CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

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

SECCIÓN CUARTA

ASUNTO K.U. c. FINLANDIA

(Demanda nº 2872/02)

SENTENCIA

ESTRASBURGO

2 diciembre 2008

DEFINITIVA

02/03/2009

En el asunto K. U. contra Finlandia.
El Tribunal Europeo de Derechos Humanos (Sección Cuarta), constituido, en una Sala compuesta por los siguientes Jueces, Nicolas Bratza, *Presidente*, Lech Garlicki, Giovanni Bonello, Ljiljana Mijović, David Thór Björgvinsson, Ján Šikuta, Päivi Hirvelä, así como por Lawrence Early, *Secretaria de Sección*,
Después de haber deliberado en privado el 13 de noviembre de 2008
Dicta la siguiente
SENTENCIA

PROCEDIMIENTO

1. El asunto tiene su origen en una demanda (núm. 2872/02) dirigida contra la República de Finlandia que un ciudadano finlandés («el demandante»), había presentado el 1 de enero de 2002 ante el Tribunal con arreglo al artículo 34 del Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales («el Convenio»). El Presidente de la Sala accedió a la solicitud del demandante de no revelar su nombre (artículo 47.3 del Reglamento del Tribunal).
2. El demandante estuvo representado por el señor P. Huttunen, abogado colegiado en Helsinki. El Gobierno Finlandés («el Gobierno») estuvo representado por su agente, el señor Arto Kosonen, del Ministerio de Asuntos Exteriores.
3. El demandante alegó, en concreto, que el Estado había incumplido su obligación de proteger su derecho al respeto de la vida privada, de conformidad con el artículo 8 del Convenio.
4. Mediante Decisión de 27 junio 2006, el Tribunal declaró la demanda admisible.
5. El demandante y el Gobierno presentaron sendos escritos de alegaciones (artículo 59.1 del Reglamento del Tribunal). Habiendo decidido la Sala, tras consultar con las partes, que no se requería celebrar una vista sobre el fondo (artículo 59.3 *in fine*), las partes respondieron por escrito a dichas observaciones. Además, se recibieron comentarios de una tercera parte, la Fundación de Helsinki para los Derechos Humanos, a quien el Presidente había dado permiso para intervenir en el proceso escrito (artículo 36.2 del Convenio y artículo 44.2 del Reglamento del Tribunal).

HECHOS

I. LAS CIRCUNSTANCIAS DEL CASO

6. El demandante nació en 1986.
7. El 15 de marzo de 1999 una persona o personas desconocidas colocaron un anuncio en un sitio de citas de Internet en nombre del demandante, que tenía 12 años en ese momento, sin su conocimiento. El anuncio mencionaba su edad y año de nacimiento, daba una descripción detallada de sus características físicas, un enlace a la página web que tenía en aquel momento y que mostraba su fotografía, así como su número de teléfono, que era el correcto excepto en un dígito. En el anuncio, afirmaba que buscaba una relación íntima con un chico de su edad o mayor «para enseñarle como se hacía».
8. El demandante se enteró del anuncio de Internet al recibir un correo electrónico de un hombre, ofreciéndole conocerse y «así ver qué quieres».
9. El padre del demandante solicitó a la policía que identificara a la persona que había colgado el anuncio para demandarlo. El proveedor del servidor, sin embargo, rechazó divulgar la identidad del propietario de la denominada dirección dinámica IP (Internet Protocole),considerándose obligado a ello por el secreto de las comunicaciones según define la Ley.
10. A continuación, la policía pidió al Tribunal del Distrito de Helsinki (*käräjäoikeus, tingsrätten*) que obligara al proveedor del servidor a divulgar dicha información de conformidad con el artículo 28 de la Ley de Investigaciones Penales (*esitutkintalaki, förundersökningslagen*; Ley núm. 449/1987, modificada por la Ley núm. 692/1997).
11. En una decisión emitida el 19 de enero de 2001, el Tribunal del Distrito rehusó, al no haber una disposición legal explícita que le autorizara a ordenar al proveedor del servidor revelar los datos de identificación de los usuarios de las telecomunicaciones incumpliendo el secreto profesional. El Tribunal señaló que, en virtud del capítulo 5º, artículo 3, de la Ley de Medidas Coercitivas (*pakkokeinolaki*, *tvångsmedelslagen*; Ley núm. 450/1987) y del artículo 18 de la Ley de Protección de la Privacidad y Seguridad de Datos en las Telecomunicaciones (*laki yksityisyydensuojasta televiestinnässä ja teletoiminnan tietoturvasta, lag om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet*; Ley núm. 565/1999) la policía tenía derecho a obtener los datos de identificación de usuarios de las telecomunicaciones en asuntos relativos a ciertos delitos, a pesar de la obligación de guardar el secreto. Sin embargo, la difamación no era uno de esos delitos.
12. El 14 de marzo de 2001, el Tribunal de Apelación (*hovioikeus, hovrätten*) confirmó la Decisión y el 31 de agosto de 2001, el Tribunal Supremo (*korkein oikeus*, *högsta domstolen*) denegó al demandante la posibilidad de presentar un recurso.
13. La persona que respondió al anuncio de citas y contactó con el demandante fue identificado a través de su dirección de correo electrónico.
14. No fue posible interponer una demanda contra el director general de la compañía que proveía el servicio de Internet, ya que en su Decisión de 2

