EuroISPA

Рада Європи

Керівні принципи у сфері прав людини для інтернет-провайдерів

Розроблені Радою Європи
у співпраці з
Європейською асоціацією інтернет-провайдерів
(EuroISPA)

Спільна програма Європейського Союзу та Ради Європи
«Зміцнення інформаційного суспільства в Україні»

Фінансується Європейським Союзом та Радою Європи

EUROPEAN UNION

COUNCIL OF EUROPE

CONCEIL DE L'EUROPE

Впроваджується Радою Європи

Це видання опубліковано в рамках спільної програми Ради Європи та Європейського Союзу «Зміцнення інформаційного суспільства в Україні».

Розроблені Радою Європи у тісній співпраці з Європейською асоціацією інтернет- провайдерів (EuroISPA), ці керівні принципи надають контрольні показники у сфері прав людини для інтернет-провайдерів (ІП). Підкреслюючи важливу роль, яку ІП відіграють у наданні користувачам Інтернету таких основних послуг, як доступ, електронна пошта чи контент-послуги, вони наголошують на важливості безпеки користувачів та їх права на приватність і свободу вираження поглядів, а також, у зв'язку з цим, на важливості усвідомлення провайдерами можливого впливу своєї діяльності на права людини.

Європейський Союз складається з 28 держав-членів та їх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років нам знадобилось для створення зони миру, демократії, стабільності й процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їх народами та з народами з-поза їх меж. Більше інформації про ЄС: http://delukr.ec.europa.eu.

Рада Європи – це міжурядова організація, до якої входить 47 держав-членів, завданням якої є захищати права людини, плюралістичну демократію та верховенство права; сприяти усвідомленню та оцінці європейської культурної самобутності та розмаїття європейських культур; знаходити вирішення проблем, що існують у суспільстві (національні меншини, ксенофобія, нетерпимість, захист навколишнього середовища, клонування, СНІД, наркотики, організована злочинність і т. ін.); допомагати стверджувати стабільність демократії у Європі через підтримку політичних, законотворчих та конституційних реформ. Більше інформації про Офіс Ради Європи в Україні: http://www.coe.int/en/web/kyiv.

Спільна програма Європейського Союзу та Ради Європи «Зміцнення інформаційного суспільства в Україні» має на меті покращити свободу, різноманітність і плюралізм медіа, а також сприяти ефективності системи захисту персональних даних. Також – програма спрямована на відкритий, всебічний і сталий підхід до управління Інтернетом, що ґрунтується на правах людини і ставить людину в центр уваги. Крім того, програма сприятиме виконанню обов'язків і зобов'язань України перед Радою Європи, реалізації Угоди про асоціацію з ЄС і Плану дій з лібералізації ЄС візового режиму для України. Більше інформації про програму: http://www.coe.int/en/web/kyiv/41.

Керівні принципи у сфері прав людини для інтернет-провайдерів

Розроблені Радою Європи
у співпраці з
Європейською асоціацією інтернет-провайдерів
(EuroISPA)

ЗМІСТ

Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду.

Стаття 10 Європейської конвенції з прав людини

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

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 8 Європейської конвенції з прав людини

Розуміння ролі та позиції інтернет-провайдерів у дотриманні й заохоченні прав людини

1. Забезпечуючи базову інфраструктуру та основні послуги, які дозволяють користувачам отримувати доступ до Інтернету, користуватися ним і тим самим здійснювати свої права на отримання користі від інформаційного суспільства, інтернет-провайдери (ІП) надають послуги, які мають значну цінність для служіння суспільству.

2. ІП знаходяться в унікальному положенні та мають можливість забезпечувати здійснення і дотримання прав та основних свобод людини. Крім того, надання інтернет-послуг все більше стає передумовою для всеохоплюючої партиципаторної демократії (демократії участі). ІП також відіграють важливу роль по відношенню до держав, які віддані справі захисту та забезпечення цих прав і свобод в рамках своїх зобов'язань за міжнародним правом.

3. ІП надають своїм клієнтам різноманітні послуги, чи то в якості провайдерів доступу, чи як провайдери інших послуг інформаційного суспільства (провайдери застосунків, контент-провайдери та/або хостинг-провайдери). У цьому керівництві визнано, що не всі ІП відіграють однакову роль та мають однакові обов'язки по відношенню до користувачів, але вони можуть залежати від видів послуг, які надає ІП, і сегменту клієнтів, яких він обслуговує.

4. Провайдери доступу допомагають увійти до мережі Інтернет, а тому й до різноманітності інформації, культури та мов; часто вони є першою точкою контакту і довіри для користувачів. Їх роль є передумовою для надання користувачам можливості та права на отримання доступу до благ інформаційного суспільства, зокрема, на пошук і поширення інформації та ідей, формування знань та отримання доступу до освіти.

5. Провайдерів доступу, зокрема тих, які обслуговують домашніх користувачів та сім'ї, можна вважати такими, що частково виконують роль публічної служби, яка сприяє забезпеченню прав своїх клієнтів на отримання користі від інформаційного суспільства та, у зв'язку з цим, посиленню здійснення та реалізації їх прав і свобод.

6. Подібним чином, оскільки провайдери доступу, а особливо хостинг-провайдери, можуть виконувати рішення і вчиняти дії відносно доступності послуг (наприклад, видаляти, блокувати або фільтрувати контент), це може впливати на права і свободи.

7. ІП мають доступ до різних об'ємів інформації (контенту і/або даних щодо трафіку), що підкреслює їх важливу роль і позицію по відношенню до прав і свобод користувачів. На ІП не повинно покладатися загальне зобов'язання активно відслідковувати контент і дані щодо трафіку; проте в особливих випадках, визначених законодавством, та внаслідок конкретних розпоряджень від ІП може потребуватися допомога у відслідковуванні контенту чи даних або передачі інформації про користувачів третій стороні. Такі випадки можуть впливати на свободу вираження поглядів чи право на приватне життя.

8. В цілому, ІП, особливо хостинг- і контент-провайдери, мають значний потенціал для забезпечення можливостей і благ інформаційного суспільства; це слід підкреслювати та доводити до відома користувачів, держав і, що найголовніше, самих ІП.

9. У зв'язку з цим, ІП рекомендується взяти до уваги, обговорити і докласти всіх зусиль для виконання наступних керівних принципів (див. на зворотному боці аркуша), а також розглянути можливість посилання на них на своїх веб-сайтах та в угодах з кінцевими користувачами.

