



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

© Consiliul Europei/Curtea Europeană a Drepturilor Omului, 2012. Această traducere a fost efectuată cu sprijinul Fondului fiduciar pentru drepturile omului al Consiliului Europei ([www.coe.int/humanrightstrustfund](http://www.coe.int/humanrightstrustfund)). Nu obligă Curtea. Pentru mai multe informații, a se vedea referințele cu privire la drepturile de autor de la sfârșitul prezentului document.

© Council of Europe/European Court of Human Rights, 2012. This translation was commissioned with the support of the Human Rights Trust Fund of the Council of Europe ([www.coe.int/humanrightstrustfund](http://www.coe.int/humanrightstrustfund)). It does not bind the Court. For further information see the full copyright indication at the end of this document.

© Conseil de l'Europe/Cour Européenne des Droits de l'Homme, 2012. La présente traduction a été effectuée avec le soutien du Fonds fiduciaire pour les droits de l'homme du Conseil de l'Europe ([www.coe.int/humanrightstrustfund](http://www.coe.int/humanrightstrustfund)). Elle ne lie pas la Cour. Pour plus de renseignements veuillez lire l'indication de copyright/droits d'auteur à la fin du présent document.

### SECȚIA A PATRA

### CAUZA K.U. C. FINLANDEI

*(Cererea nr. 2872/02)*

HOTĂRÂRE

STRASBOURG

2 decembrie 2008

**DEFINITIVĂ**

*02/03/2009*

*Această hotărâre poate fi subiect al revizuirii editoriale.*



**În cauza K.U. c. Finlandei,**

Curtea Europeană a Drepturilor Omului (Secția a Patra), întrunită în cadrul Camerei compusă din:

Nicolas Bratza, *Președinte*,

Lech Garlicki,

Giovanni Bonello,

Ljiljana Mijović,

David Thór Björgvinsson,

Ján Šikuta,

Päivi Hirvelä, *judcători*,

și Lawrence Early, *Grefier al Secției*,

Deliberând în ședință închisă la 13 noiembrie 2008,

Pronunță următoarea hotărâre, care a fost adoptată la acea dată:

**PROCEDURA**

1. La originea cauzei se află o cerere (nr. 2872/02) depusă împotriva Republicii Finlanda la Curte, în conformitate cu prevederile articolului 34 al Convenției pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale („Convenția”), de către un cetățean al Republicii Finlanda (“reclamantul”), la 1 ianuarie 2002. Președintele Camerei a admis cererea reclamantului de a nu-i dezvălui numele (articolul 47 § 3 al Regulamentului Curții).

2. Reclamantul a fost reprezentat de către dl P. Huttunen, un avocat din Helsinki. Guvernul finlandez (“Guvernul”) a fost reprezentat de către Agentul său, dl Arto Kosonen de la Ministerul Afacerilor Externe.

3. Reclamantul a pretins, în special, că statul nu și-a onorat obligațiile sale pozitive de a-i proteja dreptul la respectarea vieții private în temeiul articolului 8 al Convenției.

4. Printr-o decizie din 27 iunie 2006, cererea a fost declarată admisibilă.

5. Atât reclamantul, cât și Guvernul au prezentat observații scrise cu privire la fondul cauzei (articolul 59 § 1 al Regulamentului Curții). Camera a decis, după consultarea părților, că pentru examinarea fondului cauzei, nu era necesară audierea (articolul 59 § 3 *in fine* al Regulamentului Curții) și părțile și-au răspuns reciproc în scris la observații. În plus, au fost primite comentarii de la Fundația Helsinki pentru Drepturile Omului, care a fost autorizată de către Președinte să intervină în calitate de terț intervenient în procedura scrisă (articolul 36 § 2 al Convenției și articolul 44 § 2 al Regulamentului Curții). ÎN FAPT

## I. CIRCUMSTANȚELE CAUZEI

6. Reclamantul este născut în 1986.

7. La 15 martie 1999, o persoană sau persoane necunoscute au plasat un anunț pe un site matrimonial pe Internet în numele reclamantului, care avea 12 ani la acel moment, fără cunoștința acestuia. Anunțul oferea detalii privind vârsta reclamantului, anul nașterii și trăsăturile fizice ale acestuia, un link la pagina web pe care el o avea la acel moment, pe care apărea fotografia lui, precum și numărul lui de telefon, care era corect, cu excepția unei cifre. În anunț se menționa că acesta era în căutarea unei relații intime cu un băiat de vârsta sa sau mai în vârstă ”pentru a fi inițiat”.

8. Reclamantul a devenit conștient de anunțul de pe Internet atunci când a primit un e-mail de la un bărbat, care i-a oferit să se întâlnească și ”apoi să vadă ce dorește”.

9. Tatăl reclamantului a cerut poliției să identifice persoana care a plasat anunțul pentru a înainta pretenții împotriva acesteia, însă furnizorul de servicii Internet a refuzat să divulge identitatea titularului adresei IP în cauză, considerându-se obligat să păstreze confidențialitatea telecomunicațiilor, după cum aceasta era definită prin lege.

10. Poliția a cerut atunci Judecătoriei Helsinki (*käräjaoikeus, tingsrätten*) să oblige furnizorul de servicii să divulge informația respectivă, în conformitate cu articolul 28 al Legii cu privire la urmărirea penală (*esitutkintalaki, förundersökningslagen*; Legea nr. 449/1987, după cum a fost modificată prin Legea nr. 692/1997).

11. Printr-o decizie emisă la 19 ianuarie 2001, Judecătoria de sector a refuzat, deoarece nu exista nicio dispoziție legală expresă care să o autorizeze să oblige furnizorul de servicii să divulge datele de identificare de telecomunicații, cu încălcarea secretului profesional. Curtea a notat că, în temeiul Capitolului 5a, articolul 3 al Legii cu privire la măsurile coercitive (*pakkokeinolaki, tvångsmedelslagen*; Legea nr. 450/1987) și a articolului 18 al Legii privind protecția confidențialității și securității datelor în telecomunicații (*laki yksityisyydensuojasta televiestinnässä ja teletoiminnan tietoturvasta, lag om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet*; Legea nr. 565/1999), poliția avea dreptul să obțină datele de identificare de telecomunicații în cazurile referitoare la anumite infracțiuni, în pofida obligației de a respecta confidențialitatea. Totuși, denaturarea intenționată a identității nu constituia o astfel de infracțiune.

