COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Рекомендація CM/Rec(2014)6

Комітету міністрів Ради Європи державам-членам щодо використання Посібника з прав людин користувачів

(ухвалена Комітетом міністрів 16 квітня 2014 року на 1197-му засіданні постійних представників м

1. Держави-члени Ради Європи зобов'язані забезпечити кожному, хто знаходиться в межах їхньої юри основоположні свободи, закріплені Європейською конвенцією про захист прав людини (СЕД № 5, Ко зобов'язання поширюється й на сферу використання мережі Інтернет. Ці питання врегульовано також конвенціями та документами Ради Європи, якими передбачено захист права на свободу вираження по інформації, права на свободу зібрань, захист від кіберзлочинності, а також захист права на приватне ж персональних даних.

2. До зобов'язань держав поважати, захищати та підтримувати права людини належить і контроль за д компаніями. Права людини, які є універсальними та неподільними, а також пов'язані з ними стандарт силу перед загальними вимогами та умовами, що висуваються до Інтернет-користувачів будь-якими с приватного сектора.

3. Інтернет має цінність як суспільна служба. Люди, спільноти, органи державної влади та приватні ко свою діяльність через Інтернет і законно сподіваються на те, що матимуть доступ до Інтернет-послуг, надаватися без будь-якої дискримінації, за розумну ціну, а також будуть безпечними, надійними та бе того, ніхто не повинен підлягати неправомірному, самовільному або безпідставному втручанню в реал основоположних свобод при користуванні Інтернетом.

4. Користувачі повинні отримувати підтримку для розуміння ними та ефективної реалізації прав люди обмеження або порушення їхніх прав та свобод. Така підтримка повинна передбачати інформування п ефективних засобів правового захисту. Зважаючи на можливості, які надає Інтернет для забезпечення підзвітності в управлінні державними справами, користувачі повинні мати можливість використовува участі в демократичному житті.

5. Із метою забезпечення однакового дотримання прав людини та основоположних свобод в офлайні т міністрів згідно з вимогами статті 15.*b* Статуту Ради Європи рекомендує своїм державам-членам таке

5.1. активно поширювати Посібник із прав людини для Інтернет-користувачів, як це передбачено в До громадян, органів державної влади, суб'єктів приватного сектора та здійснювати конкретні заходи, сп застосування, з метою забезпечення реалізації користувачами в повному обсязі своїх прав і основопол Інтернеті;

5.2. здійснювати оцінку, періодично переглядати та при необхідності знімати обмеження щодо реаліз Інтернеті, зокрема у тих випадках, коли вони не відповідають вимогам Конвенції та практиці її застос Європейським судом з прав людини. Будь-яке обмеження повинно бути передбачене законом, бути не демократичному суспільстві, мати законну мету, а також бути пропорційним бажаній меті;

5.3. забезпечувати доступ Інтернет-користувачів до ефективних засобів правового захисту у разі обме

свобод або коли вони вважають, що їхні права були порушені. Це потребує поглиблення координації
відповідними установами, організаціями та спільнотами. Це також передбачає залучення та ефективн
суб'єктами приватного сектора та організаціями громадянського суспільства. Залежно від держави мо
механізми відшкодування, забезпечені органами захисту даних, національними правозахисними орга
омбудсменами), а також через застосування судових процедур та гарячих ліній;

5.4. розвивати співпрацю з іншими державними і недержавними структурами всередині Ради Європи
щодо стандартів і процедур, які мають вплив на захист прав людини й основоположних свобод в Інте

5.5. заохочувати приватний сектор до повноцінного діалогу з відповідними органами державної влади
суспільством із питань їхньої корпоративної соціальної відповідальності, зокрема, прозорості та підзв
діяльності згідно з вимогами «Керівних принципів підприємницької діяльності в аспекті прав людини
ООН «Захист, повага і засоби правового захисту». Приватний сектор потрібно заохочувати до сприян
Посібника;

5.6. заохочувати громадянське суспільство до підтримки поширення і застосування Посібника таким
стало ефективним інструментом для Інтернет-користувачів.

Додаток до Рекомендації CM/Rec(2014)6

Вступ

1. Цей Посібник є інструментом, призначеним для вас, Інтернет-користувачі, з метою ознайомлення в
правами в Інтернеті, їх можливими обмеженнями та доступними засобами правового захисту у випад
Права людини та основоположні свободи повинні однаковою мірою забезпечуватися в офлайні та онл
передбачає повагу до прав і свобод інших Інтернет-користувачів. Посібник надає вам інформацію про
означають права і свободи в контексті використання Інтернету, як ними користуватися, діяти відповід
як отримати доступ до засобів правового захисту. Робота над цим документом не припиняється; він за
відкритим для періодичного оновлення.

