CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

QUATRIÈME SECTION

AFFAIRE K.U. c. FINLANDE

(Requête n° 2872/02)

ARRÊT

STRASBOURG

2 décembre 2008

DÉFINITIF

02/03/2009

.

En l'affaire K.U. c. Finlande,

La Cour européenne des droits de l'homme (quatrième section), siégeant en une chambre composée de :

Nicolas Bratza, *président*,
Lech Garlicki,
Giovanni Bonello,
Ljiljana Mijović,
Davíd Thór Björgvinsson,
Ján Šikuta,
Päivi Hirvelä, *juges*,

et de Lawrence Early, *greffier de section*,

Après en avoir délibéré en chambre du conseil le 13 novembre 2008,

Rend l'arrêt que voici, adopté à cette date :

PROCÉDURE

1. A l'origine de l'affaire se trouve une requête (n° 2872/02) dirigée contre la République de Finlande et dont un ressortissant de cet Etat (« le requérant ») a saisi la Cour le 1er janvier 2002 en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »). Le président de la chambre a accédé à la demande de non-divulgation de son identité formulée par le requérant (article 47 § 3 du règlement).

2. Le requérant a été représenté par Me P. Huttunen, avocat à Helsinki. Le gouvernement finlandais (« le Gouvernement ») a été représenté par son agent, M. A. Kosonen, du ministère des Affaires étrangères.

3. Dans sa requête, le requérant alléguait en particulier que l'Etat avait manqué à son obligation positive de protéger son droit au respect de sa vie privée garanti par l'article 8 de la Convention.

4. Par une décision du 27 juin 2006, la Cour a déclaré la requête recevable.

5. Tant le requérant que le Gouvernement ont déposé des observations écrites complémentaires (article 59 § 1 du règlement). La chambre ayant décidé après consultation des parties qu'il n'y avait pas lieu de tenir une audience consacrée au fond de l'affaire (article 59 § 3 *in fine*), les parties ont chacune soumis des commentaires écrits sur les observations de l'autre. Par ailleurs, des observations ont été reçues de la Fondation Helsinki pour les droits de l'homme, que le président avait autorisée à intervenir dans la procédure écrite (articles 36 § 2 de la Convention et 44 § 2 du règlement).

EN FAIT

I. LES CIRCONSTANCES DE L'ESPÈCE

6. Le requérant est né en 1986.

7. Le 15 mars 1999, alors qu'il était âgé de douze ans, une ou plusieurs personnes non identifiées publièrent à son insu une annonce à son nom sur un site de rencontres par Internet. L'annonce mentionnait son âge et son année de naissance et le décrivait physiquement de manière détaillée. Elle contenait également un lien vers sa page web, où figuraient sa photographie et son numéro de téléphone, exact à un chiffre près ; et elle indiquait qu'il recherchait une relation intime avec un garçon de son âge ou plus âgé que lui afin qu'il lui « montre comment on fait ».

8. Le requérant prit connaissance de cette annonce lorsqu'il reçut un courrier électronique d'un homme qui lui proposait de le rencontrer et « de voir ensuite ce qu'[il] voulait ».

9. Le père du requérant demanda à la police d'identifier l'auteur de l'annonce afin d'intenter contre lui une action en justice. Le fournisseur d'accès refusa de communiquer l'identité du détenteur de l'adresse dynamique IP (Protocole Internet) correspondante, s'estimant lié par la confidentialité des télécommunications prévue par la loi.

10. La police demanda alors au tribunal de district (*käräjäoikeus, tingsrätten*) d'Helsinki d'obliger le fournisseur d'accès à divulguer l'information en vertu de l'article 28 de la loi sur les enquêtes pénales (*esitutkintalaki, förundersökningslagen*, loi n° 449/1987 modifiée par la loi n° 692/1997).

11. Par une décision rendue le 19 janvier 2001, le tribunal de district rejeta cette demande au motif qu'aucune disposition légale ne permettait expressément d'obliger le fournisseur d'accès à rompre le secret professionnel et à divulguer des données permettant l'identification des utilisateurs de télécommunications. Le tribunal jugea que l'article 3 du chapitre 5a de la loi sur les mesures de contrainte (*pakkokeinolaki, tvångsmedelslagen*, loi n° 450/1987) et l'article 18 de la loi sur la protection de la vie privée et la sécurité des données dans les télécommunications (*laki yksityisyydensuojasta televiestinnässä ja teletoiminnan tietoturvasta, lag om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet*, loi n° 565/1999) autorisaient certes la police à se faire communiquer des données permettant l'identification des utilisateurs de télécommunications pour certaines infractions, nonobstant l'obligation de confidentialité, mais que la diffamation ne faisait pas partie de ces infractions.

