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

FOURTH SECTION

CASE OF K.U. v. FINLAND

(Application no. 2872/02)

JUDGMENT

STRASBOURG

2 December 2008

FINAL

02/03/2009

In the case of K.U. v. Finland,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Nicolas Bratza, *President*,
Lech Garlicki,
Giovanni Bonello,
Ljiljana Mijović,
Davíd Thór Björgvinsson,
Ján Šikuta,
Päivi Hirvelä, *judges*,
and Lawrence Early, *Section Registrar*,

Having deliberated in private on 13 November 2008,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 2872/02) against the Republic of Finland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Finnish national ("the applicant"), on 1 January 2002. The President of the Chamber acceded to the applicant's request not to have his name disclosed (Rule 47 § 3 of the Rules of Court).

2. The applicant was represented by Mr P. Huttunen, a lawyer practising in Helsinki. The Finnish Government ("the Government") were represented by their Agent, Mr A. Kosonen of the Ministry of Foreign Affairs.

3. The applicant alleged, in particular, that the State had failed in its positive obligation to protect his right to respect for private life under Article 8 of the Convention.

4. By a decision of 27 June 2006, the Court declared the application admissible.

5. The applicant and the Government each filed further observations (Rule 59 § 1). The Chamber having decided, after consulting the parties, that no hearing on the merits was required (Rule 59 § 3 *in fine*), the parties replied in writing to each other's observations. In addition, third-party comments were received from the Helsinki Foundation for Human Rights, which had been given leave by the President to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 2).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

6. The applicant was born in 1986.

7. On 15 March 1999 an unidentified person or persons placed an advertisement on an Internet dating site in the name of the applicant, who was 12 years old at the time, without his knowledge. The advertisement mentioned his age and year of birth, gave a detailed description of his physical characteristics, a link to the web page he had at the time, which showed his picture, as well as his telephone number, which was accurate save for one digit. In the advertisement, it was claimed that he was looking for an intimate relationship with a boy of his age or older "to show him the way".

8. The applicant became aware of the advertisement on the Internet when he received an e-mail from a man, offering to meet him and "then to see what you want".

9. The applicant's father requested the police to identify the person who had placed the advertisement in order to bring charges against that person. The service provider, however, refused to divulge the identity of the holder of the so-called dynamic Internet Protocol (IP) address in question, regarding itself bound by the confidentiality of telecommunications as defined by law.

10. The police then asked the Helsinki District Court (*käräjäoikeus, tingsrätten*) to oblige the service provider to divulge the said information pursuant to section 28 of the Criminal Investigations Act (*esitutkintalaki, förundersökningslagen*; Act no. 449/1987, as amended by Act no. 692/1997).

11. In a decision issued on 19 January 2001, the District Court refused since there was no explicit legal provision authorising it to order the service provider to disclose telecommunications identification data in breach of professional secrecy. The court noted that by virtue of Chapter 5a, section 3, of the Coercive Measures Act (*pakkokeinolaki, tvångsmedelslagen*; Act no. 450/1987) and section 18 of the Protection of Privacy and Data Security in Telecommunications Act (*laki yksityisyydensuojasta televiestinnässä ja teletoiminnan tietoturvasta, lag om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet*; Act no. 565/1999) the police had the right to obtain telecommunications identification data in cases concerning certain offences, notwithstanding the obligation to observe secrecy. However, malicious misrepresentation was not such an offence.

12. On 14 March 2001 the Court of Appeal (*hovioikeus, hovrätten*) upheld the decision and on 31 August 2001 the Supreme Court (*korkein oikeus, högsta domstolen*) refused leave to appeal.

13. The person who had answered the dating advertisement and contacted the applicant was identified through his e-mail address.

14. The managing director of the company which provided the Internet service could not be charged, because in his decision of 2 April 2001 the prosecutor found that the alleged offence had become time-barred. The alleged offence was a violation of the Personal Data Act (*henkilötietolaki, personuppgiftslagen*; Act no. 523/99, which came into force on 1 June 1999). More specifically, the service provider had published a defamatory advertisement on its website without verifying the identity of the sender.