10. У співпраці з асоціаціями ІП, державами-членами, і, за необхідності, з допомогою Ради Європи, ІП також рекомендується довести ці керівні принципи і підняті в них питання до відома ключового персоналу своїх організацій.

11. Асоціації ІП можуть відігравати важливу роль, беручи на себе колективну відповідальність за підвищення обізнаності та надання інформації стосовно питань, піднятих у цих керівних принципах. Їм рекомендується активно просувати ці керівні принципи серед своїх членів, наприклад, посилаючись на них, включаючи їх до власних кодексів поведінки та надаючи експертні консультації.

12. Стосовно інформації, яка повинна надаватися клієнтам, ІП можуть прийняти рішення про її передачу через асоціації ІП, зокрема коли йдеться про малі підприємства і якщо ця інформація не є специфічною для провайдера (наприклад, інформація про ризики в мережі Інтернет). Крім того, асоціації ІП можуть сприяти гармонізації інформації про користувачів і накопичувати знання стосовно питань, піднятих у керівних принципах. Крім того, вони можуть здійснювати співробітництво та обмін знаннями з існуючими структурами у сфері інтернет-безпеки, такими як Програма Європейського Союзу "Безпечніший Інтернет Плюс".

13. Керівні принципи не порушують зобов'язання, застосовні до ІП, та їх діяльності, передбачені національним, європейським та міжнародним правом, і повинні розглядатися у поєднанні з ними.

Сфера застосування цих керівних принципів

14. Наступні керівні принципи згруповані в декілька розділів відповідно до ролей, які відіграють ІП. Перший розділ застосовується до провайдерів доступу до Інтернету (провайдерів послуг з надання доступу до Інтернету "на вимогу" або спеціалізованих послуг з доступу до Інтернету). Другий розділ застосовується до таких провайдерів інших послуг інформаційного суспільства, як хостинг-провайдери, контент-провайдери і провайдери застосунків. Третій розділ застосовується, відповідно, до всіх інтернет-провайдерів.

15. Керівні принципи не застосовуються до простих транзитних провайдерів.

Керівні принципи у сфері прав людини для інтернет-провайдерів

Керівні принципи для ІП, які надають послуги доступу

• 16. Переконайтеся, що ваші клієнти мають доступ до інформації про потенційні загрози своїм правам, безпеці та приватності в Інтернеті, в тому числі до інформації про те, що ви робите, щоб допомогти своїм клієнтам протистояти цим загрозам. Надайте інформацію про доступні інструменти і програмне забезпечення, які ваші клієнти можуть використовувати, щоб надалі захищати себе. Якщо ви надаєте цю інформацію самостійно, переконайтеся, що вона надається в якомога точніший, доступніший і сучасніший спосіб. Якщо ви не надаєте цю інформацію самостійно, дайте своїм клієнтам посилання на адекватні інформаційні ресурси, зокрема, на ресурси асоціацій ІП або мереж у сфері інтернет-безпеки. Зокрема, можна було б надати доступ до інформації про такі загрози:

16.1. Незаконний та/або шкідливий контент, загрози для дітей

• Надайте інформацію або посилання на інформацію про ризики натрапити на незаконний контент в Інтернеті чи сприяти його поширенню, а також про ризик того, що дітей буде піддано шкідливому контенту або поведінці під час їх знаходження в мережі. Останнє може включати контент або поведінку, що здатні негативно впливати на фізичне, емоційне і психологічне здоров'я дітей, наприклад, онлайн-порнографія, зображення та прославляння насильства, самоушкодження, приниження, дискримінаційні або расистські висловлювання або апологія (виправдання) такої поведінки, зваблення (грумінг), залякування, переслідування та інші форми домагання. Хоча від вас не чекатимуть консультацій щодо того, який контент чи поведінка є незаконними і/або шкідливими, надана вами інформація цілком могла б включати в себе:

– пояснення того, що ви робите для протидії такому контенту і поведінці, зокрема, інформацію про вашу співпрацю з гарячими лініями для боротьби з незаконним контентом (наприклад, з мережею "Inhope");

– вказівки щодо того, як користувачі можуть захиститися від ризиків натрапити на незаконний та/або шкідливий контент і

– поведінку (наприклад, давши їм посилання на відповідну інформацію на веб-сайтах, присвяченим безпеці в мережі Інтернет);

– інформацію про доступні програмні інструменти, призначені для захисту користувачів від незаконного та/або шкідливого контенту, в тому числі інформацію про те, як ці інструменти працюють і як користувачі можуть пристосувати їх для задоволення своїх індивідуальних потреб.

• Надайте інформацію або посилання на інформацію про те, що ваші клієнти можуть зробити, щоб захистити своїх дітей в Інтернеті. Зробіть посилання на веб-сайти з безпечним для дітей контентом і наявні інтернет-ресурси з питань безпеки, такі як довідник Ради Європи "Інтернет-грамотність" (www.coe.int/internet-literacy), розроблена Радою Європи онлайн-гра "Wild Web Woods" ("Дикі веб ліси") (www.wildwebwoods.org) або веб-сайти безпечних вузлів Інтернету (www.saferinternet.org).

16.2. Загрози безпеці

• У разі потреби, поясніть, що ви робите для захисту своїх клієнтів від загроз безпеці. Такі загрози можуть стосуватися цілісності даних (віруси, хробаки, трояни тощо), конфіденційності (наприклад, при здійсненні транзакцій в мережі), безпеки мережі або інших ризиків (наприклад, фішинг).

• Підвищіть поінформованість ваших клієнтів або дайте їм посилання на додаткову інформацію про те, як протистояти загрозам безпеці в Інтернеті.

16.3. Загрози для приватності

• Надайте інформацію або посилання на інформацію про потенційні загрози конфіденційності клієнтів під час користування Інтернетом. Такі загрози можуть стосуватися прихованого збирання, запису та обробки даних (шпигунське програмне забезпечення, профілювання). У разі потреби, дайте посилання на сайти ваших національних органів, які містять інформацію про відповідні закони, що стосуються приватності та захисту персональних даних.

• Надайте вашим клієнтам додаткову інформацію та вказівки щодо технічних засобів, якими вони можуть користуватися, щоб захистити себе від загроз для приватності (антишпигунські програми тощо).

