Internet, comme la collecte, l'enregistrement et le traitement de données effectués à leur insu sur certains sites (logiciel espion, profilage). Si nécessaire, prévoyez des liens vers l'autorité nationale responsable de l'information sur la législation sur la vie privée et sur la protection des données personnelles.

• Donnez des informations et des conseils supplémentaires à vos clients sur les moyens techniques auxquels ils peuvent recourir pour protéger leur vie privée (outils de protection contre les logiciels espions, etc).

• 17. Lorsque vos clients ont besoin d'une aide supplémentaire pour faire face aux risques évoqués précédemment, veillez à ce qu'ils puissent soit l'obtenir sous la forme la plus appropriée (téléphone, messagerie électronique, courrier, contact personnel…), soit être dirigés vers les sources d'information adéquates.

• 18. Soyez prudents lorsque vous procédez à un blocage ou à la réduction de la qualité des services que vous proposez concernant l'utilisation de certains logiciels ou applications reposant sur un protocole technique donné. Si vous limitez la bande passante, que vous filtrez ou bloquez partiellement le trafic, assurez-vous que vos clients ont été préalablement informés sans ambiguïté de ces restrictions du service.

• 19. Soyez prudent lorsque vous interrompez l'accès aux comptes de vos clients. Ce peut être une limitation des droits du client à accéder aux avantages de la société de l'information et à exercer ses droits à la liberté d'expression et d'information. L'accès à Internet ne devrait être interrompu qu'en application de la législation nationale ou pour d'autres raisons légitimes et strictement nécessaires telles que la violation des obligations contractuelles ou des abus intentionnels. Il faut, le cas échéant, avertir préalablement le client, lui donner des raisons valables de procéder à cette interruption et lui indiquer les mesures à prendre en vue du rétablissement de l'accès.

Lignes directrices à l'intention des FSI fournissant d'autres services de la société de l'information (hébergement, applications, contenus et transit)

• 20. Assurez-vous que tout filtrage ou blocage de services est légitime, proportionné et transparent pour vos clients conformément à la recommandation CM/Rec (2008) 6 du Conseil de l'Europe sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet. Informez clairement vos clients de l'installation sur vos serveurs de tout logiciel de blocage ou de filtrage qui peuvent entrainer la suppression ou l'inaccessibilité de contenus, ainsi que de la nature du filtrage effectué (type de filtrage, règles générales de filtrage, motivation).

• 21. Avant tout filtrage, blocage ou suppression d'un contenu illicite, vous devriez en vérifier l'illégalité, par exemple en contactant l'autorité compétente chargée de veiller au respect de la loi. Toute mesure prise sans vérification préalable peut être considérée comme une ingérence dans un contenu licite et une atteinte aux droits et libertés des personnes qui créent et communiquent ces contenus, en particulier le droit à la liberté d'expression et d'information.

• 22. Informez vos clients de votre politique générale à l'égard des plaintes concernant des contenus prétendument illicites que vous pourriez héberger. Donnez des indications claires au public sur la marche à suivre pour déposer une plainte et à vos clients sur les réponses à apporter.

• 23. Informez vos clients de votre politique générale à l'égard des plaintes concernant des contenus prétendument illicites que vous pourriez héberger. Donnez des indications claires au public sur la marche à suivre pour déposer une plainte et à vos clients sur les réponses à apporter.

• 24. Bien qu'on ne puisse pas vous demander d'indiquer quels contenus sont illicites ou dommageables, vous pourriez utilement informer enseignants et parents sur les risques que les enfants peuvent courir en utilisant vos applications de services (espaces de chat, affichage de messages, etc.), en particulier les risques de se trouver confrontés à des contenus ou à des comportements préjudiciables (sollicitations à des fins sexuelles, harcèlement, etc.).

• 25. En fournissant à vos clients des applications de messagerie électronique, veillez à ce que les outils que vous pouvez offrir, tels que reconnaissance ou filtrage de spam, soient efficaces et que vos clients soient suffisamment informés sur leurs fonctionnalités et les méthodes employées ainsi que sur les possibilités d'adapter leur configuration.

• 26. Si vous fournissez à vos clients des services portant sur des contenus (par exemple, informations web ou services de presse en ligne), envisagez d'octroyer aux utilisateurs un droit de réponse permettant de rectifier rapidement des informations erronées conformément aux principes minimaux énoncés dans la recommandation Rec (2004) 16 du Conseil de l'Europe sur le droit de réponse dans le nouvel environnement des médias.

Lignes directrices à l'intention des FSI concernant le droit au respect de la vie privée et la protection des données

• 27. Etablissez les procédures appropriées et employez les technologies disponibles pour protéger la vie privée des utilisateurs et la confidentialité des contenus et des données de trafic, en garantissant notamment l'intégrité des données, la confidentialité ainsi que la sécurité physique et logique du réseau et des services fournis sur le réseau. Le niveau de sécurité devrait être adapté au type de service offert.

