



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

ЧЕТВЕРТА СЕКЦІЯ

СПРАВА K.U. v. FINLAND

(Заява № 2872/02)

РІШЕННЯ

СТРАСБУРГ

2 грудня 2008 року

ОСТАТОЧНЕ

02/03/2009

У тексті рішення можливі редакційні правки.

© Рада Європи/Європейський суд з прав людини, 2012. Цей переклад було замовлено за підтримки Трастового фонду з прав людини Ради Європи (www.coe.int/humanrightstrustfund). Переклад не є обов'язковим для Суду. Для додаткової інформації дивіться повний текст копірайту наприкінці цього документа.

© 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). 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). 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.

У справі K.U. v. Finland [К.Ю. проти Фінляндії],

Європейський суд з прав людини (Четверта секція), засідаючи Палатою у такому складі:

Ніколас Братца (Nicolas Bratza), *Голова*,
Лех Гарліцкі (Lech Garlicki),
Джіванні Бонелло (Giovanni Bonello),
Лільяна Мійовіч (Ljiljana Mijović),
Девід Тор Бйоргвінссон (David Thór Björgvinsson),
Ян Шікута (Ján Šikuta),
Пааіві Хірвелаа (Päivi Hirvelä), *судді*,

та Лоуренс Ерлі (Lawrence Early), *секретар секції*,
після обговорення у закритому засіданні 13 листопада 2008 року,
виносить таке рішення, яке було прийнято в той день:

ПРОЦЕДУРА

1. Справу розпочато за заявою (№ 2872/02) проти Республіки Фінляндія, поданою до Суду 1 січня 2002 року відповідно до статті 34 Конвенції про захист прав людини і основоположних свобод (“Конвенція”) громадянином Фінляндії (“заявник”). Голова Палати погодився з проханням заявника не розкривати його імені (пункт 3 правила 47 Регламенту Суду).

2. Заявника представляв пан П. Хуттунен (P. Huttunen), адвокат, що практикує у Гельсінкі. Уряд Фінляндії (“Уряд”) представляла його Уповноважена особа при Суді пан Арто Косонен (Arto Kosonen) з Міністерства закордонних справ.

3. Заявник стверджував, зокрема, що держава не виконала свій позитивний обов’язок захисту його права на повагу до приватного життя відповідно до статті 8 Конвенції.

4. Рішенням від 27 червня 2006 року Суд визнав заяву прийнятною.

5. Заявник та Уряд подали кожен свої додаткові письмові зауваження (пункт 1 правила 59). Після рішення Палати, яка перед тим проконсультувалася зі сторонами, про відсутність необхідності у проведенні слухання по суті (пункт 3 правила 59 *in fine*), сторони відповіли письмово на зауваження одна одній. Крім того, було отримано коментарі третьої сторони від Гельсінської фундації за права людини (Helsinki Foundation for Human Rights), якій Голова дав дозвіл долучитися за процедурою письмового провадження (пункт 2 статті 36 Конвенції та пункт 2 правила 44).

ФАКТИ

I. ОБСТАВИНИ СПРАВИ

6. Заявник народився у 1986 році.

7. 15 березня 1999 року невідома особа чи особи розмістили рекламне оголошення на сайті знайомств в інтернеті від імені заявника, якому тоді було 12 років, без його відома. У повідомленні згадувалися його вік та рік народження, давався детальний опис його фізичних характеристик, наводився лінк на веб-сторінку, яку він мав на той час, де було зображено його фото, а також телефонний номер, який був правильний за винятком однієї цифри. У повідомленні стверджувалося, що заявник прагнув інтимних відносин з хлопцем його віку чи старше, який би “показав би йому як це робиться”.

8. Заявник дізнався про оголошення в інтернеті, коли він отримав лист електронною поштою від чоловіка, який запропонував зустрітися і “тоді дізнатися, чого ти хочеш”.

9. Батько заявника звернувся до поліції з проханням ідентифікувати особу, яка розмістила оголошення, з тим, що пред’явити їй обвинувачення. Однак, постачальник послуг інтернет відмовився розкрити особу володільця так званої динамічної IP-адреси, про яку йшлося, вважаючи себе зобов’язаним додержуватися вимог конфіденційності телекомунікацій, як це було визначено законом.

10. Тоді поліція звернулася до районного суду Гельсінкі (*käräjäoikeus, tingsrätten*) з тим, щоб зобов’язати інтернет-провайдера розкрити зазначену інформацію відповідно до статті 28 Закону про кримінальні розслідування (*esitutkintalaki, förundersökningslagen*; Закон № 449/1987 зі змінами, внесеними Законом № 692/1997).

11. У рішенні, прийнятому 19 січня 2001 року, районний суд відмовив, оскільки не існувало чіткого законодавчого положення, яке б дозволяло йому зобов’язати постачальника послуг розкрити телекомунікаційні ідентифікаційні дані в порушення професійної таємниці. Суд зазначив, що згідно зі статтею 3 розділу 5а Закону про примусові заходи (*pakkokeinolaki, tvångsmedelslagen*; Закон № 450/1987) і статтею 18 Закону про захист приватності та безпеку даних у телекомунікаціях (*laki yksityisyydensuojasta televiestinnässä ja teletoiminnan tietoturvasta, lag om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet*; Закон № 565/1999) поліція мала право отримати телекомунікаційні ідентифікаційні дані у випадках, які стосувалися певних порушень, незважаючи на обов’язок додержувати їх таємницю. Проте зловмисне введення в оману не належало до таких порушень.