12. Le 14 mars 2001, la cour d'appel (*hovioikeus, hovrätten*) confirma ce jugement et, le 31 août 2001, la Cour suprême (*korkein oikeus, högsta domstolen*) refusa à l'appelant l'autorisation de la saisir.

13. La personne qui avait répondu à l'annonce de rencontre et contacté le requérant fut identifiée grâce à son adresse de messagerie électronique.

14. Il ne fut pas possible d'engager une action pénale contre le gérant du fournisseur d'accès à Internet, le procureur ayant conclu dans une décision du 2 avril 2001 à la prescription de l'infraction à la loi sur les données personnelles (*henkilötietolaki, personuppgiftslagen*, loi n° 523/1999, entrée en vigueur le 1er juin 1999) censée être résultée de ce que le fournisseur d'accès avait publié sur son site une annonce diffamatoire sans vérifier l'identité de son auteur.

II. LE DROIT ET LA PRATIQUE INTERNES PERTINENTS

15. La loi sur la Constitution finlandaise (*Suomen hallitusmuoto, Regeringsform för Finland*, loi n° 94/1919 modifiée par la loi n° 969/1995) est restée en vigueur jusqu'au 1er mars 2000. L'article 8 de cette loi correspondait à l'article 10 de la Constitution finlandaise actuelle (*Suomen perustuslaki, Finlands grundlag*, loi n° 731/1999), qui dispose que le droit de chacun à la vie privée est garanti.

16. Au moment des faits, l'article 3 du chapitre 27 du code pénal (*rikoslaki, strafflagen*, loi n° 908/1974) était ainsi libellé :

> « Quiconque, d'une manière autre que celle visée ci-dessus, diffame autrui par une déclaration insultante, une menace ou un autre acte dégradant, est condamné pour diffamation à une amende ou à une peine de prison d'une durée maximale de trois mois.
>
> Si la diffamation est commise en public ou par écrit, si elle est publiée, ou si elle se trouve dans une représentation graphique diffusée par l'auteur ou dont l'auteur est à l'origine, le responsable est condamné à une amende ou à une peine de prison d'une durée maximale de quatre mois. »

17. Au moment des faits, l'article 3 du chapitre 5a de la loi sur les mesures de contrainte se lisait ainsi :

> **« Conditions préalables à la surveillance des télécommunications**
>
> 1) d'une infraction passible d'une peine de prison d'au moins quatre mois ;
>
> 2) d'une infraction contre un système informatique utilisant un terminal, d'une infraction en matière de stupéfiants ; ou
>
> 3) d'une tentative répréhensible de commission de l'une des infractions visées au présent article ;
>
> l'autorité menant l'enquête pénale peut être autorisée à surveiller une ligne de télécommunications détenue par le suspect ou présumée être utilisée par lui, ou à la désactiver temporairement, si les informations censées être obtenues par la surveillance ou la désactivation de la ligne sont susceptibles de présenter une importance majeure pour l'enquête sur l'infraction en question (...) »

18. L'article 18 § 1, alinéa 1, de la loi sur la protection de la vie privée et la sécurité des données dans les télécommunications, entrée en vigueur le 1er juillet 1999 et abrogée le 1er septembre 2004, était ainsi libellé :

> « Nonobstant l'obligation de confidentialité prévue à l'article 7, la police a le droit de se faire communiquer :
>
> 1) les données d'identification relatives aux transmissions vers un transcripteur donné, avec le consentement de la partie lésée et du détenteur de l'abonnement à la ligne, si ces données sont nécessaires aux fins d'une enquête sur une infraction visée à l'article 9a du chapitre 16, à l'article 13, alinéa 2, du chapitre 17, ou à l'article 3a du chapitre 24 du code pénal (loi nº 39/1889) (...) »

19. L'article 48 de la loi sur les données personnelles dispose que le fournisseur d'accès engage sa responsabilité pénale s'il ne vérifie pas l'identité de l'auteur avant de publier sur son site web une annonce diffamatoire. En vertu de l'article 47, sa responsabilité civile est également engagée.

20. Au moment des faits, le traitement et la publication sur un serveur Internet d'informations sensibles relatives à un comportement sexuel sans le consentement de la personne concernée était constitutif d'une infraction pénale en vertu de l'article 43 de la loi nº 630/1995 sur les dossiers personnels et de l'article 9 du chapitre 38 du code pénal (loi nº 578/1995), ainsi que d'une violation de l'obligation de protection des données énoncée à l'article 44 de la loi sur les dossiers personnels. En outre, elle pouvait faire naître une responsabilité civile en vertu de l'article 42 de la loi nº 471/1987 sur les dossiers personnels.