• 17. Якщо ваші клієнти потребують підтримки у боротьбі з вищезазначеними загрозами, переконайтеся, що вони можуть робити подальші запити у належній формі (наприклад, телефоном, електронною поштою, листами або через особисті контакти) або дайте їм посилання на відповідні інформаційні ресурси.

• 18. Будьте обережними, блокуючи або погіршуючи якість своїх послуг задля використання деяких застосунків або програмного забезпечення на основі певного технічного протоколу. Якщо ви використовуєте обмежувачі пропускної здатності, фільтри або блокуєте певний трафік, переконайтеся, що ваших клієнтів було чітко і заздалегідь поінформовано про такі обмеження послуг.

• 19. Відключення доступу до облікових запитів окремих клієнтів становить обмеження прав вашого клієнта на доступ до благ інформаційного суспільства та на здійснення ним своїх прав на свободу вираження поглядів та інформаціїї. Відключення доступу має здійснюватися тільки на прохання правоохоронних органів чи з інших законних і строго необхідних підстав, таких як порушення договірних зобов'язань або навмисне зловживання, а також з урахуванням правових гарантій, що можуть застосовуватися відповідно до національного законодавства. Де це доцільно, клієнт має бути належним чином попереджений і заздалегідь поінформований, йому мають бути наведені достатні підстави для відключення доступу надані інструкції про заходи, яких потрібно вжити для відновлення доступу.

Керівні принципи для ІП, які надають інші послуги інформаційного суспільства (хостинг, застосунки та контент)

• 20. Переконайтеся, що будь-яке фільтрування чи блокування послуг здійснюється законно, пропорційно і прозоро для ваших клієнтів відповідно до Рекомендації Ради Європи № CM/Rec(2008) 6 щодо заходів з розвитку поваги до свободи вираження поглядів та інформації у зв'язку з інтернет-фільтрами. Повідомте своїм клієнтам про будь-яке програмне забезпечення для фільтрації або блокування, встановлене на ваших серверах, що може призвести до видалення або недоступності контенту, а також про характер фільтрації, що здійснюється (про форму фільтрації, загальні критерії, що використовуються для фільтрації, причини застосування фільтрів).

• 21. Фільтрування, блокування або видалення нелегального контенту повинно здійснюватися вами тільки після підтвердження незаконності контенту, наприклад, після звернення до компетентних

правоохоронних органів. Здійснення таких дій без попередньої перевірки та підтвердження може вважатися втручанням у легальний контент і права та свободи тих, хто створює, поширює й отримує доступ до такого контенту, зокрема, у право на свободу вираження поглядів та інформації.

• 22. Повідомте своїм клієнтам про ваш загальний підхід до розгляду скарг на нібито незаконний контент, який ви можете зберігати. Дайте громадськості чіткі вказівки щодо того, як подавати скарги, а вашим клієнтам – як на них реагувати.

• 23. Якщо ви надаєте своїм клієнтам з специфічні програмні послуги, такі як використання чату, електронної пошти, блогів тощо, ви повинні подбати про те, щоб використання застосунків було якомога безпечнішим і щоб ваші клієнти розуміли, яким чином працюють ці застосунки. Надаючи такі послуги, як чат-кімнати або дискусійні форуми, переконайтеся, що було встановлено чіткі правила реєстрації користувачів і використання ніків та що до того, як користувачі почали користуватися вашими послугами, їх було чітко поінформовано про ці правила.

• 24. Хоча ви не повинні надавати консультації щодо того, який контент чи поведінка є незаконними та/або шкідливими, ви могли б надати вчителям і батькам корисну інформацію про загрози для дітей при використанні програмних послуг, що ви надаєте (чат-кімнати, дошки оголошень тощо), зокрема, щодо ризику натрапити на шкідливий контент чи поведінку (грумінг, залякування тощо) під час користування вашими послугами.

• 25 Надаючи вашим клієнтам застосунки для користування електронною поштою, переконайтеся, що будь-які засоби, якими ви їх забезпечуєте, наприклад, програмні засоби для виявлення чи фільтрації спаму, є дієвими (такими, що виявляють або фільтрують спам, не перешкоджаючи законному електронному листуванню), а ваших клієнтів належним чином поінформовано про їх функціональність та методику, а також про можливість змінити їх конфігурацію.

• 26 Якщо ви надаєте вашим клієнтам такі контент-послуги, як інформаційні послуги з використанням мережі Інтернет чи новинні послуги, розгляньте можливість надання користувачам права на відповідь, що дозволить швидко виправляти невірну інформацію відповідно до мінімальних принципів, що містяться в Рекомендації Ради Європи (2004) 16 щодо права на відповідь в умовах нового медіасередовища.

Керівні принципи для ІП щодо права на повагу до приватного життя і захисту даних

• 27. Встановіть належні процедури і використовуйте доступні технології для захисту приватності користувачів, таємниці контенту і даних щодо трафіку, зокрема, шляхом забезпечення цілісності даних, конфіденційності, а також фізичної й логічної безпеки мережі та послуг, які надаються через неї. Відповідно, рівень захисту повинен бути адаптованим до типу послуг, які ви надаєте.

• 28. Надайте вашим клієнтам додаткову інформацію та вказівки щодо технічних засобів, якими вони можуть користуватися, щоб захистити себе від загроз безпеці даних і засобів зв'язку (наприклад, засоби антишпигунського програмного забезпечення, брандмауери, технології шифрування або цифровий підпис тощо).

• 29. Вчинення дій відносно комунікації користувачів (наприклад, надання дозволу на перехоплення або моніторинг їх електронної пошти) повинно здійснюватися лише за наявності правового обов'язку робити це, конкретних наказів або інструкцій компетентного державного органу, виданих в порядку, передбаченому законодавством. Не здійснюйте активний моніторинг змісту комунікації у вашій мережі. Більше того, видалення та внесення змін до кореспонденції користувача (наприклад, з допомогою спам-фільтрів) повинні зумовлюватися наданням користувачем явної згоди до моменту активації спам-фільтра тощо.

• 30. Не розкривайте особистість користувачів, дані щодо їхнього трафіку або зміст даних, доступ до яких вони надали третій стороні, якщо тільки для цього не існує правового обов'язку або компетентний державний орган не видав для цього конкретні накази чи інструкції в порядку, передбаченому законодавством. Запити на вчинення таких дій, які надійшли до вас з-за кордону, повинні розглядатися компетентними органами вашої країни.