12. 14 березня 2001 року Апеляційний суд (*hovioikeus, hovrätten*) підтримав це рішення, а 31 серпня 2001 року Верховний суд (*korkein oikeus, högsta domstolen*) відмовив у наданні дозволу на подання апеляції.

13. Особу, яка відповіла на оголошення на сайті знайомств та сконтактувала із заявником, було ідентифіковано через його адресу електронної пошти.

14. Виконавчий директор компанії, яка надавала інтернет-послуги, не міг бути притягнений до відповідальності, оскільки у своєму рішенні від 2 квітня 2001 року прокурор установив, що строк давності вплив для відповідного порушення. Відповідним порушенням було порушення Закону про персональні дані (*henkilötietolaki, personuppgiftslagen*; Закон № 523/99, який набув чинності 1 червня 1999 року). Якщо точніше, то постачальник послуг оприлюднив наклепницьке повідомлення на своєму веб-сайті, не перевірявши особу відправника.

II. ВІДПОВІДНЕ НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО ТА ПРАКТИКА

15. Конституційний Акт Фінляндії (*Suomen hallitusmuoto, Regeringsform för Finland*; Закон № 94/1919 зі змінами, внесеними Законом № 969/1995) був чинним до 1 березня 2000 року. Його стаття 8 відповідала статті 10 чинної Конституції Фінляндії (*Suomen perustuslaki, Finlands grundlag*; Закон № 731/1999), яка передбачає, що гарантується право кожного на приватне життя.

16. У період подій, про які йдеться у справі, стаття 3 розділу 27 Кримінального кодексу (*rikoslaki, strafflagen*; Закон № 908/1974) передбачала:

“Особа, яка в інший за згаданий вище спосіб вчинить акт зловмисного введення в оману проти іншої особи шляхом образливого висловлювання, погрози чи іншої принизливої дії, карається за зловмисне введення в оману штрафом чи ув’язненням на строк не більше трьох місяців.

Якщо зловмисне введення в оману вчинено публічно або поширено у друкованому, письмовому чи графічному вигляді винуватою особою або внаслідок її дій, відповідальна особа карається штрафом або ув’язненням на строк не більше чотирьох місяців.”

17. У період подій, про які йдеться у справі, стаття 3 розділу 5а Закону про примусові заходи передбачала:

“Умови для моніторингу телекомунікацій

У разі наявності підстави підозрювати особу у вчиненні

1) порушення, що карається не менше ніж ув'язненням строком у чотири місяці,

2) порушення проти комп'ютерної системи з використанням пристрою-терміналу, порушення у сфері наркотиків, або

3) карний замах на вчинення порушення, згаданого вище в цій статті,

орган, що веде кримінальне розслідування, може бути уповноважений на моніторинг телекомунікаційного зв'язку, який знаходиться у володінні підозрюваного чи який за припущенням знаходиться у його користуванні, або на тимчасове відключення такого зв'язку, якщо інформація, отримана за допомогою моніторингу чи відключення зв'язку, може вважатися дуже важливою для розслідування порушення ...”

18. Пункт 1(1) статті 18 Закону про захист приватності та безпеки даних у телекомунікаціях, який набув чинності 1 липня 1999 року та був скасований 1 вересня 2004 року, передбачав:

“Незважаючи на обов'язок таємниці, передбачений у статті 7, поліція має право отримувати:

(1) ідентифікаційні дані щодо передачі на конкретний пристрій за згоди потерпілої сторони та власника засобу зв'язку, якщо це необхідно в цілях розслідування порушення, передбаченого в статті 9а розділу 16, статті 13(2) розділу 17 або статті 3а розділу 24 Кримінального кодексу (Закон № 39/1889) ...”.

19. Стаття 48 Закону про персональні дані передбачає, що постачальник послуги під загрозою кримінальної відповідальності зобов'язаний перевіряти відправника перед тим, як оприлюднити наклепницькі повідомлення на своєму веб-сайті. Стаття 47 передбачає, що постачальник послуги також відповідає за відшкодування шкоди.

20. У період подій, про які йдеться у справі, обробка та оприлюднення чутливої інформації стосовно сексуальної поведінки на інтернет-сервері без згоди суб'єкта даних каралася в кримінальному порядку в якості порушення захисту даних у статті 43 Закону про персональні файли (Закон № 630/1995) та статті 9 розділу 38 (Закон № 578/1995) Кримінального кодексу, а також в якості порушення захисту даних у статті 44 Закону про персональні файли. Крім того, це також могло призвести до відповідальності за завдання шкоди згідно зі статтею 42 (Закон № 471/1987) зазначеного Закону.