21. L'article 17 de la loi sur l'exercice de la liberté d'expression dans les médias (*laki sanavapauden käyttämisestä joukkoviestinnässä, lagen om yttrandefrihet i masskommunikation*, loi nº 460/2003), qui est entrée en vigueur le 1er janvier 2004, énonce ceci :

> **« Communication d'informations identifiantes pour les messages sur réseau**
>
> A la demande d'un agent habilité à procéder à des arrestations, d'un procureur ou d'une partie lésée, un tribunal peut ordonner à l'exploitant d'un transmetteur, d'un serveur ou d'un autre dispositif analogue de communiquer au demandeur les informations nécessaires à l'identification de l'expéditeur d'un message sur le réseau, sous réserve qu'existent des motifs raisonnables de penser que la teneur du message est telle que le fait de le rendre public constitue une infraction pénale. Cependant, la communication à la partie lésée des informations relatives à l'identité de l'expéditeur ne peut être ordonnée que dans le cas où ladite partie a le droit d'engager des poursuites privées relativement à l'infraction en question. La demande doit être introduite devant le tribunal de district du lieu de domiciliation de l'exploitant du dispositif ou devant le tribunal de district d'Helsinki dans les trois mois suivant la publication du message. Le tribunal peut assortir l'ordonnance correspondante d'une astreinte pécuniaire. »

III. LES DOCUMENTS INTERNATIONAUX PERTINENTS

A. Le Conseil de l'Europe

22. Le développement rapide des technologies des télécommunications ces dernières décennies a d'une part fait apparaître de nouvelles formes de criminalité et d'autre part permis l'émergence de nouveaux modes de commission d'infractions déjà connues. Le Conseil de l'Europe a reconnu l'importance d'une réponse adéquate et rapide à ce nouveau défi dès 1989, année où le Comité des ministres a adopté la Recommandation N° R (89) 9 sur la criminalité en relation avec l'ordinateur. Résolu à faire en sorte que les autorités d'enquête soient investies des pouvoirs spéciaux appropriés aux fins des investigations sur les infractions en relation avec l'ordinateur, le Comité des ministres a adopté en 1995 la Recommandation N° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information. Au point 12 des principes figurant en annexe de cette recommandation, il a estimé que :

> « Des obligations spécifiques devraient être établies pour les fournisseurs de services qui offrent des services de télécommunication au public via des réseaux de communication publics ou privés, de délivrer l'information nécessaire, lorsque les autorités compétentes chargées de l'enquête l'ordonnent, pour identifier l'utilisateur. »

23. Les autres principes relatifs à l'obligation de coopérer avec les autorités d'enquête sont les suivants :

> « 9. Sous la réserve des protections ou privilèges prévus par la loi, la plupart des législations permettent aux autorités chargées de l'enquête d'ordonner à des personnes de remettre des objets qui sont sous leur contrôle et qui sont requis pour servir de preuve. Le droit de procédure pénale devrait, de la même manière, accorder le pouvoir d'ordonner à des personnes de leur présenter toute donnée spécifique qui se trouve sous leur contrôle, dans un système informatique, dans la forme requise par les autorités chargées de l'enquête.
>
> 10. Sous la réserve des protections ou privilèges prévus par la loi, les autorités chargées de l'enquête devraient avoir le pouvoir d'ordonner aux personnes qui ont des données spécifiques sous leur contrôle de fournir toutes les informations nécessaires pour permettre l'accès au système informatique et aux données qu'il renferme. Le droit de procédure pénale devrait assurer que les autorités chargées de l'enquête puissent donner une instruction similaire à d'autres personnes ayant une connaissance du fonctionnement du système informatique ou de toute mesure employée pour préserver les données y contenues. »

24. En 1996, le Comité européen pour les problèmes criminels a créé un comité d'experts chargés de la cybercriminalité. L'idée était que, bien que les deux précédentes recommandations sur les dispositions matérielles et procédurales ne fussent pas restées vaines, seul un instrument international contraignant pourrait garantir l'efficacité nécessaire en matière de lutte contre les infractions commises dans le cyberespace. La Convention sur la

cybercriminalité a été ouverte à la signature le 23 novembre 2001. Elle est entrée en vigueur le 1er juillet 2004. Ouverte à tous les Etats, elle constitue le premier et le seul traité international sur les infractions commises via Internet. Elle impose d'incriminer les agissements suivants : accès illégal à un système informatique, interception illégale de données informatiques, atteinte à l'intégrité des données ou du système, abus de dispositifs, falsification et fraude informatiques, pornographie enfantine, atteinte à la propriété intellectuelle et aux droits connexes. Le protocole additionnel à cette convention, adopté en 2003, impose en outre l'incrimination des discours haineux, de la xénophobie et du racisme. Les dispositions procédurales de cette convention ont une portée qui dépasse les infractions définies dans le texte, puisqu'elles s'appliquent à toute infraction commise au moyen d'un ordinateur :

Article 14
Portée d'application des mesures du droit de procédure

« 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. (...) chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :

a) aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;

b) à toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c) à la collecte des preuves électroniques de toute infraction pénale.