• 31. Повідомте своїм клієнтам, за яких обставин ви маєте правовий обов'язок розкривати дані щодо їх особистості, підключення або трафіку на запит правоохоронних органів тощо. Таку інформацію можуть, зокрема, надавати асоціації ІП, до яких ви можете забажати приєднатися. Якщо ви отримуєте запит на розкриття таких даних, обов'язково перевірте автентичність запиту та факт його подання компетентним органом в порядку, передбаченому законодавством.

• 32. Не збирайте, не обробляйте і не зберігайте дані про користувачів, якщо це не є необхідним у явних, визначених і законних цілях, передбачених законодавством у сфері захисту даних. Не зберігайте дані довше, ніж цього вимагає закон чи це необхідно для досягнення мети обробки даних.

• 33. Не використовуйте персональні дані користувачів у власних рекламних або маркетингових цілях, крім випадків, якщо тільки поінформований про ваші наміри користувач не погодився на це і не відкликав свою згоду. Не робіть персональні дані загальнодоступними! Їх оприлюднення може порушити конфіденційність інших осіб, а також може заборонятися законом.

Витяги з існуючих стандартів Ради Європи, що стосуються ролі та обов'язків ІП

Рекомендація № R (99) 5 Комітету міністрів державам-членам щодо захисту недоторканності приватного життя в Інтернеті[1]

Керівні принципи щодо захисту особистості при зборі та обробці персональних даних на інформаційних магістралях, що можуть бути включені чи долучені до кодексів поведінки

III. Постачальникам інтернет-послуг (провайдерам)

1. Використовуйте відповідні процедури і доступні технології, переважно сертифіковані, для захисту приватності відповідних осіб (навіть якщо вони не є користувачами Інтернету), особливо шляхом забезпечення цілісності і конфіденційності, а також фізичної й логічної безпеки мережі та послуг, які надаються через неї.

2. Інформуйте користувачів про загрози, що існують під час користування Інтернетом, до того, як вони підпишуться на послуги або почнуть користуватися ними. Такі загрози можуть бути пов'язані з порушенням цілісності даних, конфіденційності, безпеки мережі чи з іншими загрозами конфіденційності, такими як приховане збирання або записування даних.

3. Інформуйте користувачів про технічні засоби, які вони можуть використовувати на законній підставі для зниження загрози порушення безпеки даних і комунікацій, наприклад, про дозволені законом засоби шифрування і цифровий підпис. Пропонуйте такі технічні засоби за ціною, що базується на затратах, а не за стримуючою ціною.

4. Перед тим, як погодитися на підписку і надати доступ до Інтернету, поінформуйте їх про можливість анонімного доступу до Інтернету, користування його послугами та їх анонімної оплати (наприклад, з допомогою передплачених карток доступу). Через законодавчі обмеження повна анонімність не завжди є можливою. У такому випадку, якщо це дозволяється законом, надавайте користувачам можливість використовувати псевдоніми. Інформуйте користувачів про програмні засоби, які дозволяють анонімно здійснювати пошук і переглядати інформацію в Інтернеті. Проектуйте свою систему таким чином, щоб уникнути чи мінімізувати використання персональних даних.

[1] Прийнята 23 лютого 1999 року.

5. Не читайте, не змінюйте і не видаляйте повідомлення, надіслані іншим особам.

6. Не допускайте жодного втручання у зміст повідомлень, якщо тільки це не передбачено законом і не здійснюється державними органами.

7. Збирайте, обробляйте і зберігайте дані користувачів лише тоді, коли це необхідно в ясних, точно визначених і законних цілях.

8. Не передавайте дані, якщо така передача не передбачена законом.

9. Не зберігайте персональні дані довше, ніж це необхідно для досягнення цілей обробки.

10. Не використовуйте персональні дані у власних рекламних чи маркетингових цілях, якщо тільки поінформований про ваші наміри користувач не висунув заперечення проти цього чи якщо у випадку обробки даних щодо трафіку або чутливих даних він не дав своєї явної згоди.

11. Ви відповідаєте за належне використання даних. Розмістіть на головній сторінці вашого сайту чітку заяву про вашу політику конфіденційності. Ця заява повинна містити гіперпосилання на детальне роз'яснення такої політики. Перш ніж користувач почне користуватися вашими послугами, коли він відвідає ваш сайт чи звернеться до вас із запитанням, повідомте йому про те, ким ви є, які персональні дані ви збираєте, обробляєте і зберігаєте, яким чином ви це робите і з якою метою та як довго ви їх зберігаєте. У разі потреби, запитайте в користувача його згоди. На запит відповідної особи, негайно виправляйте її невірні дані і видаляйте їх, якщо вони є надлишковими, застарілими або більше не потрібні, і припиняйте їх обробку, якщо користувач заперечує проти неї. Повідомляйте третю сторону, якій ви передали дані, про будь-які зміни. Уникайте прихованого збирання даних.

12. Інформація, надана користувачеві, повинна бути точною та актуальною.

13. Двічі подумайте перед тим, як публікувати дані на своєму сайті! Подібна публікація може порушити приватність інших людей, а також може заборонятися законом.

14. Перед тим як передавати дані в іншу країну, проконсультуйтеся, наприклад, з компетентними органами вашої країни щодо того, чи дозволяється така передача. Можливо, вам треба буде попросити приймаючу сторону забезпечити необхідні гарантії захисту даних.

Декларація Комітету міністрів про свободу спілкування в Інтернеті[2]

Принцип 6 – Обмежена відповідальність провайдерів за інтернет-контент

Держави-члени не повинні покладати на провайдерів загальне зобов'язання здійснювати моніторинг контенту в Інтернеті, до якого вони надають доступ, який вони передають або зберігають, а також здійснювати активний пошук фактів чи обставин, що вказують на незаконну діяльність.

Держави-члени повинні забезпечувати, щоб провайдери не притягались до відповідальності за контент в Інтернеті, якщо відповідно до законодавства їх функціональність обмежується передаванням інформації або наданням доступу до мережі Інтернет.

У випадку, коли функції провайдерів є ширшими і вони зберігають контент, що надходить від інших осіб, держави-члени можуть визнати їх співвідповідальними, якщо вони оперативно не вчинять дій для видалення такої інформації чи послуг або унеможливлення доступу до них одразу після того, як їм стане відомо про їх незаконний характер, що передбачено національним законодавством, або у випадку пред'явлення вимог щодо відшкодування, про факти чи обставини, які викривають нелегальність діяльності чи інформації.