II. RELEVANT DOMESTIC LAW AND PRACTICE

15. The Finnish Constitution Act (*Suomen hallitusmuoto, Regeringsform för Finland*; Act no. 94/1919, as amended by Act no. 969/1995) was in force until 1 March 2000. Its section 8 corresponded to Article 10 of the current Finnish Constitution (*Suomen perustuslaki, Finlands grundlag*; Act no. 731/1999), which provides that everyone's right to private life is guaranteed.

16. At the material time, Chapter 27, Article 3, of the Penal Code (*rikoslaki, strafflagen*; Act no. 908/1974) provided:

> "A person who in a manner other than that stated above commits an act of malicious misrepresentation against another by a derogatory statement, threat or other degrading act shall be sentenced for malicious misrepresentation to a fine or to imprisonment for a maximum period of three months.
>
> If the malicious misrepresentation is committed in public or in print, writing or a graphic representation disseminated by the guilty party or which the guilty party causes, the person responsible shall be sentenced to a fine or to imprisonment for a maximum period of four months."

17. At the material time, Chapter 5a, section 3 of the Coercive Measures Act provided:

> "*Preconditions of telecommunications monitoring*
>
> Where there is reason to suspect a person of
>
> (1) an offence punishable by not less than four months' imprisonment;
>
> (2) an offence against a computer system using a terminal device, a narcotics offence; or
>
> (3) a punishable attempt to commit an offence referred to above in this section;
>
> the authority carrying out the criminal investigation may be authorised to monitor a telecommunications connection in the suspect's possession or otherwise presumed to be in his use, or temporarily to disable such a connection, if the information obtained by the monitoring or the disabling of the connection can be assumed to be very important for the investigation of the offence ..."

18. Section 18, subsection 1(1) of the Protection of Privacy and Data Security in Telecommunications Act, which came into force on 1 July 1999 and was repealed on 1 September 2004, provided:

> "Notwithstanding the obligation of secrecy provided for in section 7, the police have the right to obtain:
>
> (1) identification data on transmissions to a particular transcriber connection, with the consent of the injured party and the owner of the subscriber connection, necessary for the purpose of investigating an offence referred to in Chapter 16, Article 9 (a), Chapter 17, Article 13 § 2 or Chapter 24, Article 3 (a) of the Penal Code (Act no. 39/1889) ..."

19. Section 48 of the Personal Data Act provides that the service provider is under criminal liability to verify the identity of the sender before publishing a defamatory advertisement on its website. Section 47 provides that the service provider is also liable in damages.

20. At the material time, processing and publishing sensitive information concerning sexual behaviour on an Internet server without the subject's consent was criminalised as a data protection offence in section 43 of the Personal Files Act (Act no. 630/1995) and Chapter 38, Article 9 (Act no. 578/1995) of the Penal Code, and as a data protection violation in section 44 of the Personal Files Act. Furthermore, it could have caused liability in damages by virtue of section 42 (Act no. 471/1987) of the said Act.

21. Section 17 of the Exercise of Freedom of Expression in Mass Media Act (*laki sanavapauden käyttämisestä joukkoviestinnässä, lagen om yttrandefrihet i masskommunikation*; Act no. 460/2003), which came into force on 1 January 2004, provides:

> "*Release of identifying information for a network message*
>
> At the request of an official with the power of arrest, a public prosecutor or an injured party, a court may order the keeper of a transmitter, server or other similar device to release information required for the identification of the sender of a network message to the requester, provided that there are reasonable grounds to believe that the contents of the message are such that providing it to the public is a criminal offence. However, the release of the identifying information to the injured party may be ordered only in the event that he or she has the right to bring a private prosecution for the offence. The request shall be filed with the District Court of the domicile of the keeper of the device, or with the Helsinki District Court, within three months of the publication of the message in question. The court may reinforce the order by imposing a threat of a fine."