21. Стаття 17 Закону про здійснення свободи вираження поглядів у засобах масової інформації (*laki sanavapauden käyttämisestä joukkoviestinnässä, lagen om yttrandefrihet i masskommunikation*: Закон № 460/2003), який набув чинності 1 січня 2004 року, передбачає:

“Розкриття ідентифікуючої інформації для повідомлення у мережі

За заявою посадової особи, уповноваженої проводити арешт, державного обвинувача чи потерпілої сторони суд може видати наказ до володільця передавача, сервера чи іншого схожого пристрою розкрити заявникові інформацію, необхідну для ідентифікації відправника повідомлення в мережі, якщо наявні розумні підстави вважати, що зміст повідомлення є таким, що його публічне поширення становить кримінальне порушення. Однак, видання наказу про розкриття ідентифікуючої інформації потерпілій стороні дозволяється лише в тому випадку, якщо він чи вона має право ініціювати справу приватного обвинувачення за таким порушенням. Заява подається до районного суду за місцем знаходження володільця пристрою або до районного суду Гельсінкі впродовж трьох місяців після оприлюднення повідомлення, про яке йдеться. Суд може посилити наказ, включивши до нього загрозу штрафу.”

III. ВІДПОВІДНІ МІЖНАРОДНІ МАТЕРІАЛИ

A. Рада Європи

22. Швидкий розвиток телекомунікаційних технологій в останні десятиріччя призвів до появи нових типів злочинів, а також зробив можливим вчинення традиційних злочинів за допомогою нових технологій. Рада Європи визнала потребу адекватної та швидкої відповіді на цей новий виклик ще в 1989 році, коли Комітет Міністрів схвалив Рекомендацію № R (89) 9 про злочини, пов'язані з комп'ютерами. Маючи рішучість забезпечити те, щоб слідчі органи мали належні спеціальні повноваження при розслідуванні комп'ютерних злочинів, у 1995 році Комітет Міністрів схвалив Рекомендацію № R (95) 13 щодо проблем кримінального процесуального права, пов'язаних з інформаційними технологіями. У пункті 12 принципів, які додавалися, було рекомендовано:

“Спеціальні обов'язки повинні покладатися на постачальників послуг, які пропонують телекомунікаційні послуги населенню через публічні чи приватні мережі, щодо надання інформації для ідентифікації абонента за наказом уповноваженого органу розслідування.”

23. В інших принципах, пов'язаних з обов'язком співпрацювати з органами розслідування, передбачалося:

“9. З урахуванням юридичних привілеїв чи захисту, більшість правових систем дозволяють органам розслідування видавати наказ особам про передачу предметів, які знаходяться в їхньому контролі, які необхідні в якості доказів. Аналогічно слід передбачити положення щодо права видавати наказ особам про подання будь-яких конкретних даних, які знаходяться в їхньому контролі в комп'ютерній системі у формі, яка вимагається органом розслідування.

10. З урахуванням юридичних привілеїв чи захисту, органи розслідування повинні мати повноваження видавати наказ особам, які мають у своєму контролі дані в комп'ютерній системі, надавати всю необхідну інформацію з тим, щоб

уможливити доступ до комп'ютерної системи та даних, які в ній містяться. Кримінальний процесуальний закон повинен забезпечувати те, щоб подібний наказ міг видаватися іншим особам, які мають знання про роботу комп'ютерної системи, або щоб були застосовані заходи збереження даних, які в ній містяться.”

24. У 1996 році Європейський комітет з проблем злочинності створив комітет експертів з питання кіберзлочинності. Існувало відчуття, що, хоча попередні дві рекомендації з матеріального та процесуального права не залишилися непоміченими, лише обов'язковий міжнародний документ міг забезпечити необхідну ефективність у боротьбі проти порушень у кіберпросторі. Конвенція про кіберзлочинність була відкрита для підписання 23 листопада 2001 року та набула чинності 1 липня 2004 року. Це перший і єдиний міжнародний договір стосовно злочинів, що вчиняються через інтернет, і він є відкритим для всіх держав. Конвенція вимагає від країн запровадити кримінальну відповідальність за такі діяння: незаконний доступ до комп'ютерної системи, незаконне перехоплення комп'ютерних даних, втручання у дані чи комп'ютерну систему, зловживання пристроями, пов'язані з комп'ютерами підробка та шахрайство, дитяча порнографія, порушення авторських та суміжних прав. Додатковий протокол до Конвенції, схвалений у 2003 році, далі вимагає криміналізації мови ненависті, ксенофобії та расизму. Сфера дії процедурних положень Конвенції виходить за межі порушень, визначених у Конвенції, оскільки вони застосовуються до будь-яких порушень, вчинених за допомогою комп'ютерної системи:

“Стаття 14 – Сфера дії процедурних положень

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань.

2. ... кожна Сторона застосовує повноваження і процедури, передбачені у пункті 1 цієї статті, до:

а) кримінальних правопорушень, встановлених відповідно до статей 2 - 11 цієї Конвенції;

б) інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем; та

с) збору доказів у електронній формі стосовно кримінального правопорушення.

3. ...”