(...) »

25. Les mesures procédurales qu'il est possible de prendre sont les suivantes : conservation rapide de données informatiques stockées, conservation et divulgation partielle rapides de données relatives au trafic, injonction de produire, perquisition et saisie de données informatiques stockées, collecte en temps réel des données relatives au trafic et interception de données relatives au contenu. Une procédure particulièrement pertinente dans le cadre de la présente affaire est celle par laquelle il est possible d'ordonner à un fournisseur d'accès de communiquer les données relatives aux abonnés à ses services. De fait, le rapport explicatif décrit la difficulté d'identifier l'auteur comme l'un des problèmes les plus difficiles que pose la lutte contre la criminalité dans l'univers des réseaux :

Article 18 – Injonction de produire

« 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a) à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et

b) à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b) l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. »

26. Le rapport explicatif indique que, dans le cadre d'une enquête pénale, les informations relatives aux abonnés peuvent être nécessaires principalement dans deux situations. Premièrement, pour déterminer les services et mesures techniques connexes qui ont été ou sont utilisés par un abonné, tels que le type de service téléphonique, le type de services connexes (renvoi automatique d'appel, messagerie téléphonique), le numéro de téléphone ou toute autre adresse technique (comme une adresse électronique). Deuxièmement, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé. Une injonction de produire constitue une mesure moins contraignante et moins onéreuse que les services répressifs peuvent mettre en œuvre à la place d'autres mesures telles que l'interception de données relatives au contenu et la collecte en temps réel des données relatives au trafic, qui doivent ou peuvent être limitées exclusivement aux infractions graves (articles 20 et 21).

27. Une conférence internationale sur la coopération contre la cybercriminalité réunie à Strasbourg les 1er et 2 avril 2008 a adopté des

Lignes directrices pour la coopération entre organes de répression et fournisseurs de services Internet contre la cybercriminalité. L'objectif de ces lignes directrices est d'aider les forces de l'ordre et les fournisseurs d'accès à Internet à structurer leurs interactions en lien avec les questions de cybercriminalité. Afin d'optimiser la cybersécurité et de réduire l'utilisation des services à des fins illicites, on a considéré qu'il était fondamental que les deux parties coopèrent efficacement. Les lignes directrices exposent les mesures pratiques que devraient prendre les forces de l'ordre et les fournisseurs d'accès, et engagent les premières et les seconds à échanger des informations afin de renforcer leur capacité à identifier et à combattre les nouvelles formes de cybercriminalité. En particulier, elles invitent les fournisseurs d'accès à coopérer avec les forces de l'ordre afin de contribuer à la réduction de l'utilisation des services pour des activités criminelles telles que les définit le droit.

B. L'Organisation des Nations unies

28. Les Nations unies ont adopté un certain nombre de résolutions relativement au cyberespace. Les plus pertinentes aux fins de la présente affaire sont les Résolutions 55/63 et 56/121 sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles adoptées par l'Assemblée générale, en date respectivement du 4 décembre 2000 et du 19 décembre 2001. Parmi les mesures à appliquer à cette fin, on trouve dans la résolution 55/63 la recommandation suivante :

> « 1. (…)
>
> f) Les systèmes juridiques devraient permettre de préserver les données électroniques concernant une enquête pénale particulière et d'y avoir accès rapidement ;
>
> (...) »

29. Dans la résolution suivante, l'Assemblée générale a pris note de la valeur de ces mesures et invité à nouveau les Etats membres à en tenir compte.

C. L'Union européenne

30. Le 15 mars 2006, le Parlement européen et le Conseil de l'Union européenne ont adopté la Directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE relative à la conservation des données. Cette directive a pour objectif d'harmoniser les dispositions des Etats membres relatives aux obligations des fournisseurs de

services de communications en matière de conservation de certaines données, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque Etat membre dans son droit interne. Elle s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques. Elle impose aux Etats membres de veiller à ce que certaines catégories de données soient conservées pendant une période de six mois à deux ans. L'article 5 précise les données à conserver :

> « 1. Les Etats membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes :
>
> a) les données nécessaires pour retrouver et identifier la source d'une communication :
>
> (...)
>
> 2) en ce qui concerne l'accès à Internet, le courrier électronique par Internet et la téléphonie par Internet :
>
> (...) ;
>
> iii) les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (Protocole Internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication ;
>
> (…) »

31. Les Etats membres avaient jusqu'au 15 septembre 2007 pour mettre en œuvre cette directive. Seize Etats, dont la Finlande, ont toutefois utilisé leur droit de différer jusqu'au 15 mars 2009 son application à l'accès à Internet, à la téléphonie par Internet et au courrier électronique par Internet.