Визначаючи в національному законодавстві зобов'язання провайдерів, викладені у попередньому параграфі, потрібно з належною обережністю врахувати питання щодо дотримання свободи вираження поглядів осіб, які першими зробили інформацію доступною, а також відповідних прав користувачів на отримання цієї інформації.

У будь-якому випадку, вищезазначені обмеження відповідальності не повинні негативно впливати на можливість видання судової заборони, яка вимагатиме від провайдерів припинити чи унеможливити, наскільки це можливо, порушення закону.

Витяги з Пояснювальної записки до Декларації про свободу спілкування в Інтернеті

Принцип 6 – Обмежена відповідальність провайдерів за інтернет-контент

Тут встановлено, що посередники в комунікаційному ланцюжку, як правило, не повинні нести відповідальність за контент, який передається з допомогою їх послуг, за винятком певного обмеженого

[2] Прийнята 28 травня 2003 року.

кола обставин. Відповідно до статей 12-15 Директиви про електронну комерцію, при звільненні від відповідальності враховуються різні типи діяльності посередників, а саме: надання доступу до комунікаційних мереж, передачі даних та розміщення (хостинг) інформації. Ступінь відповідальності залежить від можливостей провайдерів контролювати контент та їх поінформованість про його незаконний характер. Обмеження відповідальності не застосовується, якщо посередники навмисно поширюють незаконний контент.

Пункт 1 – Відсутність загального зобов'язання здійснювати моніторинг

Цей пункт заснований на статті 15 Директиви про електронну комерцію. Держави-члени не повинні покладати на провайдерів загальне зобов'язання здійснювати моніторинг контенту в Інтернеті, до якого вони надають доступ, який вони передають або зберігають. На них також не повинно покладатися загальне зобов'язання здійснювати активний пошук фактів чи обставин, що вказують на незаконну діяльність, оскільки це може обмежувати свободу вираження поглядів.

Цей пункт, що містить Принцип 6, не перешкоджає органам влади держав-членів зобов'язувати провайдерів здійснювати моніторинг діяльності своїх клієнтів у деяких випадках, наприклад, під час розслідування кримінальної справи.

Пункт 2 – "Передача інформації"

У випадку простої передачі інформації або надання доступу до комунікаційних мереж посередники не повинні відповідати за незаконний контент. Якщо роль посередників виходить за рамки простої передачі інформації, зокрема, коли вони ініціюють передачу, обирають одержувача цієї передачі, вибирають чи змінюють інформацію, що передається, їх може бути притягнуто до відповідальності.

Діяльність посередника, про яку йде мова і яка має звільнятися від відповідальності, іноді називають "передачею інформації" (порівн. статтю 12 Директиви про електронну комерцію).

Пункт 3 – "Розміщення інформації (хостинг)"

У разі розміщення (хостингу) контенту, що надходить від третіх осіб, посередники в цілому не повинні нести відповідальність (порівн. статтю 14 Директиви про електронну комерцію). Однак це не стосується випадків, коли третя сторона діє під контролем посередника, наприклад, коли компанія, яка видає газету, має

власний сервер для розміщення контенту, створеного її журналістами. Проте якщо було подано позов щодо відшкодування збитків або виявлено факти, що вказують на незаконну діяльність, а хостер знає про незаконний характер контенту, розміщеного на його серверах, його цілком може бути притягнуто до відповідальності. Національне законодавство повинно передбачати чітко умови для цього.

Пункт 4 – Процедури "попередження та видалення" і свобода вираження поглядів та інформації

Як передбачено в пункті 3 Принципу 6 Декларації, провайдерів може бути визнано відповідальними, якщо вони оперативно не вчинять дій для видалення інформації чи послуг або унеможливлення доступу до них одразу після того, як їм стане відомо про їх незаконний характер, що передбачено національним законодавством. Держави-члени мають більш докладно визначати, який рівень знань повинні мати провайдери, перш ніж їх буде притягнуто до відповідальності. У цьому відношенні дуже важливі так звані процедури "попередження та видалення". Держави-члени повинні, однак, проявляти обережність, покладаючи на провайдерів відповідальність за відсутність з їх боку реакції на таке повідомлення. Питання про те, чи є певний матеріал незаконним, є часто складним і найкраще вирішується в судовому порядку. Якщо після отримання скарги провайдери занадто швидко вчиняють дії з видалення контенту, це може бути небезпечно з точки зору свободи вираження поглядів та інформації. Таким чином, цілком законний контент може бути вилучено через страх перед юридичною відповідальністю.

Пункт 5 – Збереження можливості видання судової заборони

Відповідно до статей 12-14 Директиви про електронну комерцію, тут підкреслюється, що незважаючи на вищезазначені обмеження відповідальності зберігається можливість видання судової заборони, яка вимагатиме від провайдерів припинити чи унеможливити, наскільки це можливо, порушення закону.

Декларація Комітету міністрів про права людини та верховенство права в інформаційному суспільстві[3]

Відносно заходів саморегулювання і спільного регулювання, спрямованих на підтримку свободи вираження поглядів та комунікації, представникам приватного сектора рекомендується рішучим чином вирішувати наступні проблеми:

• негласна цензура (прихована цензура) з боку інтернет-провайдерів, наприклад, блокування або видалення контенту з власної ініціативи або на прохання третьої особи;

Рекомендація № Rec (2007) 11 Комітету міністрів державам-членам щодо забезпечення свободи вираження поглядів та інформації у новому інформаційному та комунікаційному середовищі[4]

Державам-членам, приватному сектору і громадянському суспільству рекомендується розробити спільні стандарти і стратегії для забезпечення прозорості й надання інформації, керівництва та допомоги окремим користувачам технологій і послуг, зокрема у таких ситуаціях:

...vii. видалення контенту вважається незаконним з точки зору верховенство права;

Рекомендація № Rec (2007) 16 Комітету міністрів державам-членам щодо заходів з підвищення цінності Інтернету як суспільної послуги[5]

Державам-членам слід прийняти або розробити політику збереження та, наскільки це можливо, посилення захисту прав людини і дотримання верховенства права в інформаційному суспільстві. У зв'язку з цим слід приділити особливу увагу:

• праву на приватне життя і приватну кореспонденцію в Інтернеті та при використанні інших ІКТ, у тому числі повазі до бажання користувачів не розкривати свою особистість, чому сприяє заохочення окремих користувачів, провайдерів інтернет-послуг та контент-провайдерів розділити відповідальність за вирішення цих питань;

[3] Прийнята 13 травня 2005 року.
[4] Прийнята 26 вересня 2007 року.
[5] Прийнята 7 листопада 2007 року.