• 28. Mettez à la disposition de vos clients une information et des conseils plus approfondis sur les

moyens techniques qu'ils pourraient utiliser pour se protéger des risques sur la sécurité des données et des communications (logiciels anti-espion, pare-feu, technologie d'encryptage ou signature électronique, etc.).

• 29. Soyez prudent en agissant sur les communications des utilisateurs (par exemple en utilisant l'interception ou la surveillance de leurs courriels). Ces opérations ne doivent être entreprises qu'en cas d'obligation légale, pour obéir à des ordres ou instructions particuliers d'une autorité publique compétente donnés conformément à la loi. Ne surveillez pas activement le contenu des communications sur votre réseau. De plus, la suppression ou la modification de la correspondance d'utilisateurs (par exemple, au moyen de filtres anti-spam) doit être conditionné à leur demande explicite préalable à l'activation des outils.

• 30. Veillez à ne pas révéler l'identité des utilisateurs, les données de trafic ou le contenu des données les concernant à un tiers, sauf pour répondre à une obligation légale ou à des ordres ou instructions particuliers de l'autorité publique compétente donnés conformément à la loi. Toute demande dans ce sens devrait être traitée par les autorités compétentes de votre pays.

• 31. Informez vos clients des circonstances qui vous obligent légalement à révéler - sur demande des services chargés de l'application de la loi, par exemple - leur identité ou des données relatives à leurs connexions ou au trafic de données les concernant. Cette information pourrait en particulier être fournies par les associations de FSI vers lesquelles vous établirez des liens. Si l'on vous demande de divulguer des données, veillez à authentifier la demande qui doit provenir d'une autorité compétente conformément à la loi.

• 32. Veillez à ne pas collecter, traiter ou conserver des données sur les utilisateurs, sauf si cela est nécessaire à des fins explicites, déterminées et légitimes conformes à la législation sur la protection des données. Ne conservez pas de données au-delà du temps demandé par la loi ou nécessaire à leur traitement.

• 33. Soyez attentif à ne pas utiliser de données à caractère personnel concernant les utilisateurs pour votre propre promotion ou votre marketing, à moins que l'utilisateur concerné, après avoir été informé, en ait donné son consentement et ne l'ait pas retiré. Ne publiez pas de données à caractère personnel ! Cela pourrait porter atteinte à la vie privée d'autres personnes et être interdit par la loi.

Extraits des normes du Conseil de l'Europe sur les rôles et les responsabilités des fournisseurs de services Internet (FSI)

Recommandation n° R (99) 5 du Comité des Ministres aux Etats membres sur la protection de la vie privée sur Internet[1]

Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les « inforoutes », qui pourraient être insérées dans les codes de conduite ou leur être annexées

III. Pour les fournisseurs de services Internet

1. Utilisez les procédures appropriées et les technologies disponibles, de préférence celles faisant l'objet d'une certification, garantissant la vie privée des personnes concernées (même si elles ne sont pas utilisatrices d'Internet), et notamment l'intégrité et la confidentialité des données ainsi que la sécurité physique et logique du réseau et des services fournis sur le réseau.

2. Informez les utilisateurs des risques que l'utilisation d'Internet fait courir à la vie privée avant qu'ils ne souscrivent ou commencent à utiliser des services. Il peut s'agir de risques concernant l'intégrité des données, leur confidentialité, la sécurité du réseau ou d'autres risques liés à la vie privée tels que la collecte ou l'enregistrement de données effectués à leur insu.

3. Informez les utilisateurs des moyens techniques qu'ils peuvent utiliser licitement pour diminuer les risques concernant la sécurité des données et des communications, tels que le cryptage, et les signatures électroniques légalement disponibles. Proposez ces moyens techniques à un prix orienté par les coûts et non dissuasif.

4. Avant d'accepter des abonnements et de connecter des utilisateurs à Internet, informez ces derniers des moyens d'y accéder anonymement, d'utiliser ses services et de les payer anonymement (par cartes d'accès prépayées par exemple). L'anonymat absolu peut ne pas être approprié en raison de contraintes légales. Dans ce cas, si la loi l'autorise, offrez la possibilité d'utiliser des pseudonymes. Informez les utilisateurs de l'existence de programmes permettant d'effectuer des recherches et de naviguer anonymement sur Internet. Concevez votre système d'une manière qui évite ou réduise au minimum l'utilisation de données.

5. Ne lisez pas, ne modifiez pas et ne supprimez pas les messages envoyés à d'autres.

6. Ne permettez aucune ingérence dans le contenu des communications, sauf si cette ingérence est prévue par la loi et est effectuée par une autorité publique.

7. Ne collectez, traitez et conservez des données sur les utilisateurs que lorsque cela est nécessaire pour des finalités explicites, déterminées et légitimes.