abril 2001, la Fiscalía constató la prescripción del delito contra la Ley de Datos Personales (*henkilötietolaki, personuppgiftslagen*; Ley núm. 523/99 que entró en vigor el 1 de junio de 1999), consistente en que el proveedor del servicio había publicado un anuncio difamatorio en su sitio web sin verificar la identidad de su autor.

II. LEGISLACIÓN Y JURISPRUDENCIA INTERNAS APLICABLES

15. La Constitución Finlandesa (*Suomen hallitusmuoto, Regeringsform för Finland*; Ley núm. 94/1919, modificada por la Ley núm. 969/1995) estuvo en vigor hasta el 1 de marzo de 2000. Su artículo 8 correspondía al artículo 10 de la actual Constitución Finlandesa (*Suomen perustuslaki, Finlands grundlag*), que dispone que se garantiza el derecho de toda persona a la vida privada.

16. En la época de los hechos, el capítulo 27, artículo 3 del Código Penal (*rikoslaki, strafflagen*; Ley núm. 908/1974) disponía:

> «Una persona que de manera distinta a la establecida anteriormente calumnia a otra persona mediante una afirmación despectiva, amenaza u otro acto degradante, será condenado por calumnias a multa o prisión por un período máximo de tres meses.
>
> Si la calumnia es cometida en público o por escrito, si es publicada o si se encuentra en una representación gráfica difundida por el autor o en la que el autor este en su origen, la persona responsable será condenada a una multa o prisión por un período máximo de cuatro meses».

17. En la época de los hechos, el capítulo 5, artículo 3, de la Ley de Medidas Coercitivas disponía:

> **«Condiciones previas a la vigilancia de las telecomunicaciones**
>
> Cuando existe alguna razón para sospechar que una persona ha cometido:
> Primero un delito sancionable con prisión durante no menos de cuatro meses,
> Segundo un delito contra un sistema informático utilizando un terminal, un delito de narcóticos, o
> Tercero un intento de cometer un delito sancionable en alguna de las materias anteriores de este artículo,
>
> la autoridad que esté llevando a cabo la investigación penal podrá vigilar la conexión de telecomunicaciones utilizada por el sospechoso o que presumiblemente utiliza, o a inutilizarla temporalmente si la información obtenida en la vigilancia o su desactivación pueden presumirse importantes para la investigación del delito...».

18. El artículo 18, apartado 1.1 de la Ley de Protección de la Seguridad y Privacidad de Datos en las Telecomunicaciones, que entró en vigor el 1 de julio de 1999 y fue modificada el 1 de septiembre de 2004, disponía:

> «A pesar de la obligación de guardar secreto dispuesta en el artículo 7, la policía tiene derecho a obtener:
> Primero los datos de identificación sobre transmisiones a un transcriptor particular, con el consentimiento de la parte perjudicada y del propietario de la conexión, necesarios para el objeto de la investigación de un delito referido en el artículo 9a del capítulo 16, artículo 13.2 del capítulo 17 o artículo 3a del capítulo 24 del Código Penal (Ley núm. 29/1889)...».

19. El artículo 48 de la Ley de Datos Personales dispone que el proveedor del servidor tiene la responsabilidad penal de verificar la identidad del emisor antes de publicar un anuncio difamatorio en su sitio web. El artículo 47 dispone que el proveedor del servidor es también responsable de los daños.
20. En la época de los hechos, procesar y publicar información sensible relativa al comportamiento sexual en un servidor de Internet sin el consentimiento de la persona, estaba penalizado como delito sobre la protección de datos en el artículo 43 de la Ley de Archivos Personales (Ley núm. 630/1995) y capítulo 38, artículo 9 (Ley núm. 578/1995) del Código Penal, y como violación de la protección de datos en el artículo 44 de la Ley de Archivos Personales. Asimismo, podría conllevar responsabilidad por daños y perjuicios en virtud del artículo 42 (Ley núm. 471/1987) de dicha Ley.
21. El artículo 17 de la Ley sobre el Ejercicio de la Libertad de Expresión en los Medios de Comunicación (*laki sanavapauden käyttämisestä joukkoviestinnässä, lagen om yttrandefrihet i masskommunikation*; Ley núm. 460/2003), que entró en vigor en 1 de enero de 2004, dispone:

> **«Publicación de información identificativa en un mensaje en la red.**
>
> A solicitud de una autoridad con poder para ello..., de un Fiscal o de una parte perjudicada, un Tribunal puede ordenar al supervisor de un transmisor, servidor u otro dispositivo similar a hacer pública la información requerida para la identificación del emisor de un mensaje en la red al solicitante, siempre que haya motivos razonables para creer que hacer público el contenido del mensaje es un delito penal. Sin embargo, hacer pública la información identificando a la parte perjudicada puede ser ordenado sólo en el caso en que esta persona tenga derecho a presentar una acusación privada por el delito. La solicitud debe presentarse ante el Tribunal del Distrito del domicilio del supervisor del dispositivo o ante el Tribunal del Distrito de Helsinki en los tres meses siguientes a la publicación del mensaje en cuestión. El Tribunal puede reforzar la orden imponiendo una amenaza o una multa».

III. DOCUMENTACIÓN INTERNACIONAL APLICABLE

A.El Consejo de Europa

22. El rápido desarrollo de la tecnología de las telecomunicaciones en las

últimas décadas ha dado paso a la aparición de nuevos tipos de delitos y ha permitido, asimismo, la comisión de los delitos tradicionales por medio de estas nuevas tecnologías. El Consejo de Europa reconoció la necesidad de responder adecuada y rápidamente a este nuevo desafío ya en 1989, cuando el Comité de Ministros adoptó la Recomendación núm. R (89) 9 sobre delitos informáticos. Decidido a asegurar que las autoridades de investigación poseyeran una potestad especial para investigar los delitos informáticos, el Comité de Ministros aprobó, en 1995, la Recomendación núm. R (95) 13 relativa a los problemas de la legislación de procedimiento penal relacionados con la tecnología de la información. En concreto, el punto 12 de los principios que figuran en el anexo de la recomendación, señala:

> «Deben imponerse obligaciones concretas a los proveedores del servidor que ofrecen servicios de telecomunicaciones al público, tanto a través de redes públicas como privadas, para que provean la información que identifique al usuario, cuando esto sea ordenado por una autoridad competente».

23. Los otros principios relativos a la obligación de cooperar con las autoridades de investigación establecen:

> «9. Sujetos a privilegios o protección legal, la mayoría de los sistemas legales permiten a las autoridades investigadoras ordenar a las personas a entregar objetos bajo su control requeridos para ser utilizados como prueba. De forma paralela, las disposiciones deben establecer la potestad para ordenar a las personas a presentar cualquier dato concreto bajo su control en un sistema informático en la forma requerida por la autoridad investigadora.
>
> 10. Sujetas a privilegios y protección legal, las autoridades investigadoras deben tener potestad para poder ordenar a las personas que poseen datos de un sistema informático bajo su control a que faciliten toda la información necesaria para permitir el acceso a un sistema informático y a los datos que contiene. La legislación del procedimiento penal debe asegurar que una orden similar pueda ser dada a otras personas que tengan conocimiento sobre el funcionamiento del sistema informático o aplicar medidas para asegurar los datos que contiene».

24. En 1996, el Comité Europeo sobre Problemas Penales creó un comité de expertos para tratar el ciberdelito. Se consideraba que, aunque las dos recomendaciones previas sobre derecho procesal y sustantivo no habían sido ignoradas, sólo un instrumento internacional vinculante podía asegurar la necesaria eficiencia en la lucha contra los delitos en el ciberespacio. El Convenio sobre la ciberdelincuencia fue firmado el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004. Es el primer y único tratado sobre delitos cometidos vía Internet y está abierto a todos los Estados. La Convención requiere a los países establecer como delitos penales las siguientes acciones: acceso ilegal a un sistema informático, intercepción ilegal de datos informáticos, interferencia en los datos del sistema

informático, uso incorrecto de los dispositivos, fraude y falsificación relativos a la informática, pornografía infantil, infringir los copyright y derechos relacionados. El protocolo adicional de la Convención, adoptado en 2003, además requiere penalizar el discurso del odio, la xenofobia y el racismo. El ámbito de las disposiciones procesales va más allá de los delitos definidos en el Convenio ya que se aplica a cualquier delito cometido por medio de un sistema informático:

> « **Artículo 14** – **Ámbito de aplicación de las medidas sobre procedimiento**
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos.
> 2. Cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 de este artículo a:
> a) Los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;
> b) otros delitos cometidos por medio de un sistema informático; y
> c) la obtención de pruebas electrónicas de de un delito».