2. В основу цього Посібника покладено Європейську конвенцію про захист прав людини, а також інш
документи Ради Європи, в яких розглянуто різні аспекти захисту прав людини. Всі держави-члени Ра
зобов'язані поважати, захищати і забезпечувати дотримання прав і свобод, закріплених у ратифікован
документах. У Посібнику також враховано безперервне тлумачення цих прав і свобод Європейським
та у відповідних правових документах Ради Європи.

3. Посібник не запроваджує нові права та основоположні свободи. У ньому розглянуто чинні стандар
механізми їх забезпечення[1].

Доступ і недискримінація

1. Доступ до Інтернету – це важливий засіб для реалізації вами своїх прав, свобод та участі в демокра
позбавити вас доступу до Інтернету проти вашої волі можуть лише за рішенням суду. В окремих випа
може також припинятися за умовами договору, але це має відбуватися лише після того, як були вичер

2. Ваш доступ має надаватися за розумну ціну і бути недискримінаційним. Ви повинні мати якомога ш
Інтернет-контенту, додатків і послуг, при цьому користуючись будь-якими пристроями на ваш вибір.

3. Вам варто очікувати від органів державної влади розумних зусиль і конкретних заходів, спрямован
вашому доступу до Інтернету, якщо ви проживаєте у сільській місцевості та географічно віддалених р

якщо ви належите до малозабезпечених верств населення та (або) осіб з особливими потребами чи інв

4. При взаємодії з органами державної влади, провайдерами мережі Інтернет та провайдерами Інтерне послуг, а також з іншими користувачами або групами користувачів ви не можете бути об'єктом дискр якими ознаками, такими як стать, раса, колір шкіри, мова, релігія або віра, політичні чи інші перекона або соціальне походження, належність до національної меншини, майновий стан, походження чи будь зокрема, за етнічною приналежністю, віком або сексуальною орієнтацією.

Свобода вираження поглядів та інформації

Ви маєте право шукати, отримувати та поширювати інформацію та ідеї на ваш вибір без будь-якого в незалежно від державних кордонів. Це означає, що:

1. ви можете вільно висловлюватися в Інтернеті та мати доступ до інформації, поглядів і висловлюван належать як політичні заяви, релігійні переконання, погляди і висловлювання, що сприймаються прих вважаються необразливими чи нейтральними, так і такі, що можуть завдавати образу, шокувати або в зі стану душевної рівноваги. Ви повинні приділяти належну увагу репутації та правам інших осіб, зок на приватне життя;

2. обмеження можуть накладатися на такі висловлювання, в яких містяться заклики до дискримінації, насильства. Такі обмеження повинні бути правомірними, цілеспрямованими і запроваджуватися під к

3. ви можете вільно створювати, повторно використовувати і поширювати Інтернет-контент із поваго інтелектуальної власності та авторського права;

4. органи державної влади зобов'язані поважати і захищати вашу свободу вираження поглядів та своб Будь-які обмеження цієї свободи не повинні бути безпідставними та мають переслідувати законну ме Європейської конвенції про захист прав людини таку як, зокрема, захист національної безпеки або гро охорона здоров'я населення чи моралі, а також відповідати законодавству у сфері прав людини. Крім бути ознайомлені з такими обмеженнями, а також проінформовані про те, як отримати консультації та та тривалість цих обмежень не повинні перевищувати межі, необхідні для досягнення законної мети;

5. ваш Інтернет-провайдер та провайдер Інтернет-контенту і послуг мають корпоративні зобов'язання права та забезпечувати механізми розгляду ваших скарг. Водночас ви маєте знати, що провайдери Інт соціальні мережі, можуть обмежувати окремі види контенту і поведінки у зв'язку з їхньою політикою повинні повідомляти про можливі обмеження для того, щоб ви могли прийняти свідоме рішення щодо користуватися такою послугою. Це передбачає надання конкретної інформації про те, що саме провай послуги вважає незаконним чи неналежним контентом і поведінкою при користуванні послугою, а так реагування провайдера;

6. ви можете вирішити не розкривати свою особу в Інтернеті, наприклад, скористатися псевдонімом. С знати, що органи державної влади можуть вдатися до заходів, завдяки яким вашу особу буде розкрито

Зібрання, об'єднання та участь

Ви маєте право на мирні зібрання та об'єднання з іншими особами в Інтернеті. На практиці це означає

1. ви можете вільно обирати будь-який сайт, додаток чи будь-яку іншу послугу з метою створення гру мобілізації та участі в будь-якій соціальній групі та об'єднанні незалежно від їхнього офіційного визн державної влади. Ви також повинні мати можливість використовувати Інтернет для реалізації свого п

профспілок та приєднання до них;

2. ви маєте право на мирний протест в Інтернеті. Однак ви повинні знати: якщо ваш онлайн-протест п
блокування, перебоїв у наданні послуг та (або) завдасть шкоди майну інших осіб, ви можете зіткнути
наслідками;

3. ви можете вільно користуватися доступними онлайновими можливостями для участі в місцевих, на
глобальних публічних політичних дебатах, законодавчих ініціативах, контролі за прийняттям рішень,
право підписувати петиції та брати участь в розробці політики, пов'язаної з управлінням Інтернетом.