8. Ne communiquez pas de données à des tiers, sauf si la communication est prévue par la loi.

9. Ne conservez pas de données pour une période plus longue que ce qui est nécessaire pour atteindre le but du traitement.

10. N'utilisez des données aux fins de promouvoir ou de commercialiser vos propres services que si la personne, après avoir été informée, n'y a pas mis d'objection ou si, en cas de traitement de données de trafic ou de données sensibles, elle y a consenti explicitement.

11. Vous êtes responsable de la bonne utilisation des données. Sur votre page de bienvenue, affirmez par une indication claire et visible votre politique en matière de vie privée. Cette indication devrait permettre, par un « hyperlien », d'accéder à une explication détaillée de vos pratiques en matière de vie privée. Avant

1. adoptée le 23 février 1999.

que l'utilisateur ne commence à utiliser des services, lorsqu'il visite votre site et chaque fois qu'il en fait la demande, informez-le de votre identité, des données que vous collectez, traitez et conservez, de quelle manière, pour quelles finalités et pour quelle durée vous les conservez. Au besoin, demandez-lui son consentement. A la demande de la personne concernée, rectifiez sans attendre les données inexactes, effacez-les si elles sont excessives, si elles ne sont pas mises à jour ou si elles ne sont plus nécessaires, et arrêtez le traitement des données si l'utilisateur s'y oppose. Notifiez aux tiers aux vous avez communiqué les données toute modification. Evitez toute collecte de données effectuée à l'insu de l'intéressé.

12. L'information fournie à l'utilisateur doit être exacte et mise à jour.

13. Réfléchissez à deux fois avant de publier des données sur votre site ! Une telle publication pourrait porter atteinte à la vie privée d'autres personnes et pourrait aussi être interdite par la loi.

14. Avant d'envoyer des données à destination d'un autre pays, informez-vous, par exemple auprès de vos autorités, sur la possibilité de procéder à ce transfert. Le cas échéant, vous devrez demander à la personne qui reçoit les données de prendre les garanties nécessaires pour assurer la protection des données.

Déclaration du Comité des Ministres sur la liberté de communication sur l'Internet[2]

Principe 6 – Responsabilité limitée des fournisseurs de services pour les contenus diffusés sur l'Internet

Les Etats membres ne devraient pas imposer aux fournisseurs de services l'obligation générale de surveiller les contenus diffusés sur l'Internet auxquels ils donnent accès, qu'ils transmettent ou qu'ils stockent, ni celle de rechercher activement des faits ou des circonstances révélant des activités illicites.

Les Etats membres devraient veiller à ce que les fournisseurs de services ne soient pas tenus responsables des contenus diffusés sur l'Internet lorsque leurs fonctions se limitent, selon la législation nationale, à transmettre des informations ou à donner accès à l'Internet.

Si les fonctions des fournisseurs de services sont plus larges et qu'ils stockent des contenus émanant d'autres parties, les Etats membres peuvent les tenir pour coresponsables dans l'hypothèse où ils ne prennent pas rapidement des mesures pour supprimer ou pour bloquer l'accès aux information ou aux services dès qu'ils en ont connaissance, comme cela est défini par le droit national, de leur caractère illicite ou, en cas de plainte pour préjudice, de fait ou de circonstances révélant la nature illicite de l'activité ou de l'information.

En définissant, dans le droit national, les obligations des fournisseurs de services telles qu'énoncées au paragraphe précédent, une attention particulière doit être portée au respect de la liberté d'expression de ceux qui sont à l'origine de la mise à disposition des informations, ainsi que du droit correspondant à des usagers à l'information.

Dans tous les cas, les limitations de responsabilité susmentionnées ne devraient pas affecter la possibilité d'adresser des injonctions lorsque les fournisseurs de services sont requis de mettre fin à ou d'empêcher, dans la mesure du possible, une violation de la loi.

Extraits du rapport explicatif de la Déclaration sur la liberté de la communication sur l'Internet

Principe 6 – Responsabilité limitée des fournisseurs de services pour les contenus d'Internet

Il est ici établi qu'en règle générale, les intermédiaires de la chaîne de la communication ne devraient pas être tenus responsables, sauf dans certaines circonstances limitées, des contenus transmis par leurs services. Dans le même sens que les articles 12 à 15 de la Directive sur le commerce électronique, les exemptions de responsabilité prennent en compte les différents types d'activités des intermédiaires, à savoir donner accès aux réseaux de communication, transmettre des données et héberger des informations. Le degré de responsabilité dépend des possibilités dont disposent les fournisseurs de services pour contrôler le contenu et de leur connaissance de son caractère illicite. Les limitations de responsabilités ne s'appliquent pas si les intermédiaires diffusent des contenus illicites de manière intentionnelle.