IV. LE DROIT COMPARÉ

32. Une étude comparée de la législation nationale des différents Etats membres du Conseil de l'Europe montre que, dans la plupart d'entre eux, il pèse sur les fournisseurs de services de télécommunications une obligation spécifique de communication des données informatiques, y compris celles relatives à l'abonné, à la demande des autorités d'enquête ou des autorités judiciaires, quelle que soit la nature de l'infraction. Certains pays ont simplement des dispositions générales relatives à la production de documents et d'autres données, qui pourraient en pratique recouvrir également l'obligation de communiquer certaines données informatiques ou relatives aux abonnés. Plusieurs pays n'ont pas encore mis en œuvre les

dispositions de l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité.

V. LES OBSERVATIONS DE LA PARTIE INTERVENANTE

33. La Fondation Helsinki pour les droits de l'homme estime que la présente affaire pose la question de l'équilibre entre la protection de la vie privée, de l'honneur et de la réputation et l'exercice de la liberté d'expression. Elle est d'avis que c'est là pour la Cour l'occasion de définir les obligations positives de l'Etat dans ce domaine, et ainsi de favoriser l'émergence de normes communes en matière d'utilisation d'Internet dans tous les Etats membres.

34. Elle souligne qu'Internet est un mode de communication très particulier, dont l'un des principes fondamentaux est l'anonymat. Le caractère quasi absolu de cet anonymat favoriserait la liberté de parole et l'expression d'idées différentes. D'un autre côté, il placerait les victimes potentielles dans une position vulnérable face à ceux qui souhaiteraient les insulter, les diffamer ou violer leur droit à la vie privée, agresseurs pour lesquels il constituerait un outil puissant. A la différence des moyens de communication classiques, Internet ne permettrait pas d'identifier facilement l'auteur d'une diffamation, celui-ci pouvant se cacher derrière un pseudonyme ou même utiliser une fausse identité.

EN DROIT

I. SUR LA VIOLATION ALLÉGUÉE DES ARTICLES 8 ET 13 DE LA CONVENTION

35. Invoquant les articles 8 et 13 de la Convention, le requérant dénonce une atteinte à sa vie privée et se plaint de ne pas avoir eu de recours effectif permettant de découvrir l'identité de la personne qui avait publié sur Internet, en son nom, un texte diffamatoire.

L'article 8 est ainsi libellé :

> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. 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. »

L'article 13 énonce ceci :

« Toute personne dont les droits et libertés reconnus dans la (...) Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles. »

A. Thèses des parties

36. Le requérant soutient que la législation finlandaise de l'époque protégeait le criminel tandis que la victime n'avait aucun moyen de se protéger contre des atteintes à sa vie privée ou d'obtenir réparation en cas de telles atteintes. L'acte litigieux aurait de fait été pénalement répréhensible, mais le Gouvernement aurait négligé de veiller à la cohérence des dispositions respectives de la loi nº 565/1999 sur la protection de la vie privée et la sécurité des données dans les télécommunications et de la loi nº 450/1987 sur les mesures de contrainte. La possibilité aléatoire de demander des dommages-intérêts, en particulier à un tiers, ne suffirait pas à protéger les droits de la victime. A cet égard, le requérant souligne qu'il n'a pas eu la possibilité d'identifier la personne qui avait publié l'annonce sur Internet. Il estime que si l'indemnisation peut dans certains cas constituer un recours effectif, encore faut-il qu'elle soit versée par l'auteur de l'atteinte aux droits de la victime. Or tel n'aurait pas été le cas en l'espèce. A l'argument du Gouvernement selon lequel de nouveaux textes de loi ont été adoptés qui, s'ils avaient existé au moment des faits, auraient rendu ce recours inutile, le requérant répond que le Gouvernement était censé lui accorder la protection voulue au moment des faits et qu'il a manqué à cette obligation. Il estime ainsi avoir été victime de violations des articles 8 et 13 de la Convention.

37. Le Gouvernement souligne qu'en l'espèce l'atteinte à la vie privée du requérant a été commise par un tiers. Il indique que l'acte litigieux était considéré en droit interne comme un acte diffamatoire et, à ce titre, passible de sanctions, dont il estime qu'elles avaient un effet dissuasif. Une enquête aurait été ouverte pour identifier l'auteur de l'annonce publiée sur Internet, et son échec serait dû à la législation alors en vigueur, qui visait à protéger la liberté d'expression et le droit à l'anonymat de l'expression. La protection accordée par cette législation aux personnes publiant anonymement des messages sur Internet aurait également profité aux auteurs de messages susceptibles de porter atteinte à la vie privée de tiers. Cet effet connexe de la protection en cause aurait été dû au fait que la notion de message portant atteinte à la protection de la vie privée n'était alors pas clairement définie, et qu'il n'était donc pas possible d'exclure avec précision de tels messages de la protection de la loi. Il y aurait cependant eu d'autres possibilités d'obtenir