25. Процедурні повноваження включають таке: термінова охорона даних, які зберігаються, термінова охорона і часткове розкриття даних про рух інформації, наказ про надання даних, обшук і арешт

комп'ютерних даних, збирання інформації про рух даних у режимі реального часу та перехоплення змісту даних. Особливо важливим є повноваження видавати наказ постачальнику послуг про надання інформації про абонента послуг стосовно таких послуг; дійсно, пояснювальна доповідь описує складність ідентифікації порушника як одну з головних перешкод у боротьбі проти злочинності в мережевому середовищі:

“Стаття 18 – Наказ про надання

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам видавати накази:

а. особі, яка знаходиться на її території, - про надання конкретних комп'ютерних даних, які знаходяться у володінні чи контролі такої особи і які зберігаються у комп'ютерній системі або на носії комп'ютерної інформації; та

б. постачальнику послуг, який пропонує свої послуги на території Сторони, - про надання інформації про абонента, пов'язаної з такими послугами, яка знаходиться у володінні чи контролі такого постачальника послуг.

2. Повноваження і процедури, про які йдеться у цій статті, регулюються статтями 14 і 15.

3. Для цілей цієї статті термін "інформація про абонента" означає будь-яку інформацію у формі комп'ютерних даних чи в будь-якій іншій формі, яка знаходиться у постачальника послуг, стосується абонентів його послуг, крім руху даних або власне змісту даних, та за допомогою якої можна встановити:

а. тип комунікаційної послуги, яка використовується, її технічні положення і період користування послугою;

б. особу абонента, поштову або географічну адресу, телефонний та інший номер доступу, інформацію про рахунки і платежі, яка наявна на підставі угоди або домовленості про постачання послуг;

с. будь-яку іншу інформацію за місцем встановлення комунікаційного обладнання, яка наявна на підставі угоди або домовленості про постачання послуг.”

26. У пояснювальній доповіді зазначається, що під час кримінального розслідування інформація про абонента може бути потрібна в основному у двох ситуаціях. По-перше, для визначення того, які послуги та пов'язані технічні засоби використовувалися або використовуються абонентом, такі як тип використовуваної телефонної послуги, тип інших пов'язаних послуг (наприклад, переадресація дзвінків, голосова пошта), телефонний номер чи інша технічна адреса (наприклад, адреса електронної пошти). По-друге, коли технічна адреса відома, інформація про абонента потрібна для

того, щоб допомогти в ідентифікації відповідної особи. Наказ про надання інформації є заходом з меншим рівня втручання та менш обтяжливим заходом, який правоохоронні органи можуть застосувати замість таких заходів, як перехоплення змісту даних чи збирання даних у режимі реального часу, які повинні чи можуть бути обмежені лише серйозними порушеннями (статті 20 та 21).

27. На всесвітній конференції “Співпраця проти кіберзлочинності”, яка була проведена у Страсбурзі 1-2 квітня 2008 року, було схвалено “Настанови щодо співпраці між правоохоронними органами та постачальниками інтернет-послуг проти кіберзлочинності”. Їхня мета - допомогти правоохоронним органам та постачальникам інтернет-послуг структурувати свою взаємодію стосовно питань кіберзлочинності. Уважалося надзвичайно важливим, щоб дві сторони співпрацювали одна з одною в ефективний спосіб задля покращення кібербезпеки та мінімізації використання послуг для незаконних цілей. Настанови описують практичні заходи, яких слід ужити правоохоронним органам та постачальникам послуг, заохочуючи їх обмінюватися інформацією з тим, щоб посилити свої можливості в ідентифікації та протидії новим типам кіберзлочинності. Зокрема, постачальники послуг заохочувалися до співпраці з правоохоронними органами для того, щоб допомогти мінімізувати використання послуг для злочинної діяльності, визначеної законом.

В. Організація Об'єднаних Націй

28. З багатьох резолюцій, ухвалених у сфері кіберпростору, найбільш доречними для цілей цієї справи є резолюції Генеральної Асамблеї № 55/63 від 4 грудня 2000 року та № 56/121 від 19 грудня 2001 року з назвою “Протидія кримінальному зловживанню інформаційними технологіями”. Серед заходів, спрямованих на протидію такому зловживанню, у Резолюції № 55/63 було рекомендовано таке:

“(f) Правні системи повинні дозволяти збереження та швидкий доступ до електронних даних, які стосуються конкретного кримінального розслідування;”.

29. Наступна резолюція відмітила цінність різних заходів та знову запросила держави-члени взяти їх до уваги.

С. Європейський Союз

30. 15 березня 2006 року Європейський Парламент та Рада Європейського Союзу схвалили Директиву № 2006/24/ЕС про збереження даних, створених або оброблених у зв'язку з наданням загальнодоступних електронних комунікаційних послуг або

громадських мереж зв'язку, що вносила зміни до попередньої Директиви про збереження даних № 2002/58/ЕС. Метою Директиви є гармонізація положень законодавства держав-членів стосовно обов'язків постачальників телекомунікаційних послуг щодо збереження певних даних з тим, щоб забезпечити доступність таких даних у цілях розслідування, виявлення та кримінального переслідування серйозних злочинів, як вони визначені кожною державою-членом у своєму національному законодавстві. Директива застосовується до даних про трафік і місцезнаходження щодо як юридичних, так і фізичних осіб, та до дотичних даних, необхідних для ідентифікації абонента або зареєстрованого користувача. Вона не застосовується до змісту електронних комунікацій. Директива вимагає від держав-членів забезпечити, щоб певні категорії даних зберігалися строком від шести місяців до двох років. Стаття 5 визначає дані, які повинні зберігатися:

“1. Держави-члени повинні забезпечити те, щоб такі категорії даних зберігалися відповідно до цієї Директиви:

(а) дані, необхідні для відстеження та ідентифікації джерела комунікацій:

...