1er paragraphe – pas d'obligation générale de surveillance

Ce paragraphe est basé sur l'article 15 de la Directive sur le commerce électronique. Les Etats membres ne devraient pas faire peser sur les fournisseurs de services d'obligation générale de surveillance des informations sur l'Internet auxquelles ils donnent accès, qu'ils transmettent ou qu'ils stockent. Ils ne devraient pas non plus être soumis à une obligation générale de rechercher activement des faits ou circonstances révélateurs d'une activité illicite, car cela pourrait constituer un frein à la liberté d'expression.

Ce paragraphe du principe 6 n'empêche pas les pouvoirs publics au sein des Etats membres d'obliger les fournisseurs de services dans certains cas, par exemple lorsqu'une enquête

2. adoptée le 28 mai 2003.

criminelle est menée, de surveiller les activités de leurs clients.

2e paragraphe – « simple transport »

Dans le cas d'une simple transmission d'information, ou lorsqu'ils donnent accès aux réseaux de communication, les intermédiaires ne devraient pas être tenus pour responsables du fait des contenus illicites. Lorsque le rôle des intermédiaires va au-delà, en particulier lorsqu'ils sont à l'origine de la transmission, sélectionnent le receveur de la transmission ou sélectionnent ou modifient l'information transmise, leur responsabilité peut être invoquée.

L'activité de l'intermédiaire qui est ici en question, et qui devrait être exempt de responsabilité, est parfois appelée « simple transport » (voir article 12 de la Directive sur le commerce électronique).

3e paragraphe – « hébergement »

Dans le cas de l'hébergement de contenus émanant de tiers, les intermédiaires ne devraient en général pas être tenus pour responsables (voir article 14 de la Directive sur le commerce électronique). Cependant, ceci ne s'applique pas lorsque le tiers agit sous le contrôle de l'intermédiaire, par exemple lorsqu'une agence de presse possède son propre serveur afin d'héberger des contenus produits par ses journalistes. Toutefois, si l'hôte prend conscience soit de la nature illicite des contenus hébergés sur ses serveurs soit, en cas de plainte pour préjudice, de faits révélateurs d'une activité illicite, il peut raisonnablement être tenu pour responsable. Les conditions précises devraient être définies par le droit national.

4e paragraphe – procédures de « notification et suppression » et liberté d'expression et d'information

Comme stipulé au paragraphe 3 du principe 6 de la Déclaration, les fournisseurs de services peuvent être tenus pour responsables s'ils ne suppriment ou n'empêchent pas rapidement l'accès aux informations ou services dont ils ont pris connaissance, selon les principes énoncés par le droit national, du caractère illicite. Il est attendu des Etats membres qu'ils définissent de manière plus détaillée le niveau de connaissance requis des fournisseurs de services avant la mise en cause de leur responsabilité. A cet égard, les procédures de « notification et suppression » sont très importantes. Les Etats membres devraient cependant rester prudents quant à la mise en cause de la responsabilité des fournisseurs de services qui n'ont pas réagi à de telles notifications. Les questions concernant le caractère illicite de certains contenus sont souvent complexes, et relèvent plutôt des tribunaux. Il peut être dangereux du point de vue de la liberté d'expression et d'information que les fournisseurs de services suppriment trop rapidement un contenu après réception d'une plainte. Un contenu parfaitement légitime pourrait ainsi être supprimé par crainte de voir sa responsabilité juridique mise en cause.

5e paragraphe – la possibilité d'adresser des injonctions demeure intacte

Il est ici souligné, dans le droit fil des articles 12 à 14 de la Directive sur le commerce électronique, qu'en dépit des limitations de responsabilité susmentionnées, la possibilité d'adresser des injonctions lorsque l'on requiert des fournisseurs de services qu'ils mettent fin ou qu'ils empêchent, dans la limite du possible, une atteinte à la loi, demeure intacte.

Déclaration sur les droits de l'homme et l'état de droit dans la Société de l'information[3]

S'agissant des mesures d'autorégulation et de corégulation visant à défendre la liberté d'expression et de communication, les acteurs du secteur privé sont encouragés à s'attaquer résolument au problème suivant :

• la censure (censure cachée) par les prestataires de services Internet privés, par exemple le blocage ou l'élimination de contenus de leur propre initiative ou à la demande d'une tierce partie.

Recommandation Rec (2007) 11 du Comité des Ministres aux Etats membres sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication[4]

Les Etats membres, le secteur privé et la société civile sont encouragés à développer des normes et des stratégies communes pour promouvoir la transparence et la mise à disposition d'informations, de conseils et d'assistance aux utilisateurs individuels de technologies et de services, en particulier dans les situations suivantes :

…

vii. la suppression de contenus jugés illégaux par rapport aux considérations de l'Etat de droit ;

3. adoptée le 13 mai 2006.
4. adoptée le 26 septembre 2007.