réparation, par exemple en vertu de la loi n° 523/1999 sur les données personnelles, qui aurait apporté une protection contre la diffamation en obligeant l'exploitant du serveur, par des dispositions engageant sa responsabilité civile et pénale, à garantir que les données sensibles enregistrées par lui ne soient traitées qu'avec le consentement de la personne concernée. Le Gouvernement ajoute que, même si les infractions en matière de données personnelles étaient déjà prescrites, le requérant avait toujours la possibilité de se faire indemniser par la personne qui avait publié l'annonce. Comparant la présente espèce avec l'affaire *X et Y c. Pays-Bas* (26 mars 1985, série A n° 91), il estime qu'en l'occurrence, où l'infraction considérée était moins grave, la responsabilité civile offrait un effet dissuasif suffisant. De plus, le requérant aurait eu à sa disposition d'autres mécanismes, tels que l'enquête de police préliminaire, les poursuites pénales, et la demande de dommages-intérêts, au besoin par la voie judiciaire.

38. Selon le Gouvernement, il importe de replacer la situation législative au moment des faits dans son contexte social, à savoir une augmentation rapide et récente de l'utilisation d'Internet. La législation actuelle, c'est-à-dire la loi n° 460/2003 sur l'exercice de la liberté d'expression dans les médias (articles 2 et 17), entrée en vigueur le 1er janvier 2004, donnerait à la police des pouvoirs plus larges pour lever, aux fins d'une enquête pénale, la protection des personnes ayant publié anonymement un message sur Internet. Le nouveau texte serait né de la réaction du législateur face à l'évolution de la société, dans laquelle le développement de l'utilisation – et, dans le même temps, des abus – d'Internet aurait appelé une redéfinition des limites de cette protection. Ainsi, la société ayant changé, le législateur aurait renforcé la protection de la vie privée par rapport à celle de la liberté d'expression, et en particulier celle des personnes publiant anonymement des messages sur Internet.

39. Cela étant, le point essentiel en l'espèce serait que même la législation en vigueur au moment des faits offrait au requérant des moyens de se défendre contre la diffusion de messages portant atteinte à sa vie privée, puisque l'exploitant du serveur Internet sur lequel le message avait été publié était légalement tenu de vérifier que la personne concernée avait consenti au traitement sur le serveur d'informations sensibles la concernant. Cette obligation aurait été renforcée par une responsabilité pénale et civile en cas de manquement. Ainsi, les textes en vigueur auraient offert au requérant une protection de sa vie privée suffisante et des recours effectifs.

B. Appréciation de la Cour

40. La Cour note d'emblée que le requérant, qui était à l'époque un mineur de douze ans, a fait l'objet d'une annonce à caractère sexuel sur un site de rencontres par Internet. Or la législation alors en vigueur n'a pas

permis d'obtenir du fournisseur d'accès à Internet l'identité de la personne qui avait passé l'annonce.

41. La présente affaire relève sans conteste de l'article 8 de la Convention : les faits à l'origine de la requête concernent une question de « vie privée », notion qui recouvre l'intégrité physique et morale de la personne (*X et Y c. Pays-Bas*, précité, § 22). Même si, en droit interne, l'affaire a été envisagée sous l'angle de la diffamation, la Cour préfère s'attacher à ces aspects particuliers de la notion de vie privée, compte tenu du risque physique et moral que la situation litigieuse pouvait comporter pour le requérant et de la vulnérabilité due à son jeune âge.

42. La Cour rappelle que, si l'article 8 a essentiellement pour objet de prémunir l'individu contre des ingérences arbitraires des pouvoirs publics, il ne se contente pas d'astreindre l'Etat à s'abstenir de pareilles ingérences : à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée ou familiale (*Airey c. Irlande*, 9 octobre 1979, § 32, série A n° 32).

43. Ces obligations peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux. Il existe différentes manières d'assurer le respect de la vie privée et la nature de l'obligation de l'Etat dépend de l'aspect de la vie privée qui se trouve en cause. Si le choix des moyens d'assurer le respect de l'article 8 dans le domaine de la protection contre les actes d'individus relève en principe de la marge d'appréciation de l'Etat, une dissuasion effective contre des actes graves mettant en jeu des valeurs fondamentales et des aspects essentiels de la vie privée appelle des dispositions pénales efficaces (*X et Y c. Pays-Bas*, précité, §§ 23, 24 et 27, *August c. Royaume-Uni* (déc.), n° 36505/02, 21 janvier 2003, et *M.C. c. Bulgarie*, n° 39272/98, § 150, CEDH 2003-XII).