25. Los poderes procesales incluyen lo siguiente: facilitar la conservación de los datos almacenados, facilitar la conservación y revelación parcial los datos de tráfico, orden de comunicación, registro y embargo de datos informáticos, recopilación en tiempo real de datos de tráfico e intercepción del contenido de los datos. Es de particular relevancia el poder ordenar a un proveedor de un servidor que presente información relativa a los servicios de sus abonados; en efecto, el informe explicativo describe la dificultad para identificar al autor siendo uno de los mayores desafíos para combatir el delito en el entorno de la red.

> **« Artículo 18 – Orden de presentación**
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:
> a) A una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y
> b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios;
> 2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 15.
> 3. A los efectos del presente artículo, por "datos relativos a los abonados" se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:
> a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;
> b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre

facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;
c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios».

26. La explicación de motivos señala que, en el transcurso de una investigación penal, la información relativa a los abonados puede ser necesaria, principalmente, en dos situaciones. En primer lugar, para identificar qué servicios y medidas técnicas han sido utilizadas o están siendo utilizadas por un abonado, como el servicio de teléfono, u otros servicios asociados (por ejemplo desvío de llamadas, mensajería de voz), número de teléfono u otras direcciones técnicas (por ejemplo correo electrónico). En segundo lugar, cuando una dirección técnica es conocida, la información de los abonados se necesita para ayudar a identificar a la persona concernida. Una orden de comunicación constituye una medida menos invasora y menos onerosa que otras que pueden aplicar las autoridades sancionadoras como la intercepción del contenido de datos y la recopilación a tiempo real de datos de tráfico, que debe ser limitada a delitos graves, únicamente (artículos 20 y 21).
27. Una conferencia global «Cooperación contra el Ciberdelito» celebrada en Estrasburgo los días 1 y 2 de abril de 2008 adoptó las «Directrices para la cooperación en la lucha contra el ciberdelito entre los organismos encargados de aplicar la Ley y los proveedores de servicios de Internet». Su propósito es ayudar a las autoridades encargadas de ejecutar la legislación y a los proveedores de servicios de Internet a estructurar su interacción en relación a las cuestiones del ciberdelito. Para mejorar la seguridad del ciberespacio y minimizar la utilización de los servicios con propósitos ilegales, se ha considerado esencial que las dos partes cooperen entre ellas de manera eficiente. Las directrices exponen medidas prácticas a adoptar por las autoridades ejecutivas y los proveedores de servicios, animándoles a intercambiar información para aumentar su capacidad de identificación y así combatir los nuevos delitos del ciberdelito. En concreto, los proveedores de servicios fueron animados a cooperar con las autoridades competentes para ayudarles a minimizar el alcance para el que los servicios son utilizados en las actividades delictivas como define la Ley.

B. Organización de las Naciones Unidas

28. De entre varias resoluciones adoptadas en el ámbito del ciberespacio, las más importantes para el propósito del presente asunto son las resoluciones de la Asamblea General 55/63, de 4 diciembre 2000 y la 56/121, de 19 diciembre 2001 sobre la «Lucha contra la utilización de las tecnologías de la información con fines delictivos». Entre las medidas para combatir este uso incorrecto, se recomendaba en la Resolución 55/63 que:

> «(f) Los sistemas legales permitirían mantener un rápido acceso a los datos informáticos referentes a investigaciones de delitos concretos;»

29. La resolución posterior tomó nota del valor de varias medidas e invitó, de nuevo, a los Estados miembros a tenerlas en cuenta.

C. La Unión Europea

30. El 15 de marzo de 2006, el Parlamento Europeo y el Consejo de la Unión Europea adoptaron la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, por la que se modifica la anterior Directiva 2002/58/CE de conservación de datos. El objetivo de la Directiva es armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones en relación con la conservación de determinados datos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación interna de cada Estado miembro. Se aplica a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas. La Directiva requiere a los Estados miembros que garanticen que ciertas categorías de datos sean conservadas durante un período de entre seis meses y dos años. El artículo 5 especifica que para retener los datos:

> «1. Los Estados miembros garantizarán que las siguientes categorías de datos se conserven de conformidad con la presente Directiva:
>
> a) datos necesarios para rastrear e identificar el origen de una comunicación:
>
> (...).
>
> 2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
>
> (...)
>
> iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono; ...».

31. Los Estados miembros tuvieron hasta el 15 de septiembre de 2007 para la transposición de esta Directiva. Sin embargo, 16 Estados, incluido Finlandia, hicieron uso del derecho de posponer su aplicación al acceso a Internet, correo electrónico por Internet y telefonía por Internet hasta el 15

de marzo de 2009.