12. La 14 martie 2001, Curtea de Apel (*hovioikeus, hovrätten*) a menținut decizia și, la 31 august 2001, Curtea Supremă (*korkein oikeus, högsta domstolen*) a respins recursul.

13. Persoana care a răspuns anunțului matrimonial și a contactat reclamantul a fost identificată prin intermediul adresei de e-mail.

14. Directorul general al companiei care a furnizat serviciul de Internet nu a putut fi acuzat, deoarece, în decizia sa din 2 aprilie 2001, procurorul a

constatat că infracțiunea pretinsă a devenit prescrisă. Infracțiunea pretinsă constituia o violare a Legii privind datele cu caracter personal (*henkilötietolaki, personuppgiftslagen*; Legea nr. 523/99, care a intrat în vigoare la 1 iunie 1999). Mai exact, furnizorul de servicii a publicat un anunț defăimător pe pagina sa web, fără a verifica identitatea expeditorului.

## II. DREPTUL ȘI PRACTICA INTERNE PERTINENTE

15. Constituția finlandeză (*Suomen hallitusmuoto, Regeringsform för Finland*; Legea nr. 94/1919, astfel cum a fost modificată prin Legea nr. 969/1995) a fost în vigoare până la 1 martie 2000. Articolul 8 al acesteia corespunde articolului 10 al Constituției finlandeze în vigoare (*Suomen perustuslaki, Finlands grundlag*; Legea nr. 731/1999), care prevede că dreptul fiecărei persoane la viața privată este garantat.

16. La momentul desfășurării evenimentelor, Capitolul 27, articolul 3 al Codului Penal (*rikoslaki, strafflagen*; Legea nr. 908/1974) prevedea următoarele:

“O persoană care într-un alt mod decât cel menționat mai sus comite un act de denaturare intenționată a identității altei persoane printr-o declarație calomnioasă, amenințare sau altă acțiune degradantă va fi sancționată pentru denaturarea intenționată a identității cu o amendă sau cu privare de libertate pe o perioadă de maxim 3 luni.

Dacă denaturarea intenționată a identității este comisă în public sau în presa scrisă, printr-o reprezentare grafică sau în scris și este diseminată de către partea vinovată sau este generată de partea vinovată, persoana responsabilă va fi sancționată cu o amendă sau cu privațiune de libertate pe o perioadă de maxim 4 luni.

17. La momentul producerii faptelor, Capitolului 5a, articolul 3 al Legii cu privire la măsurile coercitive prevedea următoarele:

### “Condiții pentru monitorizarea telecomunicațiilor

În cazul în care nu există motive de a bănui o persoană de

1) o infracțiune pentru care pedeapsa prevăzută este de nu mai puțin de patru luni de privațiune de libertate,

2) o infracțiune împotriva unui sistem informatic cu utilizarea unui dispozitiv terminal, o infracțiune legată de droguri sau

3) o tentativă de a comite una din infracțiunile menționate mai sus în acest articol,

autoritatea care efectuează urmărirea penală poate fi autorizată să monitorizeze o conexiune de telecomunicații care se află în posesia bănuțului sau în alt mod prezumată a fi în folosința acestuia, sau să dezactiveze temporar o astfel de conexiune, dacă informația obținută prin monitorizarea sau dezactivarea conexiunii se presupune a fi foarte importantă pentru investigarea infracțiunii ...”

18. Articolul 18, punctul 1(1) al Legii privind protecția confidențialității și securității datelor în telecomunicații, care a intrat în vigoare la 1 iulie 1999 și a fost abrogat la 1 septembrie 2004, prevedea următoarele:

“În pofida obligației de confidențialitate prevăzută în articolul 7, poliția are dreptul să obțină:

(1) datele de identificare ale transmisiei la o conexiune specială transcriptor, cu consimțământul părții vătămate și a proprietarului conexiunii abonate, necesar în scopul investigării infracțiunii prevăzute la capitolul 15, articolul 9a, capitolul 17, articolul 13(2) sau capitolul 24, articolul 3a al Codului Penal (Legea nr. 39/1889) ...”

19. Articolul 48 al Legii privind datele cu caracter personal stipulează că furnizorul de servicii răspunde penal pentru verificarea identității expeditorului înainte de a publica un anunț defăimător pe pagina sa web. Articolul 46 prevede că furnizorul de servicii, de asemenea, este responsabil de cauzarea de prejudicii.

20. La momentul desfășurării evenimentelor, prelucrarea și publicarea informației sensibile cu privire la comportamentul sexual pe un server de Internet, în lipsa consimțământului subiectului, era incriminată ca infracțiune de protecție a datelor în articolul 43 al Legii privind dosarele personale și capitolul 38, articolul 9 (Legea nr. 578/1995) al Codului Penal, precum și o încălcare a protecției datelor în articolul 44 al Legii privind dosarele personale. În plus, aceasta ar fi putut determina răspunderea pentru cauzarea de prejudicii, în temeiul articolului 42 (Legea nr. 471/1987) al legii menționate.