44. Les limites de la marge d'appréciation des autorités nationales sont néanmoins tracées par les dispositions de la Convention. Celle-ci étant avant tout un mécanisme de protection des droits de l'homme, la Cour doit, lorsqu'elle interprète ses dispositions, tenir compte de l'évolution de la situation dans les Etats contractants et réagir, par exemple, au consensus susceptible de se faire jour quant aux normes à atteindre (*Christine Goodwin c. Royaume-Uni* [GC], n° 28957/95, § 74, CEDH 2002-VI).

45. En l'espèce, la Cour considère que, même si l'affaire n'atteint pas le degré de gravité de *X et Y c. Pays-Bas*, où la violation de l'article 8 était née de ce que le viol d'une jeune fille handicapée n'avait entraîné aucune sanction pénale effective, elle ne doit pas être sous-estimée. L'acte litigieux était de nature pénale, et il concernait un mineur, désigné comme cible pour les pédophiles (voir également, à cet égard, le paragraphe 41 ci-dessus).

46. Le Gouvernement reconnaît qu'à l'époque on ne pouvait ordonner à l'exploitant du serveur de communiquer les informations propres à permettre d'identifier l'auteur des actes. Il soutient que la victime était protégée par le simple fait qu'il existait dans le droit pénal une incrimination

pour l'acte litigieux et qu'il était possible d'intenter une action pénale ou une action en réparation contre l'exploitant du serveur. Sur le premier point, la Cour observe que l'existence d'une incrimination ne peut produire qu'un effet dissuasif limité s'il n'est pas possible d'identifier l'auteur des actes incriminés et de le traduire en justice. Elle note qu'elle n'a pas exclu dans sa jurisprudence que les obligations positives de sauvegarde de l'intégrité physique et morale de l'individu incombant à l'Etat en vertu de l'article 8 puissent s'étendre aux questions relatives à l'effectivité d'une enquête pénale, même lorsque la responsabilité pénale des agents de l'Etat n'est pas en cause (*Osman c. Royaume-Uni*, 28 octobre 1998, § 128, *Recueil des arrêts et décisions* 1998-VIII). Elle estime que les Etats ont l'obligation positive, inhérente à l'article 8 de la Convention, d'adopter des dispositions en matière pénale qui sanctionnent effectivement les infractions contre la personne, y compris les tentatives, et de renforcer l'effet dissuasif de l'incrimination en les appliquant en pratique à travers une enquête et des poursuites effectives (voir, *mutatis mutandis*, *M.C. c. Bulgarie*, précité, § 153). Lorsque le bien-être physique et moral d'un enfant est menacé, cette obligation revêt une importance plus grande encore. La Cour rappelle à cet égard que les abus sexuels constituent incontestablement un type odieux de méfaits qui fragilisent les victimes. Les enfants et autres personnes vulnérables ont droit à la protection de l'Etat, sous la forme d'une prévention efficace les mettant à l'abri de formes aussi graves d'ingérence dans des aspects essentiels de leur vie privée (*Stubbings et autres c. Royaume-Uni*, 22 octobre 1996, § 64, *Recueil* 1996-IV).

47. Quant à l'argument du Gouvernement selon lequel le requérant avait la possibilité d'obtenir une indemnisation d'un tiers, à savoir le fournisseur d'accès, la Cour considère que cet élément n'était pas suffisant dans les circonstances de l'espèce. Il est évident que tant l'intérêt public que la protection des intérêts des victimes d'infractions commises contre leur bien-être physique ou psychologique commandent que soit disponible un recours permettant d'identifier l'auteur des faits (en l'espèce la personne qui a passé l'annonce au nom du requérant) et de le traduire en justice, de sorte que la victime puisse obtenir une réparation pécuniaire de cette personne.

48. La Cour admet que compte tenu des difficultés pour la police d'exercer ses fonctions dans les sociétés contemporaines, il faut interpréter les obligations positives de manière à ne pas imposer aux autorités ou, ici, au législateur un fardeau insupportable ou excessif. Une autre considération pertinente est la nécessité de s'assurer que le pouvoir de juguler et de prévenir la criminalité et d'enquêter à cette fin soit exercé d'une manière qui respecte pleinement les voies légales et autres garanties qui limitent légitimement l'étendue des actes d'investigation criminelle et de traduction des délinquants en justice, y compris les garanties figurant aux articles 8 et 10 de la Convention, garanties sur lesquelles les auteurs d'infractions peuvent eux-mêmes compter. La Cour est sensible à

l'argument du Gouvernement selon lequel tout défaut du cadre législatif doit être replacé dans le contexte social de son époque. Elle note cependant que les faits datent de 1999, c'est-à-dire d'un moment où il était bien connu qu'Internet, précisément en raison de son caractère anonyme, pouvait être utilisé à des fins criminelles (paragraphes 22 et 24 ci-dessus). De plus, la connaissance du problème répandu des abus sexuels sur des enfants s'était largement développée au cours des dix années précédentes. On ne saurait donc dire que le gouvernement défendeur n'avait pas eu l'occasion de mettre en place un système de protection des enfants face aux pédophiles sur Internet.