III. RELEVANT INTERNATIONAL MATERIALS

A. The Council of Europe

22. The rapid development of telecommunications technologies in recent decades has led to the emergence of new types of crime and has also enabled the commission of traditional crimes by means of new technologies. The Council of Europe recognised the need to respond adequately and rapidly to this new challenge as far back as in 1989, when the Committee of Ministers adopted Recommendation No. R (89) 9 on computer-related crime. Resolved to ensure that the investigating authorities possessed appropriate special powers in investigating computer-related crimes, in 1995 the Committee of Ministers adopted Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology. In point 12 of the principles appended thereto, it recommended that:

> "Specific obligations should be imposed on service providers who offer telecommunication services to the public, either through public or private networks, to provide information to identify the user, when so ordered by the competent investigating authority."

23. The other principles relating to the obligation to cooperate with the investigating authorities stated:

> "9. Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority.
>
> 10. Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedural law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein."

24. In 1996, the European Committee on Crime Problems set up a committee of experts to deal with cybercrime. It was felt that, although the previous two recommendations on substantive and procedural law had not gone unheeded, only a binding international instrument could ensure the necessary efficiency in the fight against cyberspace offences. The Convention on Cybercrime was opened for signature on 23 November 2001 and came into force on 1 July 2004. It is the first and only international treaty on crimes committed via the Internet and is open to all States. The Convention requires countries to establish as criminal offences the following acts: illegal access to a computer system, illegal interception of

computer data, interference with data or a computer system, misuse of devices, computer-related forgery and fraud, child pornography, and the infringement of copyright and related rights. The additional protocol to the Convention on Cybercrime, adopted in 2003, further requires the criminalisation of hate speech, xenophobia and racism. The scope of the Convention's procedural provisions goes beyond the offences defined in the Convention in that it applies to any offence committed by means of a computer system:

Article 14 – Scope of procedural provisions

"1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. ... each Party shall apply the powers and procedures referred to in paragraph 1 of this Article to:

(a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;

(b) other criminal offences committed by means of a computer system; and

(c) the collection of evidence in electronic form of a criminal offence.

3. ..."

25. The procedural powers include the following: expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data and interception of content data. Of particular relevance is the power to order a service provider to submit subscriber information relating to its services; indeed, the explanatory report describes the difficulty in identifying the perpetrator as being one of the major challenges in combating crime in the networked environment:

Article 18 – Production order

"1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

(a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

(b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.

3. For the purpose of this Article the term 'subscriber information' means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data and by which can be established:

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."

26. The explanatory report notes that, in the course of a criminal investigation, subscriber information may be needed mainly in two situations. Firstly, to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used, the type of other associated services used (for example, call forwarding, voicemail), or the telephone number or other technical address (for example, the e-mail address). Secondly, where a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. A production order provides a less intrusive and less onerous measure which law enforcement authorities can apply instead of measures such as interception of content data and real-time collection of traffic data, which must or can be limited only to serious offences (Articles 20 and 21 of the Convention on Cybercrime).

27. A global conference, "Cooperation against Cybercrime", held in Strasbourg on 1-2 April 2008 adopted the "Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime". The purpose of the Guidelines is to help law enforcement authorities and Internet service providers structure their interaction in relation to cybercrime issues. In order to enhance cybersecurity and minimise the use of services for illegal purposes, it was considered essential that the two parties cooperate with each other in an efficient manner. The Guidelines outline practical measures to be taken by law enforcement agencies and service providers, encouraging them to exchange information in order to strengthen their capacity to identify and combat emerging types of cybercrime. In particular, service providers are encouraged to cooperate with law enforcement agencies to help minimise the extent to which services are used for criminal activity as defined by law.

B. The United Nations

28. Out of a number of resolutions adopted in the field of cyberspace, the most pertinent for the purposes of the present case are General Assembly Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies. Among the measures to combat such misuse, it was recommended in Resolution 55/63 that:

> "(f) legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;"

29. The subsequent Resolution took note of the value of the various measures and again invited member States to take them into account.