Recommandation Rec (2007) 16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'Internet[5]

Les Etats membres devraient adopter ou développer des politiques visant à préserver et, autant que possible, à promouvoir la protection des droits de l'homme et le respect de l'Etat de droit dans la société de l'information. A cet égard, une attention particulière devrait être portée :

• au droit à la vie privée et à la confidentialité des correspondances sur Internet et lors de l'utilisation d'autres TIC, y compris le respect de la volonté des utilisateurs de ne pas révéler leur identité, promu en encourageant les internautes et les fournisseurs d'accès et de contenus à en assumer ensemble la responsabilité ;

Les Etats membres devraient promouvoir un débat public sur les responsabilités des acteurs privés, tels que les prestataires de services et de contenus Internet ainsi que les utilisateurs, et les encourager – dans l'intérêt du débat, du processus démocratique et de la protection des droits d'autrui – à prendre des mesures d'autorégulation et d'autres mesures pour optimiser la qualité et la fiabilité de l'information contenue sur l'Internet et de promouvoir l'exercice d'une responsabilité personnelle, en particulier au regard de l'établissement, de la conformité et du contrôle du respect de codes de conduite.

Recommandation CM/Rec (2008) 6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet

Le Comité des Ministres, conformément à l'article 15.*b* du Statut du Conseil de l'Europe :

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres afin de sauvegarder et de promouvoir les idéaux et les principes qui sont leur patrimoine commun ;

Rappelant que les Etats parties à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (Convention européenne des Droits de l'Homme, STE n° 5) se sont engagés à reconnaître à toute personne relevant de leur juridiction les droits et libertés définis par la Convention ;

Réaffirmant l'attachement des Etats membres du droit fondamental à la liberté d'expression, et de recevoir et de communiquer des informations et des idées sans ingérence des autorités publiques et sans considération de frontière, tel que garanti par l'article 10 de la Convention européenne des Droits de l'Homme ;

Conscient que toute intervention d'un Etat membre qui interdit l'accès à un contenu spécifique de l'Internet pourrait constituer une restriction à la liberté d'expression et d'accès à l'information dans l'environnement en ligne, et qu'une telle restriction devrait remplir les conditions de l'article 10, paragraphe 2, de la Convention européenne des Droits de l'Homme ainsi que la jurisprudence pertinente de la Cour européenne des Droits de l'Homme ;

Rappelant à cet égard la Déclaration sur les droits de l'homme et l'Etat de droit dans la société de l'information, adoptée par le Comité des Ministres le 13 mai 2005, aux termes de laquelle les Etats membres doivent préserver et renforcer les mesures juridiques et pratiques pour éviter la censure par l'Etat ou le secteur privé ;

Rappelant la Recommandation Rec (2007) 11 du Comité des Ministres aux Etats membres sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication, qui encourage les Etats membres, le secteur privé et la société civile à développer des normes et des stratégies communes pour promouvoir la transparence et la mise à disposition d'informations, de conseils et d'assistance aux utilisateurs individuels de technologies et de services, concernant, entre autres, le blocage de l'accès et le filtrage des contenus et services par rapport à la liberté de recevoir ou de communiquer des informations ;

Notant que le recours volontaire et responsable aux filtres Internet (produits, systèmes et mesures permettant de bloquer ou de filtrer le contenu de l'Internet) peut accentuer la confiance et la sécurité sur Internet des utilisateurs, en particulier des enfants et des jeunes, mais également conscient que l'utilisation de ces filtres Internet peut avoir un impact sur le droit à la liberté d'expression et à l'accès à l'information, tel que protégé par l'article 10 de la Convention européenne des Droits de l'Homme ;

Rappelant la Recommandation Rec (2006) du Comité des Ministres sur la responsabilisation et l'autonomisation des enfants dans le nouvel environnement de l'information et de la communication, qui souligne l'importance des stratégies pour l'info compétence et pour la formation à l'information destinées aux enfants afin de leur permettre de mieux comprendre et traiter les contenus (par exemple la violence sur autrui ou sur soi-même, la pornographie, la discrimination et le racisme) et les comportements (tels que la sollicitation, l'intimidation, le harcèlement ou la persécution) qui présentent un risque d'effets préjudiciables, encourageant ainsi un climat

5. adoptée le 7 novembre 2007.

de confiance, de bien-être et de respect d'autrui dans le nouvel environnement de l'information et de la communication ;

Convaincu de la nécessité de veiller à ce que les internautes connaissent, comprennent et sachent utiliser, adapter et contrôler les filtres en fonction de leurs besoins respectifs ;

Rappelant la Recommandation Rec (2001) du Comité des Ministres sur l'autorégulation des cyber-contenus (l'autorégulation et la protection des utilisateurs contre les contenus illicites ou préjudiciables diffusés sur les nouveaux services de communication et d'information), qui préconise une labellisation neutre des contenus donnant aux utilisateurs la possibilité de se faire leur propre jugement de valeur sur ces contenus, ainsi que la mise au point d'une large gamme d'outils de recherche et de profils de filtrage qui leur donnent, sur la base de descripteurs de contenus, la possibilité de sélectionner des contenus ;