IV. DERECHO COMPARADO

32. Una revisión comparativa de la legislación nacional de los Estados miembros del Consejo de Europa muestra que en la mayoría de los países existe la obligación concreta por parte de los proveedores de los servicios de telecomunicaciones de facilitar los datos informáticos, incluida la información del abonado, como respuesta a una solicitud de las autoridades judiciales o investigadoras, sin tener en cuenta la naturaleza del delito. Algunos países sólo poseen disposiciones sobre la comunicación de documentos y otros datos, que en la práctica podría extenderse también a la obligación de presentar datos específicos del ordenador y del abonado. Algunos países todavía no han implementado las disposiciones del artículo 18 del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

V. ALEGACIONES DE TERCEROS INTERVINIENTES

33. La Fundación de Helsinki para los Derechos Humanos declaró que el presente asunto plantea la cuestión de sopesar, por un lado, la protección de la privacidad, el honor y la reputación y, por otro, el ejercicio de la libertad de expresión. Es de la opinión de que el presente asunto ofrece al Tribunal una oportunidad para definir las obligaciones positivas del Estado en este ámbito y, de ese modo, promover criterios comunes en la utilización de Internet a través de los Estados miembros.

34. Señaló que Internet es un método muy especial de comunicación y uno de los principios fundamentales de su uso es el anonimato. El alto nivel de anonimato anima a la libertad de expresión de distintas ideas. Por otro lado, Internet es una poderosa herramienta que posibilita la difamación e insulto o la violación del derecho a la privacidad. Como consecuencia del anonimato de Internet, la víctima de una violación se encuentra en una posición vulnerable. Contrariamente a los medios de comunicación tradicionales, la víctima no puede identificar, fácilmente, a la persona que le ha difamado por el hecho de que es posible esconderse tras un apodo o incluso una falsa identidad.

FUNDAMENTOS DE DERECHO

I. SOBRE LA VIOLACIÓN DE LOS ARTÍCULOS 8 Y 13 DEL CONVENIO

35. El demandante se quejó, de conformidad con el artículo 8 del Convenio, de que se había producido una invasión de su vida privada y de que no

existía ningún recurso efectivo para desvelar la identidad de la persona que había colocado un texto difamatorio en su nombre en Internet, contrariamente al artículo 13 del Convenio.
El artículo 8 dispone:

> «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

El artículo 13 dispone:

> «Toda persona cuyos derechos y libertades reconocidos en el presente Convenio hayan sido violados tiene derecho a la concesión de un recurso efectivo ante una instancia nacional, incluso cuando la violación haya sido cometida por personas que actúen en el ejercicio de sus funciones oficiales».

A. Tesis de las partes

36. El demandante declaró que la legislación de Finlandia, en ese momento, protegía al delincuente mientras que la víctima no tenía ningún medio para obtener indemnización o protección contra un incumplimiento de su derecho a la privacidad. Según el Código Penal, el acto en litigio sería de hecho penalmente sancionable, pero el Gobierno no se había asegurado de que la Ley de Protección de la Privacidad y Seguridad de Datos en las Telecomunicaciones y la Ley de Medidas Coercitivas lo incluyeran. Afirmó que posibilidad aleatoria de solicitar daños civiles, en concreto, a un tercero, no era suficiente protección para sus derechos. Subrayó que no tenía medios para identificar a la persona que había colgado el anuncio en Internet. Mientras que una indemnización podía ser un recurso efectivo en algunos casos, esto dependía de si era abonada por la persona que había infringido el derecho de la víctima, lo que no era el caso en su demanda. Al argumento del Gobierno, de que con la nueva legislación, si en la época de los hechos hubiera estado vigente, habría hecho esta demanda innecesaria, el demandante contestó que el Gobierno estaba obligado a facilitarle protección de la que no había dispuesto en la época de los hechos. Consideró, por tanto, que había sido víctima de la vulneración de los artículos 8 y 13.
37. El Gobierno subrayó que en el presente asunto, la injerencia en la vida privada del demandante había sido cometida por otro individuo.El acto en cuestión fue considerado en la legislación interna como un acto difamatorio y habría sido sancionable como tal, lo que habría tenido un efecto