(2) щодо доступу в інтернет, електронної пошти та інтернет-телефонії:

...;

(iii) ім'я та адресу абонента або зареєстрованого користувача, якому на момент комунікації була надана IP-адреса, ID користувача або номер телефону;”

31. Держави-члени повинні були імплементувати цю Директиву до 15 вересня 2007 року. Проте 16 держав, у тому числі Фінляндія, скористалися правом відкласти її застосування до доступу в інтернет, інтернет-телефонії та електронної пошти до 15 березня 2009 року.

IV. ПОРІВНЯЛЬНЕ ПРАВО

32. Порівняльний аналіз законодавства держав-членів Ради Європи показує, що в більшості країн існує спеціальний обов'язок постачальників телекомунікаційних послуг надавати комп'ютерні дані, у тому числі інформацію про абонента, у відповідь на запит слідчих або судових органів незалежно від природи злочину. Деякі країни мають лише загальні положення щодо надання документів та інших даних, які на практиці можуть розширюватися і включати також обов'язок подавати конкретні комп'ютерні та абонентські дані. Декілька країн ще не впровадили положення статті 18 Конвенції Ради Європи про кіберзлочинність.

V. ПОДАННЯ ТРЕТІХ СТОРІН

33. Гельсінська фундація за права людини зауважила, що справа, яка розглядається, піднімає питання знаходження балансу між захистом приватності, честі та репутації з одного боку і здійсненням свободи вираження поглядів з іншого боку. На її думку, ця справа дає Суду можливість визначити позитивні обов'язки держави в цій сфері та таким чином сприяти спільним стандартам щодо використання інтернету у країнах-членах.

34. Фундація вказала на те, що інтернет є дуже особливим способом спілкування і одним з основоположних принципів його використання є анонімність. Високий рівень анонімності заохочує свободу слова та вираження різних ідей. З іншого боку, інтернет є потужним засобом для наклепу чи образи людей або порушення їхнього права на приватність. Через анонімність інтернету, жертва порушення знаходиться у вразливому становищі. На відміну від традиційних засобів масової інформації, жертва не може легко ідентифікувати особу, яка зводить наклеп, через той факт, що можна заховатися за псевдонімом або навіть використати чуже ім'я.

ПРАВО

I. СТВЕРДЖУВАНІ ПОРУШЕННЯ СТАТЕЙ 8 ТА 13 КОНВЕНЦІЇ

35. Заявник скаржився за статтею 8 Конвенції, що мало місце втручання у його приватне життя і що, усупереч статті 13 Конвенції, не існувало ефективного засобу юридичного захисту для з'ясування особи, яка розмістила наклепницький текст в інтернеті від його імені.

Стаття 8 передбачає:

“1. Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції.

2. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.”

Стаття 13 передбачає:

“Кожен, чий права та свободи, визнані в цій Конвенції, було порушено, має право на ефективний засіб юридичного захисту в національному органі, навіть

якщо таке порушення було вчинене особами, які здійснювали свої офіційні повноваження.”

A. Доводи сторін

36. Заявник стверджував, що законодавство Фінляндії у період, про який йдеться у справі, захищало злочинця, тоді як потерпілий не мав засобів для отримання відшкодування чи захисту проти порушення приватності. Відповідне діяння каралося за Кримінальним кодексом, але через недбалість Уряду не було забезпечено те, щоб Закон про захист приватності та безпеку даних у телекомунікаціях і Закон про примусові заходи відповідали один одному. Він стверджував, що негарантована можливість стягнення цивільної шкоди, особливо від третьої сторони, не була достатньою для захисту його прав. Він наголосив, що не мав засобів для ідентифікації особи, яка розмістила оголошення в інтернеті. Хоча в деяких випадках компенсація може бути ефективним засобом юридичного захисту, це залежало від того, чи сплатила її особа, яка порушила права потерпілого, що не було можливим у його випадку. Уряд зауважив, що було введено в дію нове законодавство, яке, якби воно існувало на час подій, зробило б цю заяву непотрібною. На думку заявника, Уряд не навів жодного пояснення тому, що він не зміг надати йому захист у відповідний період часу. Тому він уважав, що мало місце порушення статей 8 та 13.