21. Articolul 17 al Legii privind exercitarea libertății de exprimare în mass-media (*laki sanavapauden käyttämisestä joukkoviestinnässä, lagen om yttrandefrihet i masskommunikation*: Legea nr. 460/2003), care a intrat în vigoare la 1 ianuarie 2004, prevede următoarele:

“Eliberarea informației de identificare pentru un mesaj de rețea

La cererea unui funcționar cu atribuții de aplicare a arestului, a unui procuror public sau a unei părți vătămate, instanța de judecată poate ordona deținătorului unui transmițător, server sau unui alt dispozitiv asemănător, să elibereze solicitantului informația cerută pentru identificarea expeditorului mesajului de rețea, cu condiția că există motive întemeiate să se creadă că conținutul mesajelor este de natura unei infracțiuni. Totuși, eliberarea informației de identificare părții vătămate poate fi ordonată doar dacă aceasta are dreptul de a intenta o urmărire penală cu privire la infracțiune. Cererea trebuie să fie depusă la Judecătoria sectorului în care se află domiciliul deținătorului dispozitivului sau la Judecătoria Helsinki, în termen de trei luni de la publicarea mesajului în cauză. Instanța poate întări ordinul prin amenințarea impunerii unei amenzi.

### III. MATERIALELE INTERNAȚIONALE PERTINENTE

#### A. Consiliul Europei

22. Dezvoltarea rapidă a tehnologiilor de telecomunicații în ultimele decenii a dus la apariția unor noi tipuri de infracțiuni și, de asemenea, a permis comiterea infracțiunilor tradiționale prin intermediul noilor tehnologii. Consiliul Europei a recunoscut necesitatea de a răspunde adecvat și rapid la această nouă provocare încă în 1989, când Comitetul de Miniștri a adoptat Recomandarea nr. R (89) 9 privind criminalitatea informatică. Decis să se asigure că autoritățile de investigație posedă competențe speciale adecvate pentru investigarea infracțiunilor informatice, în 1995, Comitetul de Miniștri a adoptat Recomandarea nr. R (95) 13 privind problemele de procedură penală legate de tehnologiile informaționale. În punctul 12 al principiilor anexate la aceasta, el a recomandat că:

”Prestatorilor de servicii care oferă servicii de telecomunicații publicului trebuie să le fie impuse obligații specifice, prin intermediul rețelelor publice ori private, să ofere informații pentru identificarea utilizatorului, la ordinul autorității competente de investigare.”

23. Alte principii referitoare la obligarea de cooperare cu autoritățile de investigare statuează următoarele:

”9. Sub rezerva privilegiilor sau protecției, majoritatea sistemelor juridice permit autorităților de investigație să ordoneze persoanelor să predea obiectele aflate sub controlul lor, care sunt necesare pentru a servi ca mijloace de probă. În mod paralel, ar trebui să se prevadă prerogativele de a ordona unor persoane să prezinte orice date specifice aflate în controlul lor într-un sistem informatic, în forma cerută de către autoritatea de investigare.”

10. Sub rezerva privilegiilor sau protecției, autoritățile de investigație trebuie să aibă prerogativa să ordoneze persoanelor care au în controlul lor date într-un sistem informatic, să furnizeze toată informația necesară pentru a permite accesul la sistemul informatic și la datele aferente acestuia. Legea procesual penală trebuie să se asigure că un ordin similar poate fi dat altor persoane care cunosc despre funcționarea unui sistem informatic sau despre măsurile aplicate pentru securizarea datelor aferente acestuia.”

24. În 1996, Comitetul European privind Problemele Infracționale a înființat un comitet de experți care să se ocupe de criminalitatea informatică. S-a considerat că, deși cele două recomandări precedente privind dreptul material și procedural nu au fost trecute cu vederea, doar un instrument internațional obligatoriu ar putea să asigure eficiența necesară în lupta împotriva infracțiunilor informatice. Convenția privind Criminalitatea Informatică a fost deschisă pentru semnare la 23 noiembrie 2001 și a intrat în vigoare la 1 iulie 2004. Acesta este primul și unicul tratat internațional privind infracțiunile comise prin intermediul Internetului și este deschis

pentru toate statele. Convenția cere statelor să stabilească drept infracțiuni următoarele acte: accesul ilegal la un sistem informatic, interceptarea ilegală a datelor informatice, afectarea integrității datelor informatice sau a unui sistem informatic, abuzurile asupra dispozitivelor, falsificarea și fraudă informatică, pornografia infantilă, încălcarea drepturilor de autor și a drepturilor conexe. Protocolul adițional la Convenție, adoptat în 2003, cere în continuare incriminarea discursului de ură, a xenofobiei și a rasismului. Scopul prevederilor procedurale ale Convenției merge mai departe de infracțiunile definite în Convenție prin faptul că se aplică oricărei infracțiuni comise prin intermediul unui sistem informatic:

”Articolul 14 – Scopul prevederilor procedurale

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a stabili prerogativele și procedurile prevăzute în prezenta secțiune, în scopul desfășurării anchetelor sau procedurilor penale specifice.

2. ... fiecare parte va aplica prerogativele și procedurile menționate la paragraful 1 al prezentului articol:

- a) infracțiunilor stabilite în conformitate cu articolele 2 – 11 ale prezentei Convenții;
- b) tuturor celorlalte infracțiuni comise prin intermediul unui sistem informatic; și
- c) strângerii dovezilor în formă electronică referitoare la orice infracțiune.

3. ...”

25. Prerogativele procedurale includ următoarele: conservarea rapidă a datelor informatice stocate, conservarea și dezvăluirea parțială rapidă a datelor referitoare la trafic, ordinul de punere la dispoziție a datelor, percheziția și sechestrarea datelor informatice stocate, colectarea în timp real a datelor informatice și interceptarea datelor referitoare la conținut. De o importanță deosebită este prerogativa de a ordona furnizorului de servicii să prezinte informații referitoare la abonații serviciilor sale; într-adevăr, raportul explicativ descrie dificultățile de identificare a făptuitorului (perpetrator) ca fiind una din provocările majore în combaterea infracțiunilor în mediul de rețea:

”Articolul 18 - Ordinul de punere la dispoziție a datelor

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a conferi autorităților sale competente dreptul de a ordona:

- a) unei persoane prezente pe teritoriul său să comunice datele informatice menționate, aflate în posesia sau sub controlul său, care sunt stocate într-un sistem informatic ori pe un suport de stocare informatic; și



b) unui furnizor de servicii care oferă prestații pe teritoriul părții să comunice datele din posesia sau de sub controlul său referitoare la abonați și la astfel de servicii.