49. La Cour considère qu'une protection pratique et effective du requérant impliquait l'adoption de mesures efficaces pour identifier et poursuivre l'auteur, c'est-à-dire la personne qui avait passé l'annonce. Or pareilles mesures n'ont pas été prises. La prépondérance ayant été accordée à l'exigence de confidentialité, il n'a jamais été possible de procéder à une enquête efficace. Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. Sans préjudice de la question de savoir si, compte tenu de sa nature répréhensible, la conduite de la personne ayant passé l'annonce illégale sur Internet relève ou non de la protection des articles 8 et 10, le législateur aurait dû en tout cas prévoir un cadre permettant de concilier les différents intérêts à protéger dans ce contexte. Un tel cadre n'était pas en place au moment des faits, de sorte que la Finlande n'a pu s'acquitter de son obligation positive à l'égard du requérant. S'il a été remédié à cette lacune ultérieurement, les mécanismes mis en place par la loi sur l'exercice de la liberté d'expression dans les médias (paragraphe 21 ci-dessus) sont arrivés trop tard pour le requérant.

50. La Cour conclut donc qu'il y a eu violation de l'article 8 de la Convention en l'espèce.

51. Eu égard à sa conclusion sur le terrain de l'article 8, la Cour considère qu'il n'est pas nécessaire d'examiner le grief sous l'angle de l'article 13 (voir, notamment, *Sallinen et autres c. Finlande*, n° 50882/99, §§ 102 et 110, 27 septembre 2005, et *Copland c. Royaume-Uni*, n° 62617/00, §§ 50-51, CEDH 2007-I).

II. SUR L'APPLICATION DE L'ARTICLE 41 DE LA CONVENTION

52. Aux termes de l'article 41 de la Convention,

> « Si la Cour déclare qu'il y a eu violation de la Convention ou de ses Protocoles, et si le droit interne de la Haute Partie contractante ne permet d'effacer qu'imparfaitement les conséquences de cette violation, la Cour accorde à la partie lésée, s'il y a lieu, une satisfaction équitable. »

A. Dommage

53. Le requérant demande 3 500 euros (EUR) pour le préjudice moral qu'il estime avoir subi.

54. Le Gouvernement estime que la somme éventuellement octroyée ne devrait pas dépasser 2 500 EUR.

55. La Cour juge établi que le requérant a subi un dommage moral. Elle considère que le seul constat d'une violation ne suffirait pas à apporter une satisfaction équitable à cet égard, et que l'octroi d'une indemnisation est donc nécessaire. Statuant en équité, elle alloue au requérant la somme de 3 000 EUR à ce titre.

B. Frais et dépens

56. Le requérant demande 2 500 EUR au titre des frais et dépens qu'il dit avoir engagés devant les juridictions nationales et devant la Cour.

57. Le Gouvernement pose la question de savoir si l'intéressé a communiqué les justificatifs nécessaires.

58. La Cour constate que le requérant ne lui a communiqué aucun justificatif au sens de l'article 60 du règlement. Cette demande doit donc être rejetée.

C. Intérêts moratoires

59. La Cour juge approprié de calquer le taux des intérêts moratoires sur le taux d'intérêt de la facilité de prêt marginal de la Banque centrale européenne majoré de trois points de pourcentage.

PAR CES MOTIFS, LA COUR, À L'UNANIMITÉ,

1. *Dit* qu'il y a eu violation de l'article 8 de la Convention ;

2. *Dit* qu'il n'est pas nécessaire d'examiner le grief tiré de l'article 13 de la Convention ;

3. *Dit*

a) que l'Etat défendeur doit verser au requérant, dans les trois mois à compter du jour où l'arrêt sera devenu définitif en vertu de l'article 44 § 2 de la Convention, 3 000 EUR (trois mille euros) pour dommage moral, plus tout montant pouvant être dû sur cette somme à titre d'impôt ;

b) qu'à compter de l'expiration dudit délai et jusqu'au versement, ce montant sera à majorer d'un intérêt simple à un taux égal à celui de la facilité de prêt marginal de la Banque centrale européenne applicable pendant cette période, augmenté de trois points de pourcentage ;

4. *Rejette* la demande de satisfaction équitable pour le surplus.

Fait en anglais, puis communiqué par écrit le 2 décembre 2008, en application de l'article 77 §§ 2 et 3 du règlement.

Lawrence Early
Greffier

Nicolas Bratza
Président