37. Уряд наголосив, що в цій справі втручання у приватне життя заявника було вчинено іншою особою. Відповідне діяння розглядалося у національному законодавстві як зловмисне введення в оману і як таке було б караним, що мало стримуючий ефект. Було розпочато розслідування для ідентифікації особи, яка розмістила оголошення в інтернеті, але воно було неуспішним через чинне тоді законодавство, яке було спрямовано на захист свободи вираження поглядів та права на анонімне вираження поглядів. Законодавство захищало особу, яка оприлюднювала анонімне повідомлення в інтернеті, так ґрунтовно, що цей захист також поширювався на повідомлення, які могли становити втручання у приватність іншої особи. Цей побічний ефект захисту пояснювався тим фактом, що поняття повідомлення, яке становило втручання у захист приватності, не було чітким і тому не було можливості чітко відмежувати такі повідомлення від захисту, який надавався законом. Проте існували інші засоби юридичного захисту, наприклад, Закон про персональні дані, який надавав захист від зловмисного введення в оману в тому, що оператор сервера, відповідно до положень цього закону щодо кримінальної відповідальності та відповідальності за завдану шкоду, був зобов'язаний забезпечити те, щоб записані ним чутливі дані оброблялися за згодою суб'єкта даних. Крім того, хоча строк давності притягнення до відповідальності за

порушення щодо персональних даних сплив, заявник все ще мав можливість вимагати компенсації від того, хто оприлюднив оголошення. Порівняно зі справою *X and Y v. the Netherlands* (рішення від 26 березня 1985 року, Series A no. 91), у цій справі відповідальність за завдання шкоди відносно менш серйозного порушення мала достатній стримуючий ефект. На додаток, існували інші механізми, доступні для заявника, такі як досудове розслідування поліції, кримінальне переслідування, судове провадження та відшкодування шкоди.

38. Уряд стверджував, що було важливо розглядати законодавчу ситуацію у відповідний період часу в її суспільному контексті, коли різке зростання використання інтернету лише розпочиналося. Чинне законодавство, а саме Закон про здійснення свободи вираження поглядів у засобах масової інформації (статті 2 та 17), що набув чинності 1 січня 2004 року, надає поліції ширші повноваження щодо порушення захисту того, хто оприлюднює анонімне інтернет-повідомлення, у цілях розслідування злочину. Нове законодавство відображає реакцію законодавця на суспільний розвиток, де все більше використання – і водночас зловживання – інтернету вимагало зміни меж захисту. Отже, з огляду на змінену ситуацію у суспільстві, наступне законодавство далі посилило захист приватного життя по відношенню до свободи вираження поглядів і особливо захисту осіб, які оприлюднюють анонімні інтернет-повідомлення.

39. Проте найважливішим у цій справі було те, що навіть законодавство, яке діяло у відповідний період, надавало заявникові засоби впливу проти поширення повідомлень, які втручалися у приватність, оскільки оператор інтернет-сервера, на якому було оприлюднено повідомлення, був зобов'язаний за законом перевірити, що особа, про яку йшлося, дала свою згоду на обробку чутливої інформації про неї на сервері оператора. Цей обов'язок підкріплювався кримінальною відповідальністю та відповідальністю за завдання шкоди. Отже, законодавство надавало заявникові достатній захист приватності та ефективні засоби юридичного захисту.

В. Оцінка Суду

40. Суд передусім зазначає, що заявник, неповнолітня особа 12 років у відповідний період, був об'єктом оголошення сексуального характеру на інтернет-сайті знайомств. Інформацію про особу того, хто розмістив оголошення, проте, не можливо було отримати від постачальника інтернет-послуг через законодавство, яке діяло на той час.

41. Застосовність статті 8 не оспорується: факти, які лежать в основі заяви, стосуються питання “приватного життя” – поняття, що

охоплює фізичну та душевну недоторканність особи (див. цитоване вище рішення у справі *X and Y v. the Netherlands*, параграф 22). Хоча ця справа розглядається за термінологією національного законодавства як зловмисне введення в оману, Суд волів би підкреслити саме ці аспекти поняття приватного життя, з огляду на потенційну загрозу фізичному та душевному спокою заявника, до якої призвела оскаржувана ситуація, та на його вразливість через його ранній вік.

42. Суд повторює, що хоча метою статті 8 є насамперед захист особи проти свавільного втручання з боку державних органів, вона не лише зобов'язує державу утриматися від такого втручання: на додаток до цього первинного негативного зобов'язання, можуть існувати позитивні обов'язки, які складають ефективний захист приватного або сімейного життя (див. *Airey v. Ireland*, рішення від 9 жовтня 1979 року, Series A no. 32, параграф 32).

43. Ці обов'язки можуть включати вжиття заходів, спрямованих на забезпечення поваги до приватного життя навіть у сфері відносин осіб між собою. Існують різні способи забезпечення поваги до приватного життя і суть обов'язку держави залежатиме від конкретного аспекту приватного життя, про який йдеться. Хоча вибір засобів для забезпечення дотримання статті 8 у сфері захисту від дій осіб знаходиться, у принципі, у межах розсуду держави, дієве попередження тяжких діянь, які ставлять під загрозу основоположні цінності та найважливіші аспекти приватного життя, вимагає ефективних положень кримінального права (див. *X and Y v. the Netherlands*, параграфи 23-24 та 27; *August v. the United Kingdom* (рішення про прийнятність), заява № 36505/02, 21 січня 2003 року, та *M.C. v. Bulgaria*, заява № 39272/98, параграф 150, ECHR 2003-XII).

