CONSEIL DE L ' EUROPE
COMITE DES MINISTRES

RECOMMANDATION N° R (99) 5

DU COMITE DES MINISTRES AUX ETATS MEMBRES

SUR LA PROTECTION DE LA VIE PRIVEE SUR INTERNET

(adoptée par le Comité des Ministres le 23 février 1999, lors de la 660e réunion des Délégués des Ministres)

LIGNES DIRECTRICES
pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les "inforoutes"

Préambule

Le Comité des Ministres, en vertu de 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;

Notant le développement des nouvelles technologies et des nouveaux services de communication et d'information en ligne ;

Conscient que ce développement influencera notablement le fonctionnement de la société en général et les relations entre individus, en particulier en offrant des possibilités accrues de communication et d'échange d'informations aux plans national et international ;

Conscient des avantages que les utilisateurs des nouvelles technologies peuvent retirer de ce développement ;

Estimant, toutefois, que le développement des technologies et la généralisation de la collecte et du traitement de données à caractère personnel sur les "inforoutes" comportent des risques pour la vie privée des personnes ;

Estimant que les développements des technologies permettent également de contribuer au respect des droits et libertés fondamentales, notamment du droit à la vie privée, lors du traitement de données à caractère personnel concernant des personnes physiques ;

Conscient de la nécessité de développer des techniques garantissant l'anonymat des personnes concernées et la confidentialité des informations échangées par le biais des "inforoutes", dans le respect des droits et libertés d'autrui et des valeurs d'une société démocratique ;

Conscient que les communications à l'aide des nouvelles technologies de l'information sont également soumises au respect des droits de l'homme et des libertés fondamentales, notamment au respect de la vie privée et du secret de la correspondance, tels que garantis par l'article 8 de la Convention européenne des Droits de l'Homme ;

Reconnaissant que la collecte, le traitement, et notamment la communication de données à caractère personnel par le biais de nouvelles technologies de l'information, en particulier les "inforoutes", sont régis par les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Strasbourg, 1981, Série des traités européens n° 108) et par les recommandations sectorielles relatives à la protection des données, en particulier la Recommandation n° R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes, la Recommandation n° R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics et la Recommandation n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques ;

Estimant qu'il convient de sensibiliser les utilisateurs et les fournisseurs de services d'Internet à la mise en œuvre des dispositions générales de la convention citée plus haut, à l'égard de la collecte et du traitement des données à caractère personnel sur les "inforoutes",

Recommande aux gouvernements des Etats membres de diffuser largement les lignes directrices contenues dans l'annexe à la présente recommandation, en particulier auprès des utilisateurs et des fournisseurs de services d'Internet, ainsi qu'auprès de toute autorité nationale chargée de veiller au respect des dispositions de la protection des données.

Annexe à la Recommandation N° R (99) 5

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 peuvent être intégrées ou annexées à des codes de conduite

I. Introduction

Les présentes lignes directrices énoncent des principes d'une conduite loyale à observer en matière de protection de la vie privée par les utilisateurs et les fournisseurs de services d'Internet.[1] Ces principes peuvent être repris dans des codes de conduite.

Les utilisateurs devraient être conscients des responsabilités des fournisseurs de services d'Internet et vice versa. Il est donc conseillé aux utilisateurs et aux fournisseurs de services d'Internet de lire ce texte en entier, bien qu'il soit divisé en plusieurs parties pour le rendre plus facile à utiliser. Vous pouvez être concerné par une seule ou plusieurs parties de ce texte à la fois.
L'utilisation d'Internet implique une responsabilité pour chaque action et comporte des risques pour la vie privée. Il est important de se conduire de manière à se protéger et à promouvoir de bonnes relations avec les autres. Ces lignes directrices énoncent quelques solutions pratiques pour la protection de la vie privée, mais ne vous dispensent pas de connaître vos droits et obligations.

Rappelez-vous que le respect de la vie privée est un droit fondamental de tout individu qui peut être protégé également par des lois sur la protection des données. Alors, mieux vaut vérifier votre situation juridique.

II. Pour les utilisateurs

[1] Voir partie IV, paragraphe 1.

1. Rappelez-vous qu'Internet n'est pas sûr. Cependant, existent et se développent différents moyens vous permettant d'améliorer la protection de vos données.[2] Utilisez donc tout moyen disponible pour protéger vos données et vos communications, tel que le cryptage légalement disponible pour des courriers électroniques confidentiels aussi bien que des codes d'accès à votre propre PC.[3]

2. Rappelez-vous que chaque transaction effectuée, chaque visite d'un site sur Internet laissent des traces. Ces "traces électroniques" peuvent être utilisées à votre insu pour établir un profil de votre personne et de vos intérêts. Si vous ne voulez pas que votre profil soit établi, vous êtes encouragé à utiliser les dispositifs techniques les plus récents qui comprennent la possibilité d'être informé à chaque fois que vous laissez des traces et à refuser ces traces. Vous pouvez également demander à être informé des règles de conduite retenues par les différents programmes et sites en matière de protection de la vie privée et préférer ceux qui enregistrent peu de données ou qui sont accessibles d'une manière anonyme.

3. L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée. Informez-vous des moyens techniques de recourir à cet anonymat, si cela est approprié[4].

4. L'anonymat absolu peut ne pas être approprié en raison de contraintes légales. Dans ce cas, si la loi l'autorise, vous pouvez utiliser un pseudonyme, de sorte que votre identité véritable ne sera connue que de votre fournisseur de services d'Internet.