Державам-членам слід сприяти проведенню публічного обговорення питань щодо обов'язків таких приватних осіб, як провайдери інтернет-послуг, контент-провайдери і користувачі, та заохочувати їх – в інтересах демократичного процесу, дебатів, а також захисту прав інших осіб – вживати саморегуляторних та інших заходів для оптимізації якості і достовірності інформації в Інтернеті та сприяти здійсненню професійної відповідальності, зокрема, щодо створення, дотримання і контролю за дотриманням кодексів поведінки.

Рекомендація № CM/Rec (2008) 6 щодо заходів із забезпечення дотримання свободи вираження поглядів та інформації відносно інтернет-фільтрів

Комітет міністрів, відповідно до положень статті 15 (b) Статуту Ради Європи,

Вважаючи, що метою Ради Європи є досягнення більшої єдності між її членами для збереження та втілення ідеалів та принципів, які є їх спільною спадщиною;

Нагадуючи, що держави-учасниці Конвенції про захист прав людини і основоположних свобод (Європейської конвенції з прав людини, ETS № 5) взяли на себе зобов'язання гарантувати кожному, хто перебуває під їх юрисдикцією, права людини та основні свободи, визначені в Конвенції;

Підтверджуючи відданість держав-членів основоположному праву на свободу вираження поглядів, на одержання і поширення інформації та ідей без втручання органів державної влади і незалежно від державних кордонів, як це гарантується статтею 10 Європейської конвенції з прав людини;

Усвідомлюючи, що будь-яке втручання держав-членів, яке забороняє доступ до конкретного інтернет-контенту, може становити обмеження свободи вираження поглядів та доступу до інформації в онлайн-середовищі, і що таке обмеження повинно відповідати умовам, викладеним у пункті 2 статті 10 Європейської конвенції з прав людини, та відповідній судовій практиці Європейського суду з прав людини;

Згадуючи в цьому зв'язку про Декларацію про права людини і верховенство права в інформаційному суспільстві, прийняту Комітетом міністрів 13 травня 2005 року, згідно з якою держави-члени повинні підтримувати і посилювати правові та практичні заходи для запобігання державній і негласній цензурі;

Згадуючи про Рекомендацію № Rec (2007) 11 Комітету міністрів державам-членам щодо забезпечення свободи вираження поглядів та інформації у новому інформаційному та комунікаційному середовищі, відповідно до якої державам-членам, приватному сектору і громадянському суспільству пропонується розробити спільні стандарти і стратегії для забезпечення прозорості й надання інформації, керівництва і допомоги окремим користувачам технологій та послуг, що стосуються, серед іншого, блокування доступу і фільтрації контенту та послуг стосовно права на отримання та поширення інформації;

Відзначаючи, що добровільне і відповідальне використання інтернет-фільтрів (програм, систем та заходів з блокування або фільтрації інтернет-контенту) може сприяти посиленню конфіденційності та безпеки в Інтернеті для користувачів, особливо дітей та молоді, в той же час усвідомлюючи, що використання таких фільтрів може вплинути на право на свободу вираження поглядів та інформації, що захищається статтею 10 Європейської конвенції з прав людини;

Згадуючи про Рекомендацію № Rec (2006) 12 Комітету міністрів про надання дітям прав у новому інформаційному та комунікаційному середовищі, в якій підкреслюється важливість інформаційної грамотності та навчальних стратегій для дітей, щоб вони могли краще розуміти і поводитися з інтернет-контентом (таким як насильство і самоушкодження, порнографія, дискримінація та расизм) і поведінкою (наприклад, грумінг, залякування, домагання або переслідування), що несуть в собі ризик заподіяння шкоди, тим самим сприяючи посиленню почуття впевненості, благополуччя і поваги до інших осіб у новому інформаційно-комунікаційному середовищі;

Маючи переконання у необхідності забезпечити, щоб користувачі знали, розуміли і могли ефективно використовувати, налаштовувати і контролювати фільтри у відповідності зі своїми індивідуальними потребами;

Згадуючи про Рекомендацію № Rec (2001) 8 Комітету міністрів про саморегулювання відносно кібер-контенту (саморегулювання і захист користувачів від незаконного або шкідливого змісту нових комунікаційних та інформаційних послуг), яка заохочує нейтральне маркування контенту для того, щоб користувачі могли робити власні оціночні судження стосовно такого контенту, а також розвиток великої кількості інструментів пошуку і профілів фільтрації, які дають користувачам можливість вибору контенту на основі вмісту дескрипторів;

Усвідомлюючи суспільну значимість Інтернету, яку можна розуміти як значну залежність людей від Інтернету як основного інструменту в їх повсякденній діяльності (спілкування, інформація, знання, здійснення комерційних трансакцій, розваги), і закономірне очікування того, що інтернет-послуги будуть доступними, прийнятними за ціною, безпечними, надійними і безперервними, а також згадуючи у зв'язку з цим про Рекомендацію № Rec (2007) 16 Комітету міністрів щодо заходів з підвищення цінності Інтернету як суспільної послуги;

Згадуючи про Декларацію Комітету міністрів про свободу спілкування в Інтернеті від 28 травня 2003 року, в якій підкреслюється, що державні органи не повинні за рахунок вжиття заходів з блокування або фільтрації позбавляти громадськість доступу до інформації та інших способів комунікації в Інтернеті, незалежно від державних кордонів, але не заважає встановленню фільтрів для захисту неповнолітніх, зокрема, в таких доступних для них місцях, як школи і бібліотеки;

Підтверджуючи відданість держав-членів праву кожного на приватне життя і таємницю кореспонденції, що захищаються статтею 8 Європейської конвенції з прав людини, і згадуючи про Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108) та Додатковий протокол до неї стосовно органів нагляду і транскордонних потоків даних (ETS № 181), а також Рекомендацію № R (99) 5 Комітету Міністрів про захист недоторканності приватного життя в Інтернеті,

Рекомендує державам-членам прийняти спільні стандарти і стратегії відносно інтернет-фільтрів для сприяння повному здійсненню та реалізації права на свободу вираження поглядів та інформації і пов'язаних з ними прав та свобод, передбачених в Європейській конвенції з прав людини, зокрема, шляхом:

• вжиття заходів відносно інтернет-фільтрів відповідно до керівних принципів, викладених у додатку до цієї рекомендації;

• доведення цих керівних принципів до відома всіх відповідних партнерів з приватного і державного секторів, зокрема тих, які проектують, використовують (встановлюють, активують, дезактивують і реалізують) та контролюють інтернет-фільтри, а також всього громадянського суспільства, з тим, щоб вони могли долучитися до їх виконання.