Приватне життя і захист даних

Ви маєте право на приватне та сімейне життя в Інтернеті, куди входить захист ваших персональних да
конфіденційності вашої кореспонденції і спілкування. Це означає, що:

1. вам потрібно знати, що при користуванні Інтернетом ваші персональні дані регулярно обробляють
при використанні вами браузерів, електронної пошти, миттєвих повідомлень, передачі голосових пові
Інтернет-протоколи, соціальних мереж, пошукових систем, а також хмарних сервісів для зберігання д

2. при обробці ваших персональних даних органи державної влади і приватні компанії зобов'язані дот
правил та процедур;

3. ваші персональні дані повинні оброблятися лише у передбачених законом випадках або за умови на
Вам повинні повідомляти про те, які саме ваші персональні дані обробляються та (або) передаються т
також про те, коли, ким та з якою метою здійснюється така обробка. В цілому ви повинні мати можли
контроль за своїми персональними даними (перевіряти їх правильність, звертатися з проханням про в
видалення персональних даних або про їх зберігання лише протягом необхідного строку);

4. на вас не повинні поширюватися заходи загального спостереження чи перехоплення інформації. Вт
приватне життя щодо ваших персональних даних дозволяється лише за виняткових обставин, передба
наприклад, у разі здійснення кримінального розслідування. Вам повинна надаватися доступна, чітка т
про відповідне законодавство чи порядок, а також про ваші права в такому випадку;

5. ваше приватне життя має поважатися і на робочому місці. Це передбачає конфіденційність вашої пр
кореспонденції та спілкування. Ваш роботодавець повинен повідомляти вас про будь-які заходи спост
моніторингу;

6. вам можуть надавати допомогу органи захисту даних, які функціонують у більшості європейських
забезпечують дотримання законів та принципів захисту даних.

Освіта і грамотність

Ви маєте право на освіту, зокрема й право на доступ до знань. Це означає, що:

1. ви повинні мати онлайн-доступ до освітнього, культурного, наукового, навчального та іншого конт
мовою. Умови такого доступу можуть передбачати винагороду правовласників за їхню роботу. Ви так
можливість вільного доступу до наукових і культурних здобутків у Інтернеті, що фінансуються держа
відкритому доступі в Інтернеті, де це можливо;

2. у частині Інтернет- і медіаграмотності ви повинні мати доступ до інтерактивної освіти і знань для т

користуватися своїми правами та свободами в Інтернеті. Сюди входять уміння, необхідні для розумін
роботи з широким спектром інструментів Інтернету. Це має навчити вас критично оцінювати точність
контенту, додатків та послуг, до яких ви маєте чи бажаєте мати доступ.

Діти і молодь

Будучи дитиною чи молодою людиною, ви маєте всі права і свободи, викладені в цьому Посібнику. Зо
урахуванням вашого віку ви маєте право на особливий захист і консультування при користуванні Інте
що:

1. ви маєте право на вільне вираження своїх поглядів та участь у житті суспільства, на те, щоб бути по
свій вклад у вирішення питань, які торкаються ваших інтересів. Вашим поглядам повинна приділятис
урахуванням вашого віку, ступеня зрілості та без дискримінації;

2. ви можете очікувати на отримання інформації мовою, що відповідає вашому віку, а також на навча
користуванню Інтернетом, в тому числі щодо захисту вашого приватного життя, з боку ваших вчител
батьків чи опікунів;

3. ви повинні знати, що контент, який ви створюєте в Інтернеті, або контент про вас, що створюється
користувачами, може ставати доступним у будь-якому куточку світу і завдавати шкоду вашій гідност
приватному життю або іншим чином шкодити вам та вашим правам у цей час або на наступних етапа
ваш запит такий контент повинен бути вилучений або видалений протягом розумно короткого періоду

4. ви можете очікувати на отримання чіткої інформації про те, який онлайн-контент та поведінка є нез
(наприклад, домагання в Інтернеті), а також мати можливість повідомити про потенційно незаконний
інформація має бути адаптована до вашого віку та обставин, а також вам повинні надати поради та під
повагою до вашої конфіденційності та анонімності;

5. вам повинен надаватися спеціальний захист від втручання у ваше фізичне, психічне та моральне бл
захист від сексуальної експлуатації та насильства в Інтернеті та від інших форм кіберзлочинності. Кр
право на освіту, яке покликане захистити вас від подібних загроз.