2. Prerogativelor și procedurilor menționate în prezentul articol li se aplică prevederile articolelor 14 și 15.

3. În sensul prezentului articol, expresia "date referitoare la abonați" va desemna orice informație, sub formă de date informatice sau sub orice altă formă, deținută de un furnizor de servicii, referitoare la abonații acestor servicii, altele decât datele referitoare la trafic sau conținut, și care permit stabilirea:

a) tipului de serviciu de comunicații utilizat, dispozițiilor tehnice luate în această privință și perioadei serviciului;

b) identității, adresei poștale sau geografice, numărului de telefon al abonatului și oricărui alt număr de contact, precum și a datelor referitoare la facturare și plată, disponibile în baza unui contract sau a unui aranjament de servicii;

c) oricărei alte informații referitoare la locul în care se găsesc echipamentele de comunicație, disponibile în baza unui contract sau a unui aranjament de servicii."

26. Notele explicative la raport notează că, în cursul unei urmăriri penale, datele referitoare la abonați pot fi necesare în special în două situații. În primul rând, pentru a identifica care servicii și măsuri tehnice conexe au fost folosite de către un abonat, cum ar fi tipul serviciului de telefonie utilizat, tipul altor servicii asociate utilizate (de exemplu, redirectionarea apelurilor, mesageria vocală), numărul de telefon sau altă adresă tehnică (de exemplu, adresa de e-mail). În al doilea rând, atunci când adresa tehnică este cunoscută, datele referitoare la abonați sunt necesare pentru a ajuta la stabilirea identității persoanei în cauză. Ordinul de punere la dispoziție a datelor prevede o măsură mai puțin intruzivă și mai puțin oneroasă pe care autoritățile de aplicare a legii o pot aplica în locul măsurilor, cum ar fi interceptarea datelor referitoare la conținut și colectarea în timp real a datelor referitoare la conținut, care trebuie sau poate fi limitată doar la cazurile de infracțiuni grave (articolul 20 și 21).

27. O conferință la nivel mondial "Cooperarea împotriva criminalității informatice", care a avut loc la Strasbourg la 1-2 aprilie 2008, a adoptat "Ghidul privind cooperarea dintre autoritățile de aplicare a legii și furnizorii de servicii internet împotriva criminalității informatice". Scopul acestuia este de a ajuta autoritățile de aplicare a legii și furnizorii de servicii de Internet să structureze interacțiunea lor cu privire la problemele privind criminalitatea informatică. Cu scopul de a spori securitatea informatică și de a minimaliza utilizarea serviciilor în scopuri ilegale, a fost considerat esențial ca cele două părți să coopereze într-un mod eficient. Ghidul subliniază măsurile practice care urmează a fi întreprinse de către autoritățile de aplicare a legii și furnizorii de servicii, încurajându-i să facă schimb de informații cu scopul de a consolida capacitatea acestora de a

identifica și combate noile tipuri de infracțiuni informatice. În special, furnizorii de servicii au fost încurajați să coopereze cu autoritățile de aplicare a legii pentru a ajuta la minimalizarea măsurii în care serviciile sunt utilizate în scop de activitate criminală, după cum această este definită prin lege.

## **B. Organizația Națiunilor Unite**

28. Dintr-un număr de rezoluții adoptate în domeniul cibernetic, cele mai relevante în scopul acestei cauze sunt rezoluțiile Adunării Generale 55/63 din 4 decembrie 2000 și 56/121 din 19 decembrie 2001 privind ”Combaterea utilizării abuzive a tehnologiilor informaționale”. Printre măsurile de combatere a abuzului, Rezoluția 55/63 a recomandat următoarele:

”(f) Sistemele juridice ar trebui să permită păstrarea și accesul rapid la datele electronice referitoare la o anumită urmărire penală;”

29. Următoarea rezoluție a luat act de valoarea diferitelor măsuri și a invitat din nou statele membre să le ia în considerare.

## **C. Uniunea Europeană**

30. La 15 martie 2006, Parlamentul European și Consiliul Uniunii Europene au adoptat Directiva 2006/24/EC privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor publice de comunicații electronice sau a rețelelor publice de comunicații, prin care a modificat Directiva precedentă 2002/58/EC de păstrare a datelor. Scopul Directivei este de a armoniza dispozițiile statelor membre referitoare la obligațiile furnizorilor de comunicații cu privire la păstrarea anumitor date, în scopul asigurării faptului că datele sunt valabile în scopul investigării, detectării și urmăririi penale a infracțiunilor grave, după cum acestea sunt definite de dreptul intern al fiecărui stat membru. Aceasta se aplică datelor referitoare la trafic și la locație, în privința atât a persoanelor juridice, cât și a persoanelor fizice, precum și datelor necesare pentru identificarea abonatului sau a utilizatorului înregistrat. Aceasta nu se aplică conținutului comunicațiilor electronice. Directiva impune statelor membre să se asigure că anumite categorii de date sunt păstrate între șase luni și doi ani. Articolul 5 specifică datele care trebuie să fie păstrate:

”1. Statele membre trebuie să asigure păstrarea următoarelor categorii de date în temeiul acestei Directive:

(a) date necesare pentru urmărirea și identificarea sursei de comunicare:

...

(2) referitoare la accesul la Internet, Internet e-mail și telefonia prin Internet:

...;

(iii) numele și adresa abonatului sau utilizatorului înregistrat, căruia i-a fost alocată adresa Internet Protocol (IP), ID-ul utilizatorului sau numărul de telefon la momentul comunicației;

31. Statele membre au avut timp până la 15 septembrie 2007 să implementeze Directiva. Totuși, 16 state, inclusiv Finlanda, au făcut uz de dreptul de a amâna aplicarea prevederilor referitoare la accesul la Internet, Internet e-mail și telefonia prin Internet până la 15 martie 2009.