Додаток до Рекомендації № CM/Rec (2008) 6: Керівні принципи використання інтернет-фільтрів і здійснення контролю за ними для повного здійснення та реалізації права на свободу вираження поглядів та інформації

Поінформованість, розуміння і здатність користувачів ефективно користуватися інтернет-фільтрами є ключовими факторами, які дозволяють їм повною мірою здійснювати і реалізувати свої права людини й основоположні свободи, зокрема, право на свободу вираження поглядів та інформації, а також брати активну участь в демократичних процесах. Коли користувачі стикаються з фільтрами, вони повинні знати про те, що фільтр є активним і, коли це доцільно, мають вміти визначати і контролювати рівень фільтрації контенту, до якого вони мають доступ. Більш того, вони повинні мати можливість оскаржувати блокування або фільтрацію контенту, а також домагатися роз'яснень і засобів правового захисту.

У співпраці з приватним сектором і громадянським суспільством держави-члени повинні забезпечувати, щоб користувачі знали про активовані фільтри і, де це доцільно, могли активувати і дезактивувати їх, а також отримувати допомогу при зміні рівня фільтрації, зокрема, шляхом:

i. розробки та розповсюдження мінімального рівня інформації для користувачів, щоб вони могли визначати, коли було активовано фільтрацію, і розуміти, яким чином та за якими критеріями вона здійснюється (наприклад, чорні списки, білі списки, блокування ключових слів, рейтинг контенту тощо або їх поєднання);

ii. розробки мінімальних рівнів і стандартів щодо інформації, наданої користувачам, для пояснення того, чому конкретний тип контенту було піддано фільтрації;

iii. регулярного перегляду та оновлення фільтрів для підвищення їх ефективності, пропорційності і законності відносно поставленої мети;

iv. надання чіткої та стислої інформації і керівництва щодо ручного коригування активованого фільтру, зокрема, щодо того, до кого можна звернутися, коли видається, що контент блокується безпідставно, а також щодо підстав, які можуть дозволити скоригувати фільтр відносно конкретного типу контенту чи Уніфікованого покажчика ресурсів (URL);

v. забезпечення того, щоб контент, який в результаті помилки або неточності було піддано фільтрації, був доступний без надмірних складнощів і в розумні строки;

vi. просування ініціатив щодо підвищення інформованості про соціальну та етичну відповідальність осіб, які проектують, використовують і контролюють фільтри, зокрема, щодо права на свободу вираження поглядів та інформації, а також на приватне життя та активну участь у громадському житті і демократичних процесах;

vii. підвищення рівня поінформованості про потенційні обмеження свободи вираження поглядів та інформації і права на приватне життя, що виникають внаслідок використання фільтрів, а також про необхідність забезпечити пропорційність таких обмежень;

viii. сприяння обміну досвідом та передовою практикою щодо проектування, використання фільтрів і їх контролю;

ix. заохочення проведення навчальних курсів для мережевих адміністраторів, батьків, викладачів та інших осіб, які використовують і контролюють фільтри;

x. просування та співпраці з існуючими ініціативами щодо забезпечення відповідального використання фільтрів відповідно до прав людини, демократії і верховенства права;

xi. забезпечення стандартів і орієнтирів, які допоможуть користувачам вибрати фільтри та якнайкраще їх контролювати.

У цьому контексті необхідно заохочувати громадянське суспільство підвищувати рівень поінформованості користувачів про потенційні переваги і небезпеки фільтрів. Сюди має увійти заохочення розгляду питання щодо важливості і значення вільного та безперешкодного доступу до Інтернету, щоб кожна людина могла повною мірою здійснювати і реалізувати свої права людини та основоположні свободи, зокрема, право на свободу вираження поглядів та інформації, право на приватне життя, а також на ефективну участь у суспільному житті і демократичних процесах.

Належне фільтрування для дітей та молоді

Інтернет значно підвищив обсяг і різноманіття ідей, інформації та поглядів, які люди можуть отримувати і поширювати при здійсненні свого права на свободу вираження поглядів та інформації, без якого-небудь втручання з боку державної влади і незалежно від державних кордонів.

У той же час це збільшило обсяг легкодоступного контенту, що несе в собі загрозу заподіяння шкоди, особливо дітям та молоді. Для задоволення законного бажання та обов'язку держав-членів захищати дітей і молодь від контенту, що несе в собі загрозу заподіяння шкоди, пропорційне використання фільтрів може стати

доцільним засобом заохочення доступу до Інтернету і його впевненого використання, а також доповнити інші стратегії щодо того, як поводитися зі шкідливим контентом, наприклад, шляхом розвитку та забезпечення інформаційної грамотності.

У зв'язку з цим держави-члени повинні:

i. сприяти розробці стратегій з виявлення контенту, що несе в собі загрозу заподіяння шкоди дітям та молоді, враховуючи при цьому розмаїття культур, цінностей та поглядів;

ii. співпрацювати з приватним сектором і громадянським суспільством для того, щоб уникати надмірної опіки над дітьми та молоддю шляхом, серед іншого, надання підтримки у проведенні досліджень та розробок для вироблення "розумних" фільтрів, які більшою мірою враховують контекст, у якому надається інформація (наприклад, розрізняючи сам шкідливий контент і посилання на нього, які не викликають проблем, як це може мати місце на наукових веб-сайтах);

iii. сприяти і заохочувати ініціативи, які надають допомогу батькам і вихователям у виборі та використанні для дітей та молоді відповідних фільтрів, що враховують віковий розвиток;

iv. інформувати дітей та молодь про переваги та небезпеки інтернет-контенту і його фільтрації в рамках стратегій медіаосвіти в процесі отримання ними формальної та неформальної освіти.