C. The European Union

30. On 15 March 2006 the European Parliament and the Council of the European Union adopted Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, amending the previous data-retention Directive 2002/58/EC. The aim of the Directive is to harmonise member States' provisions concerning the obligations of communications providers with respect to the retention of certain data, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member State in its national law. It applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It does not apply to the content of electronic communications. The Directive requires member States to ensure that certain categories of data are retained for a period of between six months and two years. Article 5 specifies the data to be retained:

> "1. Member States shall ensure that the following categories of data are retained under this Directive:
>
> (a) data necessary to trace and identify the source of a communication:
>
> ...
>
> (2) concerning Internet access, Internet e-mail and Internet telephony:
>
> ...
>
> (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;"

31. Member States had until 15 September 2007 to implement the Directive. However, sixteen States, including Finland, made use of the right to postpone their application to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

IV. COMPARATIVE LAW

32. A comparative review of the national legislation of the member States of the Council of Europe shows that in most countries there is a specific obligation on the part of telecommunications service providers to submit computer data, including subscriber information, in response to a request by the investigating or judicial authorities, regardless of the nature of a crime. Some countries have only general provisions on the production of documents and other data, which could in practice be extended to cover also the obligation to submit specified computer and subscriber data. Several countries have not yet implemented the provisions of Article 18 of the Council of Europe Convention on Cybercrime.

V. THIRD-PARTY SUBMISSIONS

33. The Helsinki Foundation for Human Rights submitted that the present case raises the question of balancing the protection of privacy, honour and reputation on the one hand and the exercise of freedom of expression on the other. It took the view that the present case offers the Court an opportunity to define the State's positive obligations in this sphere and thereby to promote common standards in the use of the Internet throughout the member States.

34. It pointed out that the Internet is a very special method of communication and one of the fundamental principles of its use is anonymity. The high level of anonymity encourages free speech and expression of various ideas. On the other hand, the Internet is a powerful tool for defaming or insulting people or violating their right to privacy. Due to the anonymity of the Internet, the victim of a violation is in a vulnerable position. Contrary to traditional media, the victim cannot easily identify the defaming person due to the fact that it is possible to hide behind a pseudonym or even to use a false identity.

THE LAW

I. ALLEGED VIOLATIONS OF ARTICLES 8 AND 13 OF THE CONVENTION

35. The applicant complained under Article 8 of the Convention that an invasion of his private life had taken place and that no effective remedy existed to reveal the identity of the person who had put a defamatory advertisement on the Internet in his name, contrary to Article 13 of the Convention.

Article 8 provides:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Article 13 provides:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

A. The parties' submissions

36. The applicant submitted that Finnish legislation at the time protected the criminal, whereas the victim had no means to obtain redress or protection against a breach of privacy. Under the Penal Code the impugned act was punishable, but the Government had neglected to ensure that the Protection of Privacy and Data Security in Telecommunications Act and the Coercive Measures Act were consistent with each other. He argued that the random possibility of seeking civil damages, particularly from a third party, was not sufficient to protect his rights. He emphasised that he did not have the means to identify the person who had placed the advertisement on the Internet. While compensation might in some cases be an effective remedy, this depended on whether it was paid by the person who had infringed the victim's rights, which was not the case in his application. According to the Government, new legislation was in place which, had it existed at the time of the events, would have rendered this complaint unnecessary. In the applicant's view, the Government had not provided any justification for the failure to afford him this protection at the material time. He considered, therefore, that there had been breaches of Articles 8 and 13 of the Convention.