#### IV. DREPTUL COMPARAT

32. O analiză comparativă a legislației naționale a statelor membre ale Consiliului Europei arată că, în cele mai multe țări, există o obligație specifică din partea furnizorilor de servicii de telecomunicații să prezinte date informatice, inclusiv date despre abonați, ca răspuns la o cerere formulată de autoritățile de urmărire penală sau judiciare, indiferent de natura infracțiunii. Alte state au doar dispoziții generale privind prezentarea documentelor și a datelor care, în practică, ar putea fi extinse să acopere, de asemenea, și obligația de a prezenta datele specificate informatice și cu privire la abonați. Câteva țări nu au implementat prevederile articolului 18 al Convenției Consiliului Europei privind Criminalitatea Informatică.

#### V. ARGUMENTELE TERȚULUI INTERVENIENT

33. Fundația Helsinki pentru Drepturile Omului a susținut că această cauză ridică problema de echilibru între protecția vieții private, onoarei și reputației, pe de o parte, și, pe de altă parte, exercitarea libertății de exprimare. Ea a considerat că această cauză oferă Curții oportunitatea de a defini obligațiile pozitive ale statului în acest domeniu și, prin urmare, să promoveze standarde comune de utilizare a Internetului în toate statele membre.

34. Ea a subliniat că Internetul este o metodă foarte specială de comunicare și unul dintre principiile fundamentale ale utilizării sale este anonimatul. Nivelul înalt al anonimatului încurajează discursul liber și exprimarea diverselor idei. Pe de altă parte, Internetul este un instrument puternic pentru defăimarea sau insultarea persoanelor sau violarea dreptului lor la viață privată. Datorită anonimatului Internetului, victima violării se află într-o poziție de vulnerabilitate. Spre deosebire de mass-media tradițională, victima nu poate identifica cu ușurință persoana care defăimează, datorită faptului că aceasta posibil se ascunde după o poreclă sau chiar folosește o identitate falsă.

## ÎN DREPT

### I. PRETINSA VIOLARE A ARTICOLELOR 8 ȘI 13 ALE CONVENȚIEI

35. Reclamantul s-a plâns, în temeiul articolului 8 al Convenției, că a avut loc o încălcare a vieții sale private și că nu a existat vreun remediu efectiv de a dezvălui identitatea persoanei care a plasat un text defăimător pe Internet în numele său, ceea ce vine în contradicție cu articolul 13 al Convenției.

Articolul 8 prevede următoarele:

”1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului și a corespondenței sale.

2. Nu este admisă ingerența unei autorități publice în exercitarea acestui drept decât dacă aceasta este prevăzută de lege și constituie, într-o societate democratică, o măsură necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor și a libertăților altora.”

Articolul 13 prevede următoarele:

”Orice persoană ale cărei drepturi și libertăți recunoscute de prezenta convenție au fost încălcate are dreptul de a se adresa efectiv unei instanțe naționale, chiar și dacă încălcarea ar fi fost comisă de persoane care au acționat în exercitarea atribuțiilor lor oficiale.”

#### A. Argumentele părților

36. Reclamantul a susținut că, la momentul desfășurării evenimentelor, legislația finlandeză proteja infractorii, pe când victima nu avea posibilități de redresare sau protecție împotriva încălcării vieții private. În temeiul Codului Penal, fapta incriminată era pedepsită, dar Guvernul a neglijat asigurarea faptului că Legea privind protecția confidențialității și securității datelor în telecomunicații și Legea privind măsurile coercitive să fie în concordanță una cu cealaltă. El a argumentat că posibilitatea de a solicita despăgubiri civile, în special de la un terț, nu a fost suficientă pentru a proteja drepturile sale. El a subliniat faptul că nu dispunea de mijloace pentru identificarea persoanei care a plasat anunțul pe Internet. Chiar dacă despăgubirea ar putea fi un remediu efectiv în anumite cazuri, aceasta depinde de faptul dacă a fost achitată de persoana care a încălcat drepturile victimei, ceea ce nu s-a întâmplat în această cauză. Potrivit Guvernului, o nouă legislație a fost adoptată care, dacă ar fi fost în vigoare la momentul desfășurării evenimentelor, această cerere nu ar fi fost necesară. În opinia reclamantului, Guvernul nu a adus nicio justificare pentru omisiunea de a-i

acorda această protecție la momentul producerii faptelor. Prin urmare, el a considerat că a avut loc violarea articolelor 8 și 13.

37. Guvernul a subliniat că, în această cauză, ingerința în viața privată a reclamantului a fost comisă de către o altă persoană. Fapta imputată era considerată în dreptul intern ca denaturarea intenționată a identității și ar fi fost pedepsită ca atare, ceea ce a avut un efect de descurajare. Pentru identificarea persoanei care a plasat anunțul pe Internet a fost intentată o urmărire penală, dar aceasta nu s-a bucurat de succes din cauza legislației în vigoare la acel moment, care avea scopul de a proteja libertatea de exprimare și dreptul la exprimarea în anonimat. Legislația proteja persoana care publica un mesaj anonim pe Internet într-un mod atât de extins, încât protecția acoperea, de asemenea, mesajele care, posibil, duceau la o ingerință în dreptul altei persoane la viață privată. Acest efect secundar al protecției se datora faptului că mesajul care ducea la ingerința în dreptul altei persoane la viață privată nu era bine definit și, prin urmare, nu era posibil de a exclude aceste mesaje din protecția oferită de lege. Totuși, existau alte căi de atac disponibile, de exemplu Legea privind datele cu caracter personal, care oferea protecție împotriva denaturării intenționate a identității, prin faptul că operatorul serverului, în temeiul Legii privind răspunderea penală și patrimonială, era obligat să se asigure că datele înregistrate de el fuseseră procesate cu consimțământul persoanei în cauză. Mai mult ca atât, deși infracțiunea privind datele cu caracter personal a devenit prescrisă, totuși, reclamantul avea posibilitatea să solicite compensații pentru publicarea anunțului. Prin comparație cu cauza *X și Y c. Olandei* (hotărâre din 26 martie 1985, Seria A nr. 91), în contextul unei infracțiuni mai puțin grave, răspunderea patrimonială a creat un efect de descurajare suficient. În plus, au existat și alte mecanisme la dispoziția reclamantului, cum ar fi ancheta poliției, urmărirea penală, procedurile în instanța de judecată și despăgubirile.