Крім того, приватний сектор необхідно заохочувати:

i. розробляти "розумні" фільтри для здійснення фільтрації з урахуванням вікового розвитку, які можна буде пристосовувати до розвитку та віку дітей, одночасно забезпечуючи, щоб фільтрація не проводилася у випадках, коли контент вважається ані шкідливим, ані невідповідним для групи, для захисту якої цей фільтр був активований;

ii. співпрацювати з органами саморегулювання та спільного регулювання для розробки стандартів відповідних рейтингових систем з вікового розвитку стосовно контенту, що несе в собі загрозу заподіяння шкоди, враховуючи розмаїття культур, цінностей та поглядів;

iii. розробляти у співпраці з громадянським суспільством спільні мітки для фільтрів, щоб допомогти батькам і вихователям у здійсненні поінформованого вибору при придбанні фільтрів і підтвердити, що вони відповідають певним критеріям якості;

iv. забезпечувати сумісність систем для самостійної класифікації контенту провайдерами і надання допомоги у підвищенні рівня поінформованості про потенційні переваги та небезпеки таких моделей класифікацій.

Крім того, слід заохочувати громадянське суспільство:

i. обговорювати й обмінюватися своїм досвідом та знаннями при оцінці та підвищенні рівня інформованості щодо розробки та використання фільтрів у якості запобіжного захисту для дітей та молоді;

ii. регулярно проводити моніторинг та аналіз використання і впливу фільтрів на дітей і молодь, зокрема, з огляду на їх ефективність та внесок у здійснення і реалізацію прав і свобод, гарантованих статтею 10 та іншими положеннями Європейської конвенції з прав людини.

Використання та застосування інтернет-фільтрів у державному та приватному секторах

Незважаючи на важливість надання користувачам права на використання фільтрів та здійснення контролю за ними, про що говорилося вище, і відзначаючи зростання цінності Інтернету в якості суспільної послуги державні структури усіх рівнів (наприклад, адміністративні органи, бібліотеки та освітні установи), які встановлюють фільтри або використовують їх при наданні послуг суспільству, повинні забезпечувати повне дотримання прав усіх користувачів на свободу вираження поглядів та інформації, а також їх права на приватне життя і таємницю кореспонденції.

В цьому контексті держави-члени повинні:

i. утримуватися від фільтрації інтернет-контенту в електронних комунікаційних мережах, що регулюються державними органами, з інших підстав, ніж ті, що викладені в пункті 2 статті 10 Європейської конвенції з прав людини у тлумаченні Європейського суду з прав людини;

ii. гарантувати, щоб загальнодержавні загальні заходи з блокування або фільтрації впроваджувалися державою тільки з виконанням умов, передбачених пунктом 2 статті 10 Європейської конвенції з прав людини. Такі дії з боку держави повинні здійснюватися тільки в тому випадку, якщо фільтрація стосується конкретного і чітко визначеного контенту, якщо компетентний національний орган влади прийняв рішення про його незаконність і якщо рішення може бути розглянуто незалежним і неупередженим судом або

регулятивним органом відповідно до вимог статті 6 Європейської конвенції з прав людини;

iii. приймати, коли це доцільно і необхідно, положення в рамках національного законодавства про попередження навмисного зловживання фільтрами для обмеження доступу громадян до законного контенту;

iv. гарантувати, щоб усі фільтри проходили оцінювання як до, так і під час їх використання для забезпечення того, щоб результати фільтрування були пропорційними до мети обмеження, а тому й необхідними в демократичному суспільстві, для уникнення безпідставного блокування контенту;

v. забезпечувати ефективні й легкодоступні засоби правового та судового захисту, в тому числі призупинення дії фільтрів у випадках, коли користувачі та/або автори контенту заявляють, що контент був безпідставно заблокований;

vi. уникати універсального і загального блокування образливого чи шкідливого контенту для користувачів, які не є частиною групи, для захисту якої був активований фільтр, або незаконного контенту для користувачів, які обґрунтовано демонструють законний інтерес або мають необхідність у доступі до такого контенту за виняткових обставин, зокрема, у цілях проведення наукових досліджень;

vii. гарантувати, щоб при використанні і застосування фільтрів дотримувалося право на приватне життя і таємницю кореспонденції та щоб персональні дані, які вносяться, реєструються і обробляються через фільтри, використовувалися тільки для законних і некомерційних цілей.

Крім того, державам-членам і приватному сектору рекомендується:

i. регулярно оцінювати і переглядати ефективність і пропорційність впровадження фільтрів;

ii. розширювати інформацію і рекомендації для користувачів, щодо яких застосовуються фільтри в приватних мережах, в тому числі надаючи їм інформацію про наявність та підстави використання фільтра і критеріїв, відповідно до яких діє цей фільтр;

iii. співпрацювати з користувачами (клієнтами, співробітниками тощо) для підвищення рівня прозорості, ефективності та пропорційності дії фільтрів.

У цьому контексті слід заохочувати громадянське суспільство продовжувати розробку та розміщення фільтрів як з боку ключових державних органів, так і приватного сектору. Коли це доцільно,

громадянському суспільству слід закликати держави-члени і, відповідно, приватний сектор забезпечувати і сприяти дотриманню права всіх користувачів на свободу вираження поглядів та інформації, зокрема, в питанні свободи одержувати і поширювати інформацію без будь-якого втручання з боку державної влади і незалежно від державних кордонів у новому інформаційно-комунікаційному середовищі.

Розроблені Радою Європи у тісній співпраці з Європейською асоціацією інтернет- провайдерів (EuroISPA), ці керівні принципи надають контрольні показники у сфері прав людини для інтернет-провайдерів (ІП). Підкреслюючи важливу роль, яку ІП відіграють у наданні користувачам Інтернету таких основних послуг, як доступ, електронна пошта чи контент-послуги, вони наголошують на важливості безпеки користувачів та їх права на приватність і свободу вираження поглядів, а також, у зв'язку з цим, на важливості усвідомлення провайдерами можливого впливу своєї діяльності на права людини.

Для отримання додаткової інформації про діяльність
Ради Європи й асоціації EuroISPA
перейдіть за посиланнями:
www.coe.int • www.euroispa.org

Генеральний директорат
з прав людини і правових питань
Рада Європи
F-67075 Strasbourg Cedex