5. Ne communiquez à votre fournisseur de services d'Internet ou à toute autre personne que les données qui sont nécessaires pour une finalité déterminée dont vous avez été informé. Soyez particulièrement vigilant avec les cartes de crédit et les numéros de compte, qui peuvent être très facilement utilisés - abusivement - dans le cadre d'Internet.

6. Rappelez-vous que votre adresse électronique constitue une donnée à caractère personnel et que d'autres peuvent souhaiter l'utiliser à différentes fins, telles que son inclusion dans des annuaires ou des listes d'utilisateurs. N'hésitez pas à demander quelle est la finalité de ces annuaires ou de ces autres utilisations. Vous pouvez demander que votre adresse soit effacée si vous ne souhaitez pas figurer dans ces annuaires ou dans ces listes.

7. Soyez prudent à l'égard des sites qui demandent plus de données que nécessaire pour l'accès au site ou la réalisation d'une transaction, ou encore qui ne vous précisent pas pourquoi ils ont besoin de l'ensemble de ces données vous concernant.

8. Rappelez-vous que votre responsabilité juridique est engagée pour le traitement de données, par exemple si vous téléchargez ou télédéchargez illicitement et que, même si vous avez utilisé un pseudonyme, on peut vous identifier.

9. N'envoyez pas de courrier malveillant, cela peut se retourner contre vous et avoir des conséquences juridiques.

---

[2] Le terme "donnée" se rapporte aux données à caractère personnel et signifie toute information vous concernant ou concernant d'autres personnes.

[3] Par exemple, utilisez des mots de passe et modifiez-les régulièrement.

[4] Par exemple en utilisant des kiosques Internet publics ou des cartes d'accès prépayées et des cartes de paiement.

10. Votre fournisseur de services d'Internet est responsable de la bonne utilisation des données. Demandez-lui quelles données il collecte, traite et conserve, de quelle manière, et pour quelles finalités. Répétez cette demande de temps en temps. Exigez qu'il les modifie si elles sont inexactes ou qu'il les efface si elles sont excessives, si elles ne sont pas mises à jour ou ne sont plus nécessaires. Demandez au fournisseur de services d'Internet qu'il notifie cette modification aux autres parties auxquelles il a communiqué vos données[5].

11. Si vous n'êtes pas satisfait de la manière dont votre fournisseur de services d'Internet actuel collecte, traite, conserve ou communique vos données et s'il refuse de modifier son attitude, alors envisagez de changer de fournisseur. Si vous estimez que votre fournisseur de services d'Internet ne respecte pas les règles relatives à la protection des données, vous pouvez informer les autorités compétentes ou intenter une action en justice.

12. Informez-vous des risques pour la vie privée et la sécurité sur Internet ainsi que des moyens disponibles de réduire ces risques.

13. Si vous avez l'intention d'envoyer des données vers un autre pays, vous devez être conscient du fait que ces données peuvent y être moins bien protégées. S'il s'agit de vos propres données, vous êtes évidemment libre de les transmettre malgré tout. Cependant, avant d'envoyer vers un autre pays des données concernant d'autres personnes, informez-vous, par exemple auprès de vos autorités, sur la possibilité de procéder à ce transfert[6]. Le cas échéant, vous devrez demander à la personne qui reçoit les données de prendre les garanties[7] nécessaires pour assurer la protection des données.

III. Pour les fournisseurs de services d'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 l'utilisateur des moyens techniques qu'il peut 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, d'utiliser ses services et de les payer anonymement (par

---

[5] Les lois de protection des données, à l'instar de l'article 5 de la Convention sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du Conseil de l'Europe, rendent celui qui les traite responsable de l'exactitude et de la mise à jour des données.

[6] La législation de nombreux pays en Europe interdit les transferts vers les pays n'ayant pas un niveau de protection des données adéquat ou équivalent à celui de votre pays. Des exceptions sont toutefois prévues, notamment si la personne concernée a consenti à ce que ses données soient transmises vers de tels pays.

[7] Ces garanties peuvent être développées et/ou présentées, notamment dans le contrat régissant le flux transfrontière de données.

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.[8]

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

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 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 auxquels 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.[10] Le cas échéant, vous

---

[8] Généralement, les lois en matière de protection des données permettent sous diverses conditions la communication à des tiers, notamment:- de données sensibles et de données de trafic, à condition que la personne concernée y ait explicitement consenti; - d'autres données lorsque la communication est nécessaire pour atteindre la finalité légitime poursuivie ou lorsque la personne concernée, après avoir été informée, ne s'y est pas opposée.

[9] Par exemple, ne conservez pas des données de facturation, à moins que cela ne soit prévu par la loi.

[10] Voir note 10.

devrez demander à la personne qui reçoit les données de prendre les garanties[11] nécessaires pour assurer la protection des données.

IV. Clarifications et recours

1. Lorsque, dans ce texte, les termes "fournisseur" ou "prestataire de service" sont utilisés, ils s'appliquent également, le cas échéant, aux autres acteurs d'Internet tels que les fournisseurs d'accès, de contenu, de réseau, les concepteurs de logiciels de navigation, les coordinateurs de forums ou d'« info-kiosques », etc.

[11] Voir note 11.

2. Il est important de vous assurer du respect de vos droits. Les mécanismes de feedback offerts par des forums d'Internet, les associations de fournisseurs de services d'Internet, les autorités de protection des données ou autres instances sont des moyens importants pour assurer le respect de ces lignes directrices. Contactez-les si vous avez besoin de clarifications ou de recours.

3. Ces lignes directrices s'appliquent à tout type d'"inforoute".