Conscient de la valeur de service public de l'Internet, comprise comme étant le fait pour les personnes de compter de manière significative sur l'Internet comme un outil essentiel pour leurs activités quotidiennes (communication, information, savoir, transactions commerciales, loisirs) et de l'attente légitime qui en découle que les services de l'Internet soient accessibles et abordables financièrement, sécurisés, fiables et continus, et rappelant sur ce point la Recommandation Rec (2007) 16 du Comité des Ministres sur des mesures visant à promouvoir la valeur de service public d'Internet ;

Rappelant la Déclaration du Comité des Ministres du 28 mai 2003 sur la liberté de la communication sur l'Internet, qui souligne que les autorités publiques ne devraient pas, au moyen de mesures générales de blocage ou de filtrage, refuser l'accès du public à l'information et autres communications sur l'Internet, sans considération de frontière, mais que cela n'empêche pas l'installation de filtres pour la protection des mineurs, notamment dans des endroits accessibles aux mineurs tels que les écoles ou les bibliothèques ;

Réaffirmant l'attachement des Etats membres au droit qu'a chacun à la vie privée et au respect de la correspondance, tel que protégé par l'article 8 de la Convention européenne des Droits de l'Homme, et rappelant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et son Protocole additionnel sur les autorités de contrôle et les flux transfrontières de données (STE n° 181) ainsi que la Recommandation n° R (99) 5 du Comité des Ministres sur la protection de la vie privée sur Internet,

Recommande aux Etats membres d'adopter des normes et des stratégies communes en matière de filtres Internet afin de promouvoir le plein exercice et la pleine jouissance de la liberté d'expression et d'information et des autres droits et libertés relatifs, contenus dans la Convention européenne des Droits de l'Homme, en particulier :

- en prenant des mesures en ce qui concerne les filtres Internet conformément aux lignes directrices figurant en annexe à la présente recommandation ;
- en portant ces lignes directrices à la connaissance de tous les acteurs concernés des secteurs privé et public, notamment ceux qui conçoivent, utilisent (installent, activent, désactivent et mettent en œuvre) et contrôlent les filtres Internet, et de la société civile, afin qu'ils puissent contribuer à leur mise en œuvre.

Annexe à la Recommandation CM/Rec (2008) 6

Utilisation et contrôle des filtres Internet pour exercer et jouir pleinement de la liberté d'expression et d'information

Il est essentiel que les internautes connaissent, comprennent et sachent utiliser les filtres Internet pour pouvoir exercer pleinement leurs libertés et leurs droits fondamentaux dont, notamment, la liberté d'expression et d'information, et prendre une part active aux processus démocratiques. Lorsqu'un utilisateur est confronté à un filtre, il doit être informé qu'un filtre est activé et, s'il y a lieu, il doit savoir reconnaître et contrôler le niveau de filtrage auquel est soumis le contenu qu'il consulte. Il devrait, en outre, avoir la possibilité de contester le blocage ou le filtrage du contenu, et de demander des explications et la mise en place de solutions.

En coopération avec le secteur privé et la société civile, les Etats membres devraient veiller à ce que les utilisateurs soient informés des filtrages actifs en place et, s'il y a lieu, à ce qu'ils soient capables de les activer et de les désactiver ou d'en modifier le niveau. Les mesures en ce sens sont notamment les suivantes

i. développer et encourager un degré minimal de connaissances pour les utilisateurs afin qu'ils sachent repérer les filtres actifs et qu'ils comprennent comment et selon quels critères le filtrage opère (par exemple listes noires, listes blanches, blocage de mots clés, classement du contenu, etc., ou une combinaison de plusieurs de ces critères) ;

ii. assurer aux utilisateurs un minimum d'informations, ces informations étant définies par des normes, expliquant pourquoi tel ou tel contenu a été filtré ;

iii. revoir et mettre à jour régulièrement les filtres afin d'améliorer leur efficacité, leur proportionnalité et leur légitimité par rapport à l'objectif qu'ils poursuivent ;

iv. fournir des informations et des conseils clairs et concis sur le contournement manuel d'un filtre actif, à savoir l'instance à contacter quand le blocage d'un contenu s'avère injustifié et les motifs qui peuvent autoriser le contournement d'un filtre pour un type spécifique de contenu ou localisateur universel de ressources (Uniform Resource Locator - URL) ;

v. veiller à ce que les contenus filtrés par mégarde ou par erreur deviennent accessibles sans difficulté indue et dans un délai raisonnable ;

vi. promouvoir des initiatives de sensibilisation des personnes qui conçoivent, utilisent et suivent les fil-

tres, à leurs responsabilités sociales et éthiques, en mettant l'accent sur la liberté d'expression et d'information, et sur le droit à la vie privée, ainsi que sur la participation active à la vie publique et aux processus démocratiques ;

vii. sensibiliser aux limites potentielles à la liberté d'expression et d'information et au droit à la vie privé qui peuvent résulter de l'utilisation de filtres, et à la nécessité de respecter le principe de proportionnalité de ces limites ;

viii. faciliter l'échange d'expériences et de bonnes pratiques concernant la conception, l'utilisation et le contrôle des filtres ;

ix. encourager l'organisation de formations à l'attention des administrateurs de réseau, des parents, des éducateurs et des autres personnes appelées à utiliser et à contrôler des filtres ;

x. promouvoir et accompagner les initiatives existantes en faveur d'une utilisation des filtres responsable et respectueuse des droits de l'homme, de la démocratie et de l'Etat de droit ;

xi. encourager la définition de normes et de références en matière de filtres, afin d'aider les internautes à choisir et à utiliser au mieux ces produits.