Ефективні засоби правового захисту

1. Ви маєте право на ефективний засіб правового захисту у разі обмеження або порушення ваших пра
свобод. Для отримання правового захисту ви не обов'язково маєте одразу вдаватися до судових засоб
звернення по правовий захист повинні бути доступними, відомими, надаватися за прийнятною ціною
забезпечити належне відшкодування. Ефективні засоби правового захисту можна отримати безпосере
провайдерів, органів державної влади та (або) національних правозахисних органів. Залежно від пору
засобом правового захисту може бути розслідування, роз'яснення, відповідь, виправлення, вибачення
відновлення доступу та компенсація. На практиці це означає, що:

1.1. ваш Інтернет-провайдер, провайдери доступу до Інтернет-контенту чи послуг або інша компанія
державної влади повинні повідомити вас про ваші права, свободи, можливі засоби правового захисту
отримання. Таке зобов'язання передбачає забезпечення вас легкодоступною інформацією про порядо
втручання у ваші права, звернення з відповідною скаргою та відшкодування завданої шкоди;

1.2. додаткова інформація та рекомендації повинні надаватися органами державної влади, національн
органами (наприклад, омбудсменами), органами захисту даних, громадськими консультативними орга

правозахисними асоціаціями чи асоціаціями цифрових прав або організаціями споживачів;

1.3. органи державної влади зобов'язані захищати вас від кримінальної діяльності або кримінальних з
вчиняються в Інтернеті або з використанням Інтернету, зокрема коли це стосується незаконного досту
підробки або інших шахрайських маніпуляцій із вашими електронними персональними даними, комп
які в ньому зберігаються. Відповідні правоохоронні органи зобов'язані розслідувати ці факти та вжив
що передбачають застосування санкцій у разі отримання від вас скарги про завдання шкоди або втруч
персональні дані та ваше майно в Інтернеті.

2. При встановленні ваших прав та обов'язків або під час розгляду будь-якого кримінального обвинув
що стосуються Інтернету:

2.1. ви маєте право на справедливий судовий розгляд протягом розумного строку незалежним та неуп

2.2. ви маєте право на індивідуальну скаргу до Європейського суду з прав людини після вичерпання в
національних засобів правового захисту.

Постійні представники міністрів

Документи КМ

CM(2014)31 addfinal 16 квітня 2014 р.[2]

1197-е засідання, 16 квітня 2014 року

5 ЗМІ

5.1 Керівний комітет із питань ЗМІ та інформаційного суспільства
(CDMSI)

б. Рекомендація CM/Rec(2014)6 Комітету міністрів державам-членам щодо використання Посібника з
Інтернет-користувачів – Пояснювальний меморандум

Вступ

1. Інтернет відіграє важливу роль у повсякденному житті людей та у всіх аспектах життя суспільства.
розвивається і забезпечує громадянам можливість доступу до інформації та послуг, зв'язку та спілкув
думками та знаннями на глобальному рівні. Крім того, зростає вплив Інтернету на соціальну, економі
сфери діяльності.

2. Європейський суд з прав людини (надалі – «**Суд**»)[3] розглядає дедалі більше справ, пов'язаних з Інт
заявляє, що «наразі Інтернет став одним із основних засобів реалізації громадянами свого права на св
поглядів та інформації, забезпечуючи їх таким чином необхідними механізмами для участі в діяльнос
політичних питань та питань, що становлять загальний інтерес»[4].

3. У Стратегії Ради Європи щодо управління Інтернетом на 2012-2015 рр. велике значення надається к
користувачів. У главі «Максимальне забезпечення прав і свобод Інтернет-користувачів», спрямованій
доступу до Інтернету та його найоптимальніше використання, у якості напрямку діяльності зазначено
зведення існуючих прав людини для Інтернет-користувачів з метою допомоги їм у здійсненні комунік
ефективного доступу до основних суб'єктів у Інтернеті та до державних установ у тих випадках, коли
їхнім правам і свободам було завдано шкоди – для того щоб повідомити про такий випадок, подати ск
право на відповідь, компенсацію чи будь-яку іншу форму оскарження».

Історія і контекст

4. Керівний комітет із питань ЗМІ та інформаційного суспільства (CDMSI) на своєму першому засідан
року запропонував Комітету міністрів створити Комітет експертів із прав Інтернет-користувачів (MSI
сферу компетенції цього Комітету. За пропозицією CDMSI Комітет міністрів затвердив повноваження
му засіданні постійних представників міністрів, що відбулося 6 липня 2012 року[5]. Відповідно до повн
MSI-DUI, від нього очікують такі результати:

*«Підготовка зведення існуючих прав людини для Інтернет-користувачів із метою допомогти їм зроз
застосовувати свої права у тих випадках, коли вони, вважаючи, що їхнім правам і свободам було зав
вступають у контакт та намагаються отримати ефективну реакцію від основних суб'єктів у Інтер
установ (2013 р.)» (надалі – «**Зведення**»).*

5. Комітет експертів MSI-DUI провів своє перше засідання 13-14 вересня 2012 року у Страсбурзі. Бул
завданням MSI-DUI повинно бути не створення нових прав людини, а дослідження можливості застос
існуючих прав до Інтернету. MSI-DUI вирішив зібрати інформацію про проблеми, що виникають у ко
про можливі порушення їхніх прав та наявні засоби правового захисту шляхом розсилки анкети у мер