38. Guvernul a susținut că era important a se aprecia situația legislativă în vigoare la momentul producerii faptelor în contextul social la acel moment, când o creștere rapidă a utilizării Internetului era doar la început. Legislația curentă, Legea privind exercitarea libertății de exprimare în mass-media (articolele 2 și 7), care a intrat în vigoare la 1 ianuarie 2004, oferă poliției mai multe prerogative de a încălca protecția identității unei persoane care publică anunțuri anonime pe Internet, în scopul investigării unei infracțiuni. Noua legislație reflectă reacția legiuitorului la dezvoltarea socială, acolo unde utilizarea frecventă - și, în același timp, abuzul - Internetului a cerut o redefinire a limitelor de protecție. Astfel, datorită schimbării situației în societate, legislația adoptată ulterior a consolidat protecția vieții private în privința libertății de exprimare și, în special, protecția persoanelor care publică anunțuri anonime pe Internet.

39. Totuși, esențial în această cauză este că însăși legislația în vigoare la momentul producerii faptelor oferea reclamantului mijloace de acțiune

împotriva distribuirii mesajelor care încălcau viața privată, prin faptul că operatorul serverului de Internet pe care a fost publicat mesajul era obligat prin lege să verifice dacă persoana în cauză și-a exprimat consimțământul pentru procesarea informației despre ea pe serverul operatorului. Această obligație era susținută prin răspunderea penală și patrimonială. Astfel, legislația a oferit reclamantului suficientă protecție a vieții private și căi de recurs eficiente.

## B. Aprecierea Curții

40. Curtea observă de la bun început că reclamantul, un minor de 12 ani la momentul producerii faptelor, a fost subiectul unui anunț de natură sexuală pe un site matrimonial pe Internet. Identitatea persoanei care a plasat anunțul nu a putut fi, totuși, obținută de la furnizorul de Internet din cauza legislației în vigoare la acel moment.

41. Nu se contestă aplicabilitatea articolului 8: faptele care stau la baza cererii se referă la o chestiune de "viață privată", o noțiune care acoperă integritatea fizică și psihică a persoanei (*a se vedea X și Y c. Olandei*, citată mai sus, § 22). Chiar dacă cauza este privită în termeni de drept intern în calitate de denaturare intenționată a identității, Curtea ar prefera să sublinieze aceste aspecte speciale ale noțiunii de viață privată, având în vedere amenințarea posibilă a integrității sale fizice și morale provocată de situația contestată, precum și starea sa de vulnerabilitate, având în vedere vârsta sa fragedă.

42. Curtea reiterează că, deși obiectul articolului 8 este, în esență, de a proteja persoanele împotriva ingerinței arbitrare de către autoritățile publice, acesta nu doar obligă statul să se abțină de la o astfel de ingerință: în plus față de acest angajament în primul rând negativ, pot să existe obligații pozitive de respectare a vieții private sau de familie (*a se vedea Airey c. Irlandei*, hotărâre din 9 octombrie 1979, Seria A nr. 32, § 32).

43. Aceste obligații pot implica adoptarea măsurilor menite să asigure respectarea vieții private chiar și în sfera relațiilor dintre indivizi. Există diferite căi de asigurare a vieții private și natura obligațiilor statului vor depinde de aspectul specific al vieții private care este în discuție. În timp ce alegerea mijloacelor pentru a asigura conformitatea cu articolul 8 în sfera relațiilor dintre indivizi se află, în principiu, în cadrul marjei de apreciere a statului, atunci când valorile fundamentale și aspectele esențiale ale vieții private sunt în joc, efectul descurajator împotriva faptelor grave necesită prevederi eficiente de drept penal (*a se vedea X și Y c. Olandei*, §§ 23-24 și 27; *August c. Regatului Unit* (dec.), nr. 36505/02, 21 ianuarie 2003 și *M.C. c. Bulgariei*, nr. 39272/98, § 150, ECHR 2003-XII).

44. Limitele marjei de apreciere a autorităților naționale sunt, totuși, circumscrise prin prevederile Convenției. În interpretarea acestora, având în vedere faptul că Convenția este înaintea de toate un sistem de protecție a

drepturilor omului, Curtea trebuie să aibă în vedere schimbările care au loc în statele contractante și să răspundă, de exemplu, la orice evoluție convergentă în ceea ce privește standardele care urmează a fi atinse (a se vedea *Christine Goodwin c. Regatului Unit* [MC], nr. 28957/95, § 74, ECHR 2002-VI).

45. Curtea consideră că, chiar dacă această cauză poate să nu atingă gravitatea cauzei *X and Y c. Olandei*, unde o violare a articolului 8 a rezultat din lipsa unei sancțiuni penale efective pentru violul unei fete cu handicap, aceasta nu poate fi considerată neînsemnată. Fapta a fost penală, a implicat un minor și l-a făcut ținta avansurilor din partea pedofililor (a se vedea, de asemenea, paragraful 41 de mai sus în acest sens).