Dans ce contexte, il est souhaitable que la société civile soit encouragée à sensibiliser les utilisateurs aux avantages et aux dangers potentiels des filtres. Cela devrait inclure la promotion de l'importance d'un accès libre et non entravé à l'Internet afin que tous ses utilisateurs exercent et jouissent pleinement de leurs droits de l'homme et de leurs libertés fondamentales, en particulier le droit à la liberté d'expression et d'information, et le droit à la vie privée, ainsi que de leur droit à participer activement à la vie publique et aux processus démocratiques.

Mise en place d'un filtrage approprié pour les enfants et les jeunes

L'Internet a fait augmenter de manière significative le nombre et la diversité des idées, des informations et des opinions pouvant être reçues et communiquées par les personnes conformément au droit à la liberté d'expression et d'information sans ingérence de la part des pouvoirs publics et sans considération de frontière. Parallèlement, la quantité de contenus faciles d'accès et potentiellement nuisibles, en particulier pour les enfants et les jeunes, s'en est trouvée accrue. Pour satisfaire le souhait légitime et le devoir des Etats membres de mettre les enfants et les jeunes à l'abri de contenus potentiellement préjudiciables, l'utilisation proportionnée de filtres peut être une façon appropriée d'encourager l'accès à l'Internet et la confiance lors de son utilisation, en complément des autres stratégies pour combattre les contenus préjudiciables comme le développement et la mise à disposition d'une culture de l'information.

Dans ce contexte, les Etats membres devraient :

i. faciliter le développement de stratégies visant à identifier les contenus risquant de nuire aux enfants et aux jeunes, en tenant compte de la diversité des cultures, des valeurs et des opinions ;

ii. coopérer avec le secteur privé et la société civile afin d'éviter de surprotéger les enfants et les jeunes, entre autres en soutenant la recherche et développement autour de systèmes de filtrage " intelligents ", qui devraient prendre d'avantage en compte le contexte dans lequel l'information est fournie (par exemple en faisant la différence entre un contenu préjudiciable en soi et des références acceptables à ce contenu comme sur un site scientifique) ;

iii. faciliter et promouvoir les initiatives qui assistent les parents et les éducateurs à choisir et à utiliser des filtres évolutifs et adaptés à l'âge des enfants et des jeunes ;

iv. informer les enfants et les jeunes, dans le cadre de stratégies formelles et non formelles d'éducation aux médias, des avantages et des dangers des contenus de l'Internet et de leur filtrage.

En outre, le secteur privé devrait être incité :

i. à mettre au point des filtres « intelligents » offrant un filtrage évolutif et adapté à l'âge, qui peut être ajusté pour suivre le progrès et l'âge de l'enfant tout en garantissant que ne soient pas filtrés les contenus non considérés comme nuisibles ou inappropriés pour le groupe cible ;

ii. à coopérer avec les instances d'autorégulation et de corégulation afin de développer des normes en matière de systèmes évolutifs et adaptés à l'âge de classement des contenus potentiellement nuisibles, en tenant compte de la diversité des cultures, des valeurs et des opinions ;

iii. à développer, en coopération avec la société civile, une labellisation commune des filtres afin d'aider les parents et les éducateurs à faire des choix en toute connaissance de cause lors de l'acquisition des produits de filtrage, et de certifier que ceux-ci se conforment à certaines exigences de qualité ;

iv. à promouvoir l'interopérabilité des systèmes d'auto classification des contenus par les fournisseurs eux-mêmes et à aider à mieux faire connaître les avantages et les dangers potentiels de ce type de classification.

Enfin, la société civile devrait être incitée :

i. à débattre et à partager ses expériences et sa connaissance en matière d'évaluation et de sensibilisation au développement et à l'utilisation de filtres en tant que mesure de protection des enfants et des jeunes ;

ii. à contrôler régulièrement et à analyser l'usage et l'impact des filtres destinés aux enfants et aux jeunes en ce qui concerne leur efficacité et leur contribution à l'exercice et à la jouissance des droits et libertés garantis par l'article 10 et les autres dispositions de la Convention européenne des Droits de l'Homme.