6. На форумі з управління Інтернетом (6-9 листопада 2012 року, Баку) під час семінару на тему «Розш
можливостей Інтернет-користувачів – за допомогою яких інструментів?» було проведено консультаці
сторонами. Учасники форуму від MSI-DUI скористалися можливістю поспілкуватися з широкою ауди
заході, щоб дізнатися думку учасників щодо різноманітних питань, пов'язаних зі Зведенням. Під час с
семінарі з'ясувалися проблеми, що постають перед Інтернет-користувачами, зокрема, видалення конт
користувачами, без належного судового розгляду, питання, пов'язані з захистом персональних даних,
ефективних засобів правового захисту.

7. MSI-DUI провів своє друге засідання 13-14 грудня 2012 року в Страсбурзі. Було розглянуто відпові
учасниками на анкету, а також обговорено інформацію, отриману за результатами спілкування з зацік
сторонами. Комітет MSI-DUI вирішив на цьому завершити попередній етап своєї роботи та почати пр
Зведенням; перший проект було представлено вже на цьому засіданні.

8. На своєму третьому засіданні, що відбулося 20-21 березня 2013 року в Страсбурзі, Комітет MSI-DU
розглянув питання, пов'язані з правом на свободу вираження поглядів, правом на приватне життя, сво
об'єднань, онлайн-безпеку, правом на освіту, правами дітей, недискримінацією та правом на ефектив
захисту. Обговорення питань ґрунтувалося на відповідних обов'язкових і необов'язкових стандартах
прецедентному праві Суду. Комітет MSI-DUI також розглянув питання щодо того, який документ міг
Радою Європи на підтримку Зведення, наприклад, декларація чи рекомендація Комітету міністрів. Та
повинен виконувати подвійне завдання: надавати Інтернет-користувачам прості та чіткі рекомендації
онлайн, а також забезпечувати прийняття державами-членами такого документу, що відповідав би їх
Європейською конвенцією про захист прав людини (ЄКПЛ) та іншим стандартам Ради Європи.

9. На своєму третьому засіданні 23-26 квітня 2013 року в Страсбурзі CDMSI заявив, що Зведення пов

офіційну та зрозумілу мову, але при цьому потрібно уникати надмірного спрощення чинних стандарт
практики Суду у сфері прав людини. У ході обговорення було також підкреслено бажаність регулярно
Зведення з метою відображення політики у сфері Інтернету, що постійно змінюється. Для того щоб зр
спрямованість Зведення, Керівний комітет CDMSI вирішив також надати коментарі до проекту Зведен
момент консультацій), зазначивши при цьому, що документ «перебуває на стадії розробки». Отриман
підтвердили підхід Комітету MSI-DUI при підготовці зручного для користувача інформаційного доку
особливу увагу приділено праву на свободу вираження поглядів, на приватне життя, освіту, правам ді
кіберзлочинності.

10. Проект Зведення був презентований до обговорення зацікавленим сторонам під час Європейського
управління Інтернетом (EuroDIG, 20-21 червня 2013 року в Лісабоні), зокрема, на семінарі «На шляху
Інтернету? Правила, права та відповідальність для нашого майбутнього онлайн». Учасники семінару
DUI провели неформальну зустріч у Лісабоні. Була висловлена думка про те, що проект Зведення вар
його більшої доступності Інтернет-користувачам. За результатами цих обговорень та роботи членів К
між сесіями 10 вересня 2013 року в Страсбурзі було проведено спеціальне засідання для тих членів К
змогли взяти у ньому участь. На цій зустрічі було розглянуто проект рекомендації Комітету міністрів
користувачів, який містив у додатку проект Зведення прав людини та основоположних свобод для Інт
У проекті Зведення автори звертаються безпосередньо до користувача. У зв'язку з таким підходом бу
перейменувати Зведення на Посібник із прав людини для Інтернет-користувачів.

11. На своєму останньому засіданні, що відбулося 1-2 жовтня 2013 року в Страсбурзі, Комітет MSI-D
остаточно затвердив свої пропозиції для Комітету CDMSI стосовно проекту рекомендації Комітету мі
використання Посібника з прав людини для Інтернет-користувачів (надалі – «**Посібник**»). Було вирі
багатосторонні консультації, в тому числі з Відкритим форумом Ради Європи, щодо цього Посібника
управління Інтернетом (22-25 жовтня 2013 року, Індонезія). До ряду відібраних учасників від приват
громадянського суспільства, технічної та наукової спільнот звернулися з проханням про надання коме
пропозицій щодо використання Посібника. Крім того, було запропоновано надати неофіційні комента
проекту рекомендації й іншим відповідним керівним комітетам Ради Європи, у тому числі Керівному
людини (CDDH), Європейському комітету з питань правового співробітництва (CDCJ), Європейськом
проблем злочинності (CDPC), а також комітетам, пов'язаним із договорами, включно з Консультатив
питань Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (T-PD),
кіберзлочинності (T-CY), Комітетом експертів із проблем тероризму (CODEXTER) та Комітетом стор
Конвенції про захист дітей від сексуальної експлуатації та сексуального насильства (T-ES). У відпові
CDCJ та члени Бюро T-PD надали свої коментарі, які були враховані та увійшли до проекту Рекоменд
Пояснювального меморандуму, підготовлених CDMSI.