46. Guvernul a recunoscut că, la acel moment, operatorul serverului nu putea fi obligat să prezinte informații pentru identificarea infractorului. El a susținut că protecția a fost oferită prin simpla existență a infracțiunii de denaturare intenționată a identității și prin posibilitatea de a aduce acuzații penale sau existența unei acțiuni de despăgubire împotriva operatorului serverului. În ceea ce privește primul argument, Curtea notează că, în lipsa mijloacelor de a identifica infractorul real și de a-l aduce în fața justiției, existența unei infracțiuni are efecte de descurajare limitate. Aici, Curtea notează că nu este exclusă posibilitatea ca obligațiile pozitive ale statului în temeiul articolului 8 de a proteja integritatea fizică sau psihică a persoanelor poate fi extinsă la chestiunea privind eficiența unei anchete penale, chiar dacă nu este vorba despre răspunderea penală a agenților statului (a se vedea *Osman c. Regatului Unit*, hotărâre din 28 octombrie 1998, *Rapoartele de Hotărâri și Decizii* 1998-VIII, § 128). Pentru Curte, statele au o obligație pozitivă inerentă în articolul 8 al Convenției de a incrimina infracțiunile împotriva persoanei, inclusiv tentativele de infracțiune, și de a consolida efectul descurajator al incriminării prin aplicarea prevederilor de drept penal în practică, prin intermediul unei anchete și urmăririi penale eficiente (a se vedea, *mutatis mutandis*, *M.C. c. Bulgariei*, citată mai sus, § 153). În cazul în care este amenințată integritatea fizică și psihică a unui copil, interdicția dobândește o importanță și mai mare. Curtea reamintește, în acest sens, că abuzul sexual este, fără îndoială, un delict odios, cu efecte debilitante asupra victimelor sale. Copiii și alte persoane vulnerabile au dreptul la protecție din partea statului, în forma unei descurajări eficiente, de la aceste forme grave de ingerință în aspectele esențiale ale vieților lor private (a se vedea *Stubbings și Alții c. Regatului Unit*, 22 octombrie 1996, § 64, *Rapoarte* 1996-IV).

47. În ceea ce privește argumentul Guvernului, precum că reclamantul a avut posibilitatea de a obține prejudicii de la un terț, și anume de la furnizorul de servicii, Curtea consideră că acesta nu a fost suficient în circumstanțele acestei cauze. Este clar că atât interesul public, cât și protecția intereselor victimelor infracțiunilor comise împotriva integrității lor fizice și psihice necesită existența unui remediu care permite ca

infractorul real să fie identificat și adus în fața justiției, în această cauză, acesta fiind persoana care a plasat anunțul în numele reclamantului, și ca victima să obțină reparație materială din partea acestuia.

48. Curtea acceptă că, având în vedere dificultățile existente în reglementarea societăților moderne, obligația pozitivă trebuie să fie interpretată într-un mod care nu impune o sarcină imposibilă sau disproporționată pentru autorități sau, în acest caz, pentru legiuitor. Un alt argument relevant este nevoia de a asigura ca prerogativele de control, prevenire și investigare a infracțiunilor să fie exercitate într-un mod care respectă pe deplin un proces echitabil și alte garanții care impun restricții, în mod legitim, privind investigarea infracțiunilor și aducerea infractorilor în fața justiției, inclusiv garanțiile conținute în articolele 8 și 10, garanții pe care însăși infractorii se pot baza. Curtea este sensibilă la argumentul Guvernului precum că orice deficiență legislativă urmează a fi privită în contextul social la momentul producerii faptelor. Curtea notează, în același timp, că incidentul în cauză a avut loc în 1999, într-un moment când era bine-cunoscut faptul că Internetul, tocmai din cauza caracterului său anonim, putea fi folosit în scopuri criminale (a se vedea paragrafele 22 și 24 de mai sus). De asemenea, problema răspândită a abuzului sexual al copiilor a devenit bine-cunoscută în ultimii zece ani. Prin urmare, nu se poate spune că Guvernul pârât nu a avut posibilitatea de a implementa un sistem de protecție a copiilor victime - ținte ale avansurilor din partea pedofililor, prin intermediul Internetului.

49. Curtea consideră că protecția practică și eficientă a reclamantului a necesitat luarea de măsuri eficiente pentru a identifica și urmări în justiție infractorul, adică persoana care a plasat anunțul. În această cauză, o asemenea protecție nu a fost oferită. O urmărire penală eficientă nu a putut fi lansată din cauza unei cerințe primordiale de confidențialitate. Deși libertatea de exprimare și confidențialitatea comunicațiilor sunt considerații primare și utilizatorii telecomunicațiilor și a Internetului trebuie să aibă garanția că viața lor privată și libertatea de exprimare vor fi respectate, o asemenea garanție nu poate fi absolută și trebuie să cedeze uneori altor imperative legitime, cum ar fi prevenirea dezordinii sau infracțiunilor ori protecția drepturilor și libertăților altuia. Fără a prejudicia întrebarea dacă comportamentul persoanei care a plasat anunțul criminal pe Internet poate atrage protecția articolelor 8 și 10, având în vedere natura sa condamnată, este, totuși, sarcina legislatorului de a oferi cadrul pentru reconcilierea diferitor pretenții care concurează pentru protecție în acest context. Totuși, un astfel de cadru nu a fost în vigoare la momentul desfășurării evenimentelor, astfel încât Finlanda nu poate fi eliberată de obligația sa pozitivă în privința reclamantului. Această deficiență a fost abordată ulterior. Totuși, mecanismul introdus prin Legea privind exercitarea libertății de exprimare în mass-media (a se vedea paragraful 21 de mai sus) a survenit prea târziu pentru reclamant.



50. Curtea constată că, în această cauză, a avut loc violarea articolului 8.

51. Având în vedere constatarea sa în privința articolului 8, Curtea consideră că nu este necesar de a examina dacă, în această cauză, a avut loc și violarea articolului 13 (a se vedea, printre alte surse, *Sallinen și Alții c. Finlandei*, nr. 50882/99, §§ 102 și 110, 27 septembrie 2005 și *Copland c. Regatului Unit*, nr. 62617/00, §§ 50-51, ECHR 2007-...)