Utilisation et mise en œuvre de filtres Internet par les secteurs public et privé

Sans préjudice de l'importance de la responsabilisation et l'autonomisation des utilisateurs au fonctionnement et au contrôle des filtres, comme expliqué plus haut, et compte tenu de la large valeur de service public revêtue par Internet pour le grand public, les entités publiques

de tous les niveaux (telles que les administrations, les bibliothèques ou les établissements d'enseignement publics) qui introduisent des filtres ou les utilisent dans leurs prestations de services devraient veiller au plein respect de la liberté d'expression et d'information, du droit de chacun à la vie privée et au respect de la correspondance de chaque utilisateur.

Dans ce contexte, les Etats membres devraient :

i. s'abstenir de filtrer le contenu de l'Internet sur les réseaux de communication électroniques gérés par des entités publiques pour des raisons autres que celles exposées à l'article 10, paragraphe 2, de la Convention européenne des Droits de l'Homme tel qu'interprété par la Cour européenne des Droits de l'Homme ;

ii. garantir que les mesures générales de blocage ou de filtrage sur tout le territoire ne sont introduites par l'Etat que si les conditions énoncées à l'article 10, paragraphe 2, de la Convention européenne des Droits de l'Homme sont remplies. De telles mesures étatiques ne devraient être prises que si le filtrage concerne un contenu spécifique et clairement identifiable, une autorité nationale compétente a pris une décision au sujet de l'illégalité de ce contenu et la décision peut être réétudiée par un tribunal ou entité de régulation indépendant et impartial, en accord avec les dispositions de l'article 6 de la Convention européenne des Droits de l'Homme ;

iii. introduire, si nécessaire et approprié, des dispositions nationales pour la prévention des abus intentionnels des filtres pour restreindre l'accès des citoyens aux contenus légaux ;

iv. veiller à ce que tous les filtres soient évalués avant et pendant leur mise en œuvre, afin de vérifier que les effets du filtrage sont en adéquation avec l'objectif de la restriction et donc justifiés dans une société démocratique, afin d'éviter tout blocage excessif des contenus ;

v. prévoir des voies de recours et des solutions effectives et facilement accessibles, dont la suspension des filtres, dans les cas où les usagers et/ou les auteurs de contenus dénoncent qu'un contenu a été bloqué abusivement ;

vi. éviter le blocage général des contenus choquants ou préjudiciables pour les utilisateurs ne faisant pas partie du groupe qu'un filtre vise à protéger, ainsi que le blocage général des contenus illicites pour les utilisateurs pouvant attester du intérêt ou de la nécessité légitime d'y accéder dans des circonstances exceptionnelles, notamment à des fins de recherche ;

vii. veiller à ce que le droit à la vie privée et au respect de la correspondance soit respecté lors de l'utilisation et de l'application de filtres, et veiller à ce que les données personnelles enregistrées, archivées et traitées via les filtres soient utilisées uniquement dans un but légitime et non commercial.

En outre, les Etats membres et le secteur privé sont invités :

i. à évaluer et à réétudier régulièrement l'efficacité de la mise en place de filtres, et son caractère proportionnel ;

ii. à renforcer les informations et les conseils aux utilisateurs concernés par des filtres sur des réseaux privés, informations portant notamment sur l'existence de filtres et les raisons qui peuvent les justifier ainsi que sur les critères de fonctionnement des filtres ;

iii. à coopérer avec les utilisateurs (clients, employés, etc.) afin d'améliorer la transparence, l'efficacité et le caractère proportionnel des filtres.

Dans ce contexte, la société civile devrait être encouragée à suivre le développement et la mise en place des filtres par les principales parties prenantes, du secteur public comme du secteur privé. Elle devrait, le cas échéant, appeler les Etats membres et le secteur privé à, respectivement, garantir et faciliter la liberté d'expression et d'information de chaque utilisateur, en particulier s'agissant de sa liberté de recevoir des informations sans ingérence de la part des pouvoirs publics et sans considération de frontière dans le nouvel environnement de l'information et de la communication.

Ces lignes directrices, développées par le Conseil de l'Europe en coopération étroite avec l'Association européenne des fournisseurs de services Internet (EuroISPA), établissent des points de repère à l'intention des fournisseurs de services Internet (FSI). Tout en reconnaissant l'importance du rôle que jouent les FSI en tant que fournisseurs d'accès à Internet, de courrier électronique ou d'information, elles attirent également l'attention sur la nécessité de protéger les utilisateurs, et notamment leurs droits à la vie privée et à la liberté d'expression. À cet égard, les lignes directrices soulignent l'importance pour les fournisseurs en ligne d'être conscients de l'impact de leurs activités sur les droits de l'Homme.

Pour toute information complémentaire
sur les activités du Conseil de l'Europe et de l'EuroISPA,
voir : www.coe.int • www.euroispa.org

Direction générale
des droits de l'Homme et des affaires juridiques
Conseil de l'Europe
F-67075 Strasbourg Cedex