44. Межі розсуду національних органів, проте, обмежуються положеннями Конвенції. Оскільки Конвенція є насамперед і головним чином системою захисту прав людини, Суд при її тлумаченні повинен зважати на мінливі умови всередині Договірних держав та реагувати, наприклад, на будь-яку еволюцію наближення до стандартів, яких слід досягнути (див. *Christine Goodwin v. the United Kingdom* [GC], заява № 28957/95, параграф 74, ECHR 2002-VI).

45. Суд вважає, що хоча ця справа може не досягати серйозності справи *X and Y v. the Netherlands*, де порушення статті 8 впливало з відсутності ефективної кримінальної санкції за зґвалтування дівчини-інваліда, до неї не можна ставитися як до тривіальної. Йшлося про злочинне діяння, яке стосувалося неповнолітнього і зробило його об'єктом уваги педофілів (див. також у цьому зв'язку параграф 41 вище).

46. Уряд погодився, що на момент подій у справі оператору сервера не можна було наказати надати інформацію, яка ідентифікувала порушника. Уряд стверджував, що захист забезпечувався завдяки

простому існуванню кримінального правопорушення зловмисного введення в оману та можливості пред'явлення обвинувачення чи позову про відшкодування шкоди проти оператора сервера. Щодо першого, то Суд зазначає, що існування порушення має обмежений стримуючий ефект, якщо не існує засобів для ідентифікації справжнього порушника та притягнення його до відповідальності. Тут Суд зауважує, що він не виключає можливості того, що позитивні обов'язки держави за статтею 8 стосовно гарантування фізичної чи душевної недоторканності особи можуть поширюватися на питання, пов'язані з ефективністю кримінального розслідування, навіть коли не йдеться про кримінальну відповідальність представників держави (див. *Osman v. the United Kingdom*, рішення від 28 жовтня 1998 року, *Reports of Judgments and Decisions* 1998-VIII, параграф 128). З точки зору Суду, держави мають позитивний обов'язок, що впливає зі статті 8 Конвенції, установити кримінальну відповідальність за правопорушення проти особи, у тому числі замах на такі правопорушення, а також посилити стримуючий ефект такої криміналізації, застосовуючи положення кримінального закону на практиці шляхом ефективного розслідування та кримінального переслідування (див., *mutatis mutandis*, цитоване вище рішення у справі *M.C. v. Bulgaria*, параграф 153). Там, де виникає загроза фізичному чи душевному спокою дитини, такі заходи набувають навіть ще більшої важливості. Суд нагадує у цьому зв'язку, що сексуальне насильство є безсумнівно огидним типом правопорушення з у край негативними наслідками для його жертв. Діти та інші вразливі особи мають право на захист держави, у вигляді дієвого стримування, від таких тяжких форм втручання в надзвичайно важливі аспекти їхнього приватного життя (див. *Stubbings and Others v. the United Kingdom*, 22 жовтня 1996 року, параграф 64, *Reports* 1996-IV).

47. Стосовно ж того аргументу Уряду, що заявник мав можливість отримати відшкодування шкоди від третьої сторони, а саме від постачальника послуг, Суд вважає, що цього було недостатньо за обставин справи. Очевидно, що як суспільний інтерес, так і захист інтересів потерпілих від злочинів проти їхнього фізичного чи душевного спокою вимагають наявності засобу захисту, який дозволяв б виявити та притягнути до відповідальності дійсного порушника, у цій справі – особу, яка розмістила оголошення від імені заявника, і щоб потерпілий міг отримати фінансове відшкодування від нього.

48. Суд згоден, що з огляду на складності, пов'язані з підтриманням правопорядку у сучасному суспільстві, позитивний обов'язок слід розуміти таким чином, щоб не покладати неможливий чи непропорційний тягар на органи влади або, як у цій справі, на законодавця. Іншою обставиною, яку слід брати до уваги, це потреба забезпечення того, щоб повноваження з контролю, запобігання та

розслідування злочинів здійснювалися у спосіб, що повною мірою забезпечує належну юридичну процедуру та інші гарантії, які правомірно покладають обмеження на розслідування злочинів та притягнення порушників до відповідальності, у тому числі гарантії, що містяться у статтях 8 та 10 Конвенції – гарантії, на які можуть покладатися самі порушники. Суд сприймає довід Уряду, що будь-який законодавчий недолік слід розглядати в його соціальному контексті у відповідний період часу. Водночас Суд зауважує, що відповідний інцидент стався у 1999 році, тобто тоді, коли було добре відомо, що інтернет, саме через його анонімний характер, може бути використаний у злочинних цілях (див. вище параграфи 22 та 24). Також у попереднє десятиріччя широко поширеною стала проблема сексуального насильства над дітьми. Тому не можна сказати, що держава-відповідач не мала можливості запровадити систему захисту дітей від спрямованих на них атак педофілів через інтернет.