37. The Government emphasised that in the present case the interference with the applicant's private life had been committed by another individual. The impugned act was considered in domestic law as an act of malicious misrepresentation and would have been punishable as such, which had a deterrent effect. An investigation had been initiated to identify the person

who had placed the advertisement on the Internet, but had proved unsuccessful due to the legislation in force at the time, which aimed to protect freedom of expression and the right to anonymous expression. The legislation protected the publisher of an anonymous Internet message so extensively that the protection also covered messages that possibly interfered with another person's privacy. This side-effect of the protection was due to the fact that the concept of a message interfering with the protection of privacy was not clear cut, and therefore it had not been possible to clearly exclude such messages from the protection provided by law. There were, however, other avenues of redress available, for example the Personal Data Act, which provided protection against malicious misrepresentation in that the operator of the Internet server, on the basis of that Act's provisions on criminal liability and liability in damages, was obliged to ensure that sensitive data recorded by it were processed with the consent of the data subject. Furthermore, although the personal data offence had become time-barred, the applicant still had the possibility of seeking compensation from the publisher of the advertisement. By comparison with the *X and Y v. the Netherlands* case (26 March 1985, Series A no. 91), in the present case liability in damages in the context of a less serious offence provided a sufficient deterrent effect. In addition, there were other mechanisms available to the applicant, such as a pre-trial police investigation, prosecution, court proceedings and damages.

38. The Government submitted that it was important to look at the legislative situation at the material time in its social context, when a rapid increase in the use of the Internet was just beginning. The current legislation, the Exercise of Freedom of Expression in Mass Media Act (sections 2 and 17), which took effect on 1 January 2004, gives the police more extensive powers to break the protection of the publisher of an anonymous Internet message for the purposes of criminal investigations. The new legislation reflects the legislator's reaction to social development where increased use – and at the same time abuse – of the Internet has required a redefinition of the limits of protection. Thus, because of a changed situation in society, subsequent legislation has further strengthened the protection of private life in respect of freedom of expression, and especially the protection of the publishers of anonymous Internet messages.

39. However, most essential in the present case was that even the legislation in force at the material time provided the applicant with means of action against the distribution of messages invading his privacy, in that the operator of the Internet server on which the message was published was obliged by law to verify that the person in question had consented to the processing of sensitive information concerning him or her on the operator's server. This obligation was bolstered by criminal liability and liability in damages. Thus, the legislation provided the applicant with sufficient protection of privacy and effective legal remedies.

B. The Court's assessment

40. The Court notes at the outset that the applicant, a minor of 12 years at the time, was the subject of an advertisement of a sexual nature on an Internet dating site. The identity of the person who had placed the advertisement could not, however, be obtained from the Internet service provider due to the legislation in place at the time.

41. There is no dispute as to the applicability of Article 8: the facts underlying the application concern a matter of "private life", a concept which covers the physical and moral integrity of the person (*see X and Y v. the Netherlands*, cited above, § 22). Although this case is seen in domestic law terms as one of malicious misrepresentation, the Court would prefer to highlight these particular aspects of the notion of private life, having regard to the potential threat to the applicant's physical and mental welfare brought about by the impugned situation and to his vulnerability in view of his young age.

42. The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see *Airey v. Ireland*, 9 October 1979, § 32, Series A no. 32).

43. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions (see *X and Y v. the Netherlands*, cited above, §§ 23-24 and 27; *August v. the United Kingdom* (dec.), no. 36505/02, 21 January 2003; and *M.C. v. Bulgaria*, no. 39272/98, § 150, ECHR 2003-XII).

44. The limits of the national authorities' margin of appreciation are nonetheless circumscribed by the Convention provisions. In interpreting them, since the Convention is first and foremost a system for the protection of human rights, the Court must have regard to the changing conditions within Contracting States and respond, for example, to any evolving convergence as to the standards to be achieved (see *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, § 74, ECHR 2002-VI).

45. The Court considers that, while this case might not attain the seriousness of *X and Y v. the Netherlands*, where a breach of Article 8 arose

from the lack of an effective criminal sanction for the rape of a girl with disabilities, it cannot be treated as trivial. The act was criminal, involved a minor and made him a target for approaches by paedophiles (see, also, paragraph 41 above in this connection).