12. Крім того, близько 30 відгуків надійшло від представників приватного сектора (телекомунікаційн
провайдерів мережі Інтернет), ключових організацій громадянського суспільства, технічної та науков
куточків світу. Вони загалом схвально оцінювали роботу Ради Європи над проектом Посібника та над
коментарів і пропозицій до нього.

13. На своєму четвертому засіданні 3-6 грудня 2013 року Керівний комітет CDMSI розглянув пропози
стосовно проекту рекомендації Комітету міністрів щодо використання Посібника з прав людини для І
користувачів. Було враховано результати консультацій із зазначеними вище зацікавленими сторонами
затверджено проект рекомендації на основі фінальних коментарів, надісланих електронною поштою.

**Коментарі до Рекомендації CM/Rec(2014)6 Комітету міністрів державам-членам щодо використа
прав людини для Інтернет-користувачів**

14. Мета цієї Рекомендації полягає в сприянні реалізації та захисту прав людини й основоположних с

всіх державах-членах Ради Європи. Доступ окремих осіб та спільнот до Інтернету і найоптимальніше потребують їхнього інформування та розширення можливостей для реалізації ними своїх права і своб підхід був підтверджений Комітетом міністрів у Декларації про принципи управління Інтернетом 201 підкреслив своє бачення Інтернету, орієнтованого на людину і побудованого на засадах поваги до пра підвищення потенціалу Інтернет-користувачів у реалізації ними своїх прав і свобод в Інтернеті як при Інтернетом.

15. Посібник, що додається до цієї Рекомендації, надає певну базову інформацію щодо окремих прав у ЄКПЛ та інших відповідних стандартах Ради Європи. Цей документ зосереджує увагу на конкретни та пов'язаних із ними нормах міжнародного права, зокрема, праві на свободу вираження поглядів, сво об'єднань, праві на приватне життя і захист персональних даних, правах дитини, а також праві на ефе правового захисту. Посібник написаний зрозумілою для користувачів мовою. З метою максимального Комітет MSI-DUI вирішив не посилатися на суто юридичні формулювання зобов'язань держав-членів правом, у тому числі й на прецедентне право Суду.

16. Права людини та основоположні свободи гарантовано різними документами Ради Європи, дія яки простір офлайн, так і на онлайн, тобто і на Інтернет також. Зокрема, права людини та основоположні ЄКПЛ, яка тлумачиться Судом у його прецедентній практиці. Низка конвенцій Ради Європи та інші д мають обов'язкової юридичної сили, надають додаткові роз'яснення та пояснення для Інтернет-корис до позиції Комітету MSI-DUI, для того щоб Інтернет-користувачі розуміли свої права та свободи, їм п роз'яснювати їх у простих формулюваннях, що відповідають міжнародно-правовим стандартам Ради Організації Об'єднаних Націй.

Преамбула

17. У преамбулі подано пояснення причини прийняття Комітетом міністрів Рекомендації своїм держа Насамперед ця Рекомендація виходить з того, що відповідальність за забезпечення прав людини та ос свобод людини покладається на держави-члени Ради Європи, що має здійснюватися відповідно до ЄК Судом. Сюди ж належать й інші зобов'язуючі документи Ради Європи, зокрема, Конвенція про кіберз «**Будапештська конвенція**»), Конвенція про захист дітей від сексуальної експлуатації та сексуальног №201, надалі – «**Ланцаротська конвенція**»), Конвенція про захист осіб у зв'язку з автоматизованою персональних даних (СЕД №108, надалі – «**Конвенція 108**»).

18. Інші незобов'язуючі стандарти, ухвалені Комітетом міністрів, містять рекомендації державам-чле пов'язаних з Інтернетом. Серед таких стандартів: Рекомендація CM/Rec(2007)16 Комітету міністрів д заходи щодо підвищення цінності Інтернету як суспільної служби; Рекомендація CM/Rec(2008)6 Ком державам-членам про заходи з розвитку поваги до свободи слова та інформації у зв'язку з Інтернет-ф Рекомендація CM/Rec(2010)13 Комітету міністрів державам-членам про захист осіб у зв'язку з автома обробкою персональних даних у контексті профілювання; Рекомендація CM/Rec(2011)7 Комітету мін членам про нове поняття ЗМІ; Рекомендація CM/Rec(2012)4 Комітету міністрів державам-членам про у зв'язку з послугами соціальних мереж та Рекомендація CM/Rec(2012)3 Комітету міністрів державам прав людини щодо пошукових систем.