49. Суд вважає, що практичний та дієвий захист заявника вимагав вжиття дієвих кроків для ідентифікації та кримінального переслідування порушника, тобто особи, яка розмістила оголошення. У цій справі такий захист не був наданий. Ефективне розслідування ніколи не могло бути розпочато через переважаючу вимогу конфіденційності. Хоча свобода вираження поглядів та конфіденційність комунікацій є надзвичайно важливими, а користувачі телекомунікаційних та інтернет-послуг повинні мати гарантію, що їхня власна приватність та свобода вираження поглядів буде поважатися, така гарантія не може бути абсолютною і в окремих випадках повинна поступатися іншим правомірним вимогам, таким як запобігання заворушенням чи злочинам або захист прав і свобод інших осіб. Не упереджуючи питання того, чи можуть дії особи, яка розмістила неналежне оголошення в інтернеті, підлягати захисту за статтями 8 та 10, враховуючи природу цього оголошення, що варта осуду, це тим не менше є завданням законодавця створити механізми для узгодження різних вимог, які конкурують за захист у цьому контексті. Такі механізми, проте, були відсутні на момент подій у справі, що призвело до того, що позитивний обов'язок Фінляндії по відношенню до заявника не міг бути реалізований. Цей недолік було пізніше виправлено. Проте механізми, запроваджені Законом про здійснення свободи вираження поглядів у засобах масової інформації (див. параграф 21), з'явилися запізно для заявника.

50. Суд вирішує, що в цій справі мало місце порушення статті 8.

51. З огляду на рішення стосовно статті 8, Суд вважає, що немає необхідності досліджувати, чи мало місце в цій справі також порушення статті 13 (див., серед інших рішень, *Sallinen and Others v. Finland*, заява № 50882/99, параграфи 102 та 110, 27 вересня 2005 року,

та *Copland v. the United Kingdom*, заява № 62617/00, параграфи 50-51, ECHR 2007-...).

II. ЗАСТОСУВАННЯ СТАТТІ 41 КОНВЕНЦІЇ

52. Стаття 41 Конвенції передбачає:

“Якщо Суд визнає факт порушення Конвенції або протоколів до неї і якщо внутрішнє право відповідної Високої Договірної Сторони передбачає лише часткове відшкодування, Суд, у разі необхідності, надає потерпілій стороні справедливую сатисфакцію.”

A. Шкода

53. У частині моральної шкоди заявник просив 3500 євро за страждання.

54. Уряд заявив, що присуджено має бути не більше 2500 євро.

55. Суд визнає доведеним те, що заявник мав би зазнати моральної шкоди. Він вважає, що достатня справедлива сатисфакція не буде забезпечена лише визнанням порушення і тому слід присудити компенсацію. Роблячи оцінку на основі справедливості, Суд присуджує заявникові 3000 євро за цим пунктом.

B. Витрати

56. Заявник просив 2500 євро за витрати під час національного провадження та провадження перед Судом.

57. Уряд поставив під сумнів те, чи були надані заявником відповідні документи.

58. Суд зауважує, що не було подано жодних документів, як це вимагається правилом 60 Регламенту Суду. Тому ці вимоги слід відхилити.

C. Пеня

59. Суд вважає належним те, щоб пеня ґрунтувалася на граничній кредитній ставці Європейського центрального банку, до якої додаються три відсоткові пункти.

НА ЦИХ ПІДСТАВАХ СУД ОДНОГОЛОСНО

1. *Постановляє*, що мало місце порушення статті 8 Конвенції;

2. *Постановляє*, що немає необхідності розглядати скаргу за статтею 13 Конвенції;
3. *Постановляє*
 - (а) що держава-відповідач повинна сплатити заявнику, упродовж трьох місяців з дати, коли рішення стане остаточним згідно з пунктом 2 статті 44 Конвенції, 3000 (три тисячі) євро в частині моральної шкоди плюс суму будь-якого податку, що може стягуватися;
 - (b) що зі впливом зазначених вище трьох місяців і до виплати на зазначені суми у період несплати має нараховуватися простий відсоток у розмірі граничної кредитної ставки Європейського центрального банку плюс три відсоткові пункти;
4. *Відхиляє* решту вимог заявника щодо справедливої сатисфакції.

Учинено англійською мовою та повідомлено письмово 2 грудня 2008 року відповідно до пунктів 2 і 3 правила 77 Регламенту Суду.

Лоуренс Ерлі
Секретар

Ніколас Братца
Голова Суду

© Рада Європи/Європейський суд з прав людини, 2012

Офіційними мовами Європейського суду з прав людини є англійська та французька мови. Цей переклад було замовлено за підтримки Трастового фонду з прав людини Ради Європи (www.coe.int/humanrightstrustfund). Переклад не є обов'язковим для Суду, також Суд не несе жодної відповідальності за його якість. Він може бути завантажений з бази даних рішень Європейського суду з прав людини HUDOC (<http://hudoc.echr.coe.int>) чи будь-якої іншої бази даних, з якою Суд поділився цим перекладом. Переклад може бути відтворено у некомерційних цілях за умови цитування в повному обсязі назви справи, а також зазначення наведеного вище копірайту та згадки про Трастовий фонд з прав людини. Якщо планується використати будь-яку частину цього перекладу в комерційних цілях, прохання звернутися за адресою publishing@echr.coe.int.

© Council of Europe/European Court of Human Rights, 2012 [or subsequent year].

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). 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 shared 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.

© 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). 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>), ou 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 de 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.