46. The Government conceded that, at the time, the operator of the Internet server could not be ordered to provide information identifying the offender. They argued that protection was provided by the mere existence of the criminal offence of malicious misrepresentation and by the possibility of bringing criminal charges or an action for damages against the server operator. As to the former, the Court notes that the existence of an offence has limited deterrent effects if there is no means to identify the actual offender and to bring him to justice. Here, the Court notes that it has not excluded the possibility that the State's positive obligations under Article 8 to safeguard the individual's physical or moral integrity may extend to questions relating to the effectiveness of a criminal investigation even where the criminal liability of agents of the State is not at issue (see *Osman v. the United Kingdom*, 28 October 1998, § 128, *Reports of Judgments and Decisions* 1998-VIII). For the Court, States have a positive obligation inherent in Article 8 of the Convention to criminalise offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution (see, *mutatis mutandis*, *M.C. v. Bulgaria*, cited above, § 153). Where the physical and moral welfare of a child is threatened, such injunction assumes even greater importance. The Court notes in this connection that sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives (see *Stubbings and Others v. the United Kingdom*, 22 October 1996, § 64, *Reports* 1996-IV).

47. As to the Government's argument that the applicant had the possibility to obtain damages from a third party, namely the service provider, the Court considers that it was not sufficient in the circumstances of this case. It is plain that both the public interest and the protection of the interests of victims of crimes committed against their physical or psychological well-being require the availability of a remedy enabling the actual offender to be identified and brought to justice, in the instant case the person who placed the advertisement in the applicant's name, and the victim to obtain financial reparation from him.

48. The Court accepts that, in view of the difficulties involved in policing modern societies, a positive obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities or, as in this case, the legislator. Another relevant consideration is the need to ensure that powers to control, prevent and investigate crime

are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on criminal investigations and bringing offenders to justice, including the guarantees contained in Articles 8 and 10 of the Convention, guarantees which offenders themselves can rely on. The Court is sensitive to the Government's argument that any legislative shortcoming should be seen in its social context at the time. The Court notes at the same time that the relevant incident took place in 1999, that is, at a time when it was well-known that the Internet, precisely because of its anonymous character, could be used for criminal purposes (see paragraphs 22 and 24 above). Also, the widespread problem of child sexual abuse had become well known over the preceding decade. Therefore, it cannot be said that the respondent Government did not have the opportunity to put in place a system to protect child victims from being exposed as targets for paedophiliac approaches via the Internet.

49. The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged. This deficiency was later addressed. However, the mechanisms introduced by the Exercise of Freedom of Expression in Mass Media Act (see paragraph 21 above) came too late for the applicant.

50. The Court finds that there has been a violation of Article 8 of the Convention in the present case.

51. Having regard to the finding relating to Article 8, the Court considers that it is not necessary to examine whether, in this case, there has also been a violation of Article 13 of the Convention (see, among other authorities, *Sallinen and Others v. Finland*, no. 50882/99, §§ 102 and 110, 27 September 2005, and *Copland v. the United Kingdom*, no. 62617/00, §§ 50-51, ECHR 2007-I).

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

52. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

53. Under the head of non-pecuniary damage, the applicant claimed 3,500 euros (EUR) for suffering.

54. The Government submitted that the award should not exceed EUR 2,500.

55. The Court finds it established that the applicant must have suffered non-pecuniary damage. It considers that sufficient just satisfaction would not be provided solely by the finding of a violation and that compensation has thus to be awarded. Deciding on an equitable basis, it awards the applicant EUR 3,000 under this head.

B. Costs and expenses

56. The applicant claimed EUR 2,500 for costs incurred during the national proceedings and the proceedings before the Court.

57. The Government questioned whether the applicant had furnished the requisite documentation.

58. The Court notes that no documentation as required by Rule 60 of the Rules of Court has been submitted. These claims must therefore be rejected.

C. Default interest

59. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Holds* that there has been a violation of Article 8 of the Convention;

2. *Holds* that there is no need to examine the complaint under Article 13 of the Convention;

3. *Holds*

(a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 3,000 (three thousand euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 2 December 2008, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Lawrence Early
Registrar

Nicolas Bratza
President