19. Другий пункт преамбули передбачає, що зобов'язання держав дотримуватися, захищати та сприят передбачають зобов'язання здійснювати контроль над приватними компаніями. Це твердження випли ЄКПЛ, за якою держави повинні гарантувати кожному, хто перебуває під їхньою юрисдикцією, права передбачені Конвенцією. Сюди належить і захист від порушень прав людини з боку недержавних суб вживання відповідних кроків для запобігання, розслідування, покарання і відшкодування завданих по допомогою ефективного законодавства і заходів. Суд у своїх рішеннях підтвердив, що на держави по позитивне зобов'язання захищати основні права та свободи осіб в Інтернеті, зокрема ті, що стосуютьс

вираження поглядів[6], захисту дітей та молоді[7], захисту моралі та прав інших осіб[8], боротьби з расистс
ксенофобськими закликами, а також протидії дискримінації і расовій ненависті[9]. Крім того, Суд покла
відповідальність за відмову захищати своїх громадян від негативного впливу на їхні права та свободи
приватних компаній[10]. У другому пункті також відображено принцип універсальності та неподільност
закріплений у Віденській декларації, прийнятій на Саміті глав держав та урядів держав-членів Ради Є
року.

20. У третьому пункті преамбули підтверджено значення Інтернету як суспільної служби, як це перед
Рекомендації Комітету міністрів CM/Rec(2007)16[11]. Зважаючи на велику роль Інтернету в повсякденн
користувачів та необхідність забезпечувати захист їхніх прав людини в Інтернеті, у цій рекомендації
повинен ставати об'єктом неправомірного, безпідставного або необґрунтованого втручання в свої пра

21. У четвертому пункті преамбули визначено мету цієї Рекомендації – розширювати розуміння кори
людини в онлайні та сприяти їх ефективній реалізації, в тому числі завдяки доступу до ефективних за
захисту. Саме тому настільки важливо інформувати користувачів про загрози їхнім основним правам
про можливості компенсації. Заява про можливості, що надаються Інтернетом для транспарентності т
суспільних справах, пояснює природу самої основи цієї Рекомендації, яка полягає в тому, щоб дати м
особам і спільнотам брати участь у демократичному житті.

Резолютивна частина Рекомендації

22. У п'ятому пункті міститься основний принцип стандартів Ради Європи, пов'язаних з Інтернетом:
свободи однаковою мірою застосовуються в умовах онлайн і офлайн[12]. Цей підхід було підтверджено
людини в її Резолюції від 2012 року «Заохочення, захист і дотримання прав людини в Інтернеті». Спр
цього Посібника посилить захист прав людини та основоположних свобод відповідно до чинних стан
людини.

23. У підпункті 5.1 державам-членам рекомендовано розповсюджувати цей Посібник не лише через о
влади, але і залучати приватний сектор. Це може бути його публікація та поширення в друкованій фор
електронних форматах. Відповідні державні органи також можуть розміщувати цей Посібник на своїх
можна закликати і приватний сектор.

24. У підпункті 5.2 підтверджено, що здійснення прав людини та основоположних свобод в Інтернеті
обмеженням, що мають законну мету і є необхідними в демократичному суспільстві, як це передбаче
статтях ЄКПЛ. З метою забезпечення дотримання цих умов Комітет міністрів рекомендував державам
здійснювати оцінку, регулярний огляд та (де необхідно) знімати обмеження на права людини й основ
Інтернеті.

25. У підпункті 5.3 містяться заклики до держав-членів розширювати свої зусилля із забезпечення пра
засіб правового захисту, зокрема й завдяки поглибленню координації і співробітництва між існуючим
інститутами, установами (у тому числі й регуляторами електронного зв'язку) та спільнотами, які забе
компенсації, наприклад, у контексті обробки скарг, з якими звертаються Інтернет-користувачі. Ця Рек
визнає наявність різноманітних механізмів компенсації в різних державах-членах, що надають такі ст
захисту даних, омбудсмени, суди або гарячі лінії. Держави-члени можуть також здійснювати перевір
механізмів компенсації у межах своєї юрисдикції й узагальнювати відповідну інформацію в зручних
списках механізмів компенсації. Подібну інформацію можна поширювати разом із цим Посібником, н
додатку. Це один із заходів, що може бути здійснений одразу після прийняття Рекомендації.

26. За своєю природою Інтернет функціонує за принципом відправлення та одержання запитів на інф
кордони і незалежно від них. Це означає, що права людини та основоположні свободи в Інтернеті в де

можуть бути предметом дій із боку державних або недержавних суб'єктів поза межами Ради Європи; мати місце втручання в свободу вираження поглядів та доступу до інформації, а також щодо поваги п зв'язку з персональними даними. З огляду на це у підпункті 5.4 міститься рекомендація координувати державами-членами Ради Європи і державами, що не входять до складу цієї організації, а також недер суб'єктами.