## II. APLICAREA ARTICOLULUI 41 AL CONVENȚIEI

52. Articolul 41 al Convenției prevede următoarele:

”Dacă Curtea declară că a avut loc o încălcare a Convenției sau a Protocoalelor sale și dacă dreptul intern al înaltei părți contractante nu permite decât o înlăturare incompletă a consecințelor acestei încălcări, Curtea acordă părții lezate, dacă este cazul, o reparație echitabilă.”

### A. Prejudiciu

53. Reclamantul a pretins 3,500 euro (EUR) cu titlu de prejudiciu moral pentru suferință.

54. Guvernul a susținut că suma acordată nu trebuie să depășească EUR 2,500.

55. Curtea constată că a stabilit că reclamantul trebuie să fi suferit un prejudiciu moral. Ea consideră că o satisfacție echitabilă suficientă nu va fi oferită doar prin constatarea violării și, prin urmare, o compensație trebuie să fie acordată. Evaluând în mod echitabil, ea acordă reclamantului EUR 3,000 cu acest titlu.

### B. Costuri și cheltuieli

56. Reclamantul a pretins EUR 2,500 cu titlu de costuri și cheltuieli care au fost suportate în cadrul procedurilor interne și în procedurile în fața Curții.

57. Guvernul a invocat faptul că reclamantul nu a prezentat documentele necesare.

58. Curtea notează că niciun document cerut de articolul 60 al Regulamentului Curții nu a fost prezentat. Prin urmare, această cerință urmează a fi respinsă.

### C. Dobânda de întârziere

59. Curtea consideră că este potrivit ca dobânda de întârziere să fie calculată în funcție de rata minimă a dobânzii la creditele acordate de Banca Centrală Europeană, la care vor fi adăugate trei procente.

**DIN ACESTE MOTIVE, CURTEA, ÎN UNANIMITATE,**

1. *Hotărăște* că a avut loc o violare a articolului 8 al Convenției;
2. *Hotărăște* că nu este necesar de a examina pretenția în temeiul articolului 13 al Convenției;
3. *Hotărăște*
  - (a) că Statul pârât trebuie să plătească reclamantului, în termen de trei luni de la data când această hotărâre devină definitivă în conformitate cu articolul 44 § 2 al Convenției, EUR 3,000 (trei mii de euro), plus orice taxă care poate fi percepută, cu titlu de prejudiciu moral;
  - (b) că, de la expirarea celor trei luni menționate mai sus până la executarea hotărârii, urmează să fie plătită o dobândă la sumele de mai sus, egală cu rata minimă a dobânzii la creditele acordate de Banca Centrală Europeană pe parcursul perioadei de întârziere, plus trei procente;
4. *Respinge* restul pretențiilor reclamantului cu privire la satisfacția echitabilă.

Redactată în limba engleză și comunicată în scris la 2 decembrie 2008, în conformitate cu articolul 77 §§ 2 și 3 al Regulamentului Curții.

Lawrence Early  
Grefier

Nicolas Bratza  
Președinte

**© Consiliul Europei/Curtea Europeană a Drepturilor Omului, 2012**

Limbile oficiale ale Curții Europene a Drepturilor Omului sunt engleza și franceza. Această traducere a fost realizată cu sprijinul Fondului fiduciar pentru drepturile omului al Consiliului Europei ([www.coe.int/humanrightstrustfund](http://www.coe.int/humanrightstrustfund)). Nu obligă Curtea, care, de altfel, nu își asumă răspunderea pentru calitatea acesteia. Traducerea poate fi descărcată din baza de date HUDOC a Curții Europene a Drepturilor Omului (<http://hudoc.echr.coe.int>) sau din oricare altă bază de date în care Curtea a făcut această traducere disponibilă. Poate fi reprodusă în scop necomercial, cu condiția ca titlul cauzei să fie citat în întregime, împreună cu referirea la dreptul de autor menționat anterior la Fondul fiduciar pentru drepturile omului. Dacă intenționați să utilizați vreun fragment din această traducere în scop comercial, vă rugăm să contactați [publishing@echr.coe.int](mailto:publishing@echr.coe.int).

**© Council of Europe/ European Court of Human Rights, 2012**

The official languages of the European Court of Human Rights are English and French. This translation was commissioned with the support of the Human Rights Trust Fund of the Council of Europe ([www.coe.int/humanrightstrustfund](http://www.coe.int/humanrightstrustfund)). It does not bind the Court, nor does the Court take any responsibility for the quality thereof. It may be downloaded from the HUDOC case-law database of the European Court of Human Rights.

(<http://hudoc.echr.coe.int>) or from any other database with which the Court has share it. It may be reproduced for non-commercial purposes on condition that the full title of the case is cited, together with the above copyright indication and reference to the Human Rights Trust Fund. If it is intended to use any part of this translation for commercial purposes, please contact [publishing@echr.coe.int](mailto:publishing@echr.coe.int).

© **Conseil de l'Europe/ Cour Européenne des Droits de l'Homme, 2012**

Les langues officielles de la Cour Européenne des Droits de l'Homme sont le français et l'anglais. La présente traduction a été effectuée avec le soutien du Fonds fiduciaire pour les droits de l'homme du Conseil de l'Europe ([www.coe.int/humanrightstrustfund](http://www.coe.int/humanrightstrustfund)). Elle ne lie pas la Cour, et celle-ci décline toute responsabilité quant à sa qualité. Elle peut être téléchargée à partir de HUDOC, la base de jurisprudence de la Cour européenne des droits de l'homme (<http://hudoc.echr.coe.int>) où de toute autre base de données à laquelle HUDOC l'a communiquée. Elle peut être reproduite à des fins non commerciales, sous réserve que le titre de l'affaire soit cité en entier et s'accompagne de l'indication de copyright ci-dessus ainsi que la référence au Fonds fiduciaire pour les droits de l'homme. Toute personne souhaitant se servir de tout ou partie de la présente traduction à des fins commerciales est invitée à le signaler à l'adresse suivante: [publishing@echr.coe.int](mailto:publishing@echr.coe.int).