disuasorio. Una investigación fue iniciada para identificar a la persona que había colgado el anuncio en Internet, pero fracasó debido a la legislación en vigor en la época de los hechos, que tenía por objeto proteger la libertad de expresión y el derecho a la expresión anónima. La legislación protegía al autor de un mensaje anónimo en Internet tan ampliamente que la protección también amparaba mensajes que posiblemente interferían en la privacidad de otra persona. Este efecto secundario de la protección se debía al hecho de que el concepto de un mensaje interfiriendo en la protección de la privacidad no estaba claramente definido, y por tanto no hubiera sido posible excluir claramente estos mensajes de la protección dispuesta en la Ley. Había, sin embargo, otras vías de recurso accesibles, por ejemplo la Ley nº 523/1999 de Datos Personales que establecía protección contra la difamación siempre que el operador del servidor, basándose en las disposiciones de la Ley sobre responsabilidad delictiva y responsabilidad de daños, fuera obligado a asegurar que los datos sensibles se trataran con el consentimiento de la persona afectada. El Gobierno señala asimismo, que aunque el delito en materia de protección de datos haya prescrito, el demandante seguía teniendo la posibilidad de pedir indemnización al autor del anuncio. Al comparar con el caso X e Y contra Países Bajos (Sentencia de 26 marzo 1985, serie A núm. 91), considera que en este caso en el que el delito era menos grave la responsabilidad civil proporcionaba un efecto disuasorio suficiente. Además, había otros mecanismos disponibles para el demandante, como la investigación policial previa al juicio, enjuiciamiento, autos procesales e indemnización por daños y perjuicios.

38. El Gobierno declaró que era importante examinar la situación legal en la época de los hechos, en el contexto social en el que acababa de iniciarse un rápido incremento de uso de Internet. La legislación actual, la Ley del Ejercicio de la Libertad de Expresión en los Medios de Comunicación num 460/2003(artículos 2 y 17), que entró en vigor el 1 de enero de 2004, da a la policía un poder más amplio para suprimir la protección del autor de un mensaje anónimo en Internet con el objeto de investigar un delito. La nueva legislación refleja la reacción del legislador ante el desarrollo social cuando un aumento del uso –y al mismo tiempo abuso– de Internet ha requerido una redefinición de los límites de protección. De este modo, debido al cambio de la situación de la sociedad, la posterior legislación fortaleció la protección de la vida privada con respecto a la libertad de expresión y especialmente con respecto a la protección de los autores de mensajes anónimos en Internet.

39. Sin embargo, lo esencial en el presente asunto era que, incluso la legislación en vigor en esa época proporcionaba al demandante medios para defenderse de la difusión de mensajes atentatorios de su privacidad, ya que el operador del servidor de Internet a través del cual se publicó el mensaje estaba legalmente obligado a verificar que la persona en cuestión había consentido al procesamiento de información sensible. Esta obligación fue

reforzada por la responsabilidad penal y civil en caso de incumplimiento. De este modo, la legislación proporcionaba al demandante suficiente protección de la privacidad y recursos legales efectivos.

B. Valoración del Tribunal

40. El Tribunal señala, de entrada, que el demandante, un menor de 12 años de edad en la época de los hechos, fue el objeto de un anuncio de naturaleza sexual en un sitio de citas de Internet. La identidad de la persona que había colgado el anuncio en Internet no pudo, sin embargo, ser obtenida del proveedor de Internet debido a la legislación en vigor en la época.
41. No hay discusión en cuanto a la aplicabilidad del artículo 8: los hechos subyacentes a la demanda conciernen a un asunto de «vida privada», un concepto que ampara la integridad física y moral de la persona (ver, X e Y contra Países Bajos, citada *supra*, ap. 22). Incluso aunque, en términos de legislación interna, el asunto ha sido considerado difamación, el Tribunal preferiría destacar los aspectos particulares de la noción de vida privada, teniendo en cuenta la potencial amenaza ocasionada contra el bienestar físico y mental del demandante por la situación en litigio y su vulnerabilidad debido a su corta edad.
42. El Tribunal reitera que, aunque el objeto del artículo 8 es esencialmente proteger al individuo contra la injerencia arbitraria por las autoridades públicas, no obliga simplemente al Estado a abstenerse de tal injerencia: además de su obligación negativa principal, puede haber obligaciones positivas inherentes con respecto a la vida privada o familiar (ver Airey contra Irlanda, Sentencia de 9 octubre 1979, serie A núm. 32, ap. 32).
43. Estas obligaciones pueden implicar la adopción de medidas diseñadas para garantizar el respeto a la vida privada incluso en el ámbito de las relaciones entre los propios individuos. Existen diferentes maneras de asegurar el respeto a la vida privada y la naturaleza de la obligación del Estado dependerá del aspecto concreto de la vida privada que está en litigio. Aunque la elección de los medios para asegurar el cumplimiento del artículo 8 en el ámbito de la protección contra los actos de los individuos entra, en principio, dentro del margen de apreciación del Estado, la disuasión efectiva contra los actos graves, en los que los valores fundamentales y aspectos esenciales de la vida privada están en juego, requiere disposiciones eficientes en la legislación penal (ver, X e Y contra Países Bajos, aps. 23-24 y 27; August contra Reino Unido [déc], núm. 36505/02, de 21 enero 2003 y M. C. contra Bulgaria, núm. 39272/98, ap. 150, ECHR 2003-XII.
44. Los límites del margen de apreciación de las autoridades internas están, sin embargo, trazados por los artículos del Convenio. Al interpretarlos, puesto que el Convenio es sobre todo y en primer lugar un sistema de protección de los derechos humanos, el Tribunal debe tener en cuenta la evolución de la situación en los Estados Contratantes y reaccionar, por

ejemplo, al consenso necesario para las normas a adoptar (ver Christine Goodwin contra Reino Unido [GC], num. 28957/95, ap. 74, ECHR 2002-VI.

45. El Tribunal considera que, aunque este caso no pueda alcanzar la gravedad de X e Y contra Países Bajos, en el que un incumplimiento del artículo 8 se plantea por la falta de una sanción penal efectiva de la violación de una chica minusválida, tampoco puede ser tratado de trivial. El acto era de naturaleza penal, involucraba a un menor y le hacía objeto del acercamiento de pedófilos (ver, también, apartado 41 *supra* en relación con esto).

46. El Gobierno reconoció que en la época, el operador del servidor no podía ser obligado a proveer la información identificativa del autor de los hechos. Argumentó que la víctima estaba protegida por la mera existencia en derecho penal de la imputación del hecho siendo posible la interposición de una acción penal o demanda por daños y perjuicios contra el operador del servidor. Sobre el primer punto, el Tribunal señala que la existencia de un delito limita los efectos disuasorios si no existen medios para identificar al autor real del delito y llevarlo ante la justicia. Aquí, el Tribunal señala que no ha excluido la posibilidad de que las obligaciones positivas del Estado, de conformidad con el artículo 8, de garantizar la integridad moral o física del individuo puedan ampliarse a cuestiones relativas con la efectividad de una investigación penal incluso cuando la responsabilidad penal de los agentes del Estado no está en cuestión (ver Osman contra Reino Unido, Sentencia de 28 octubre 1998, *Repertorio* 1998-VIII, ap. 128). Para el Tribunal, los Estados tienen la obligación positiva inherente al artículo 8 del Convenio de penalizar delitos contra la persona incluidos las tentativas y reforzar el efecto disuasorio de la penalización poniendo en práctica las disposiciones penales mediante la investigación efectiva y el enjuiciamiento (ver, *mutatis mutandis*, M. C. contra Bulgaria, citada anteriormente, ap. 153). Cuando el bienestar físico y moral de un niño se ve amenazado, tal requerimiento judicial asume incluso mayor importancia. El Tribunal recuerda, en relación con esto, que el abuso sexual es incuestionablemente una maldad aberrante, con efectos debilitantes en sus víctimas. Niños y otros individuos vulnerables tienen derecho a la protección del Estado, en forma de disuasión efectiva, de tan grave injerencia en el aspecto privado de s vida (ver Stubbings y otros contra Reino Unido, de 22 octubre 1996, ap. 64, Repertorio 1996-IV).

47. En cuanto al argumento del Gobierno de que el demandante tenía la posibilidad de obtener una indemnización de un tercero, concretamente del proveedor del servidor, el Tribunal considera que no era suficiente en las circunstancias del caso. Está claro que tanto el interés público como la protección de los intereses de las víctimas de los delitos cometidos contra su bienestar físico o psicológico requieren la disponibilidad de un recurso que permita identificar al delincuente y llevarlo ante la justicia, en el caso que

nos ocupa, la persona que colgó el anuncio en nombre del demandante, de manera que la víctima pueda obtener una indemnización de ella.

48. El Tribunal acepta que, en vista de las dificultades que implica vigilar las sociedades modernas, una obligación positiva debe ser interpretada de modo que no imponga una carga imposible o desproporcionada sobre las autoridades o, como en este caso, sobre el legislador. Otra consideración importante es la necesidad de asegurar que los poderes de control, prevención e investigación de delitos sean ejercidos de manera que respeten plenamente el debido proceso y otras garantías que legítimamente limitan la investigación del delito y llevan a los delincuentes ante la justicia, incluyendo las garantías contenidas en los artículos 8 y 10 del Convenio, garantías con las que los propios delincuentes cuentan. El Tribunal es sensible al argumento del Gobierno de que cualquier defecto legislativo debe considerarse en su contexto social de la época. El Tribunal señala, al mismo tiempo, que el incidente en cuestión tuvo lugar en 1999, esto es, en un momento en el que era bien sabido que Internet, precisamente por su carácter anónimo, podría ser utilizado con propósitos delictivos (ver apartados 22 y 24 *supra*). También el extendido problema del abuso sexual de niños era mucho más conocido que en la década anterior. Por tanto, no se puede decir que el Gobierno demandado no tuvo ocasión de poner en marcha un sistema para proteger a las víctimas menores de ser expuestos como objetivos para acercamientos de pedófilos vía Internet.

49. El Tribunal considera que la protección práctica y efectiva del demandante requería que se llevaran a cabo fases efectivas para identificar y procesar al autor, es decir, a la persona que había colocado el anuncio. En el presente asunto tal protección no fue proporcionada. Nunca se inició una investigación efectiva debido a la exigencia de confidencialidad. Aunque la libertad de expresión y el secreto de las comunicaciones son consideraciones primordiales y los usuarios de telecomunicaciones y de los servicios de Internet deben tener una garantía de que su propia privacidad y libertad de expresión será respetada, tal garantía no puede ser absoluta y debe ceder ante otras circunstancias legítimos, como la prevención del desorden o delito o la protección de los derechos y libertades ajenos. Sin perjuicio de si la conducta de la persona que colocó el anuncio en Internet puede atraer la protección de los artículos 8 y 10, teniendo en cuenta su naturaleza reprensible sin embargo, es tarea del legislador proporcionar el marco para la reconciliación de las distintas reclamaciones que compiten por la protección en este contexto. Sin embargo, este marco no estaba en vigor en esa época, con el resultado de que la obligación positiva de Finlandia con respecto al demandante no pudo ser cumplida. Esta deficiencia fue posteriormente tratada. Sin embargo, los mecanismos introducidos por la Ley del Ejercicio de la Libertad de Expresión en los Medios de Comunicación (ver apartado 21 *supra*) llegaron demasiado tarde para el demandante.

50. El Tribunal considera que ha habido violación del artículo 8 en el presente asunto.
51. Teniendo en cuenta las consideraciones relativas al artículo 8, el Tribunal considera que no es necesario examinar si, en este caso, ha habido violación, también, del artículo 13 (ver, entre otras fuentes, Sallinen y otros contra Finlandia, núm. 50882/99, aps. 102 y 110, de 27 septiembre 2005 y Copland contra Reino Unido, núm. 62617/00, aps. 50-51, ECHR 2007-...).

II. SOBRE EL ARTÍCULO 41 DEL CONVENIO

52. El artículo 41 del Convenio dispone:

> «Si el Tribunal declara que ha habido violación del Convenio o de sus protocolos y si el derecho interno de la Alta Parte Contratante sólo permite de manera imperfecta reparar las consecuencias de dicha violación, el Tribunal concederá a la parte perjudicada, si así procede, una satisfacción equitativa».

A. Daño

53. En concepto de daño moral el demandante reclamó 3.500 euros (EUR) por su sufrimiento.
54. El Gobierno declaró que la concesión no podía exceder de 2.500 EUR.
55. El Tribunal considera demostrado que el demandante debe de haber sufrido daño moral. Considera que una satisfacción equitativa suficiente no sería proporcionada únicamente por la constatación de violación y que esta indemnización tiene, por tanto, que ser concedida. Decidiendo con fundamentos equiparables, concede al demandante 3.000 EUR por este concepto.

B. Costas y gastos

56. El demandante reclamó 2.500 EUR en concepto de los gastos satisfechos durante el procedimiento interno y el procedimiento ante este Tribunal.
57. El Gobierno preguntó si el demandante había facilitado la documentación requerida.
58. El Tribunal señala que no se había presentado ninguna documentación, como requiere el artículo 60 del Reglamento del Tribunal. La reclamación, por tanto, debe ser rechazada.

C. Intereses de demora

59. El Tribunal considera apropiado basar el tipo de los intereses de demora en el tipo de interés marginal de la facilidad de préstamo del Banco Central Europeo, incrementado en 3 puntos porcentuales.

POR ESTOS MOTIVOS, EL TRIBUNAL, POR UNANIMIDAD

1º *Declara*, que ha habido violación del artículo 8 del Convenio;

2º *Declara*, que no es necesario examinar la demanda de conformidad con el artículo 13 del Convenio;

3º *Declara*,
(a) que el Estado demandado debe abonar al demandante, dentro de un plazo de 3 meses a partir de que la sentencia sea firme de acuerdo con el artículo 44.2 del Convenio, 3.000 EUR (tres mil euros) en concepto de daño moral, más cualquier impuesto que pueda ser cargado a esta cantidad;
(b) que a contar desde el vencimiento del antedicho plazo hasta el pago, estas cantidades se verán incrementadas por un interés a un tipo marginal equivalente al del préstamo del Banco central europeo aplicable durante este período, incrementado en tres puntos;

4º *Rechaza*, el resto de las reclamaciones de indemnización.

Redactada en inglés, y notificada por escrito el 2 de diciembre de 2008, en aplicación del artículo 77.2 y 77.3 del Reglamento del Tribunal.
Firmado: Nicolas Bratza, Presidente.–Lawrence Early, Secretaria