27. У підпункті 5.5 державам-членам рекомендовано заохочувати повноцінний діалог між приватним відповідними органами державної влади і громадянським суспільством у тому, що стосується соціаль останнього. Основоположний принцип Керівних принципів підприємницької діяльності в аспекті пра тому, що приватні компанії повинні поважати права людини, а це означає, що їм варто уникати поруш осіб і протидіяти негативному впливу на права людини, до якого вони причетні. Транспарентність та суб'єктів приватного сектора визнаються важливим засобом демонстрації їхньої відповідальності шля та поширення Посібника. Наприклад, провайдери Інтернет-послуг і провайдери доступу до контенту на Посібник у положеннях та щодо умов користування їхніми послугами.

28. У підпункті 5.6 визнається той ключовий внесок, який може зробити громадянське суспільство у р застосування Посібника. Таким чином, державам-членам рекомендовано заохочувати організації гром суспільства та активістів до розповсюдження і застосування Посібника, а також до посилання на ньог виступають за імплементацію стандартів у галузі прав людини та їх дотримання.

Додаток

Посібник із прав людини для Інтернет-користувачів

Вступ

29. Цей Посібник звертається безпосередньо до користувача. Він виступає інструментом для звичайно користувача, який не має спеціальних знань про Інтернет, що ґрунтуються на відповідній освіті або на йдеться про вміння користувача правильно поводитися в Інтернеті (наприклад, щодо даних про свою персональних даних). Користувачі повинні бути поінформовані в повному обсязі щодо того, як їхній може впливати на їхні права та свободи, а також про наслідки надання згоди на те, що вони обирають розуміти обмеження щодо їхніх прав, а також знати про існуючі механізми компенсації.

30. Посібник ґрунтується на положеннях ЄКПЛ і відповідній прецедентній практиці Суду. У ньому та зобов'язуючі документи Ради Європи. Посібник спирається також на інші документи, а саме на окрем рекомендації Комітету міністрів. Цей Посібник не обмежує дотримання чинних стандартів у сфері пра яких він був розроблений. Прав і свобод, про які йдеться у Посібнику, потрібно дотримуватися відпов документів, на основі яких вони були розроблені. Посібник містить посилання на чинні стандарти у га відповідні механізми їх дотримання, при цьому не створюючи нових прав та свобод. Цей Посібник не зобов'язуючим роз'ясненням стандартів у сфері прав людини. Наприклад, наступні уточнення про мо втручання у права людини, а також рекомендації з надання допомоги користувачам щодо протидії нас в Інтернеті заслуговують подальшої уваги з тим, щоб допомогти користувачам краще розуміти свої пр та інших. Водночас Посібник лишається відкритим для оновлення та приведення його у відповідність Ради Європи та прецедентного права Суду, пов'язаних із розвитком технологій.

Доступ і недискримінація

31. У цьому Посібнику наголошено на принципах та міркуваннях, які вважаються такими, що нерозри загалом застосовні до всіх прав людини та основоположних свобод, що містяться в ньому, зокрема й

Інтернету і принципу недискримінації.

32. І хоча доступ до Інтернету досі офіційно не визнаний у якості права людини (враховуючи відмінно контекстах, зокрема й у внутрішньому законодавстві та політиці), він розглядається як умова та факто вираження поглядів та іншим правам і свободам[14]. Відповідно позбавлення Інтернет-користувачів дос негативно відобразитися на здійсненні ними своїх прав і свобод і навіть означати обмеження права на поглядів, в тому числі права на отримання і поширення інформації. Суд заявив, що в наш час Інтернет головних засобів реалізації права на свободу вираження поглядів та інформації. Свобода вираження п поширюється не лише на зміст інформації, але також на засоби її поширення, оскільки будь-яке їх обм порушує право на отримання і поширення інформації. Таке втручання може бути прийнятним лише у відповідності умовам, передбаченим у п. 2 статті 10 ЄКПЛ у її тлумаченні Судом[15]. Захід, що може вп осіб до Інтернету, передбачає відповідальність держави згідно зі статтею 10[16].

33. У зв'язку з цим у Посібнику стверджується, що Інтернет-користувачі не повинні позбавлятися дос проти їх волі за винятком тих випадків, коли відповідне рішення приймається Судом. Однак це не вар заходи законного примусового позбавлення доступу, наприклад, в контексті договірних зобов'язань. Інтернету дозволяється відключати від Інтернету у разі несплати за послуги, що їм надаються, але це крайньою мірою. Крім того, діти можуть підпадати під обмеження доступу до Інтернету в межах здій контролю за використанням Інтернету залежно від віку та зрілості дитини.

34. Інтернет-користувачі повинні мати ефективні засоби правового захисту у разі їх відключення від І випадках, коли на це немає рішення суду. Це передбачає необхідність повідомлення користувача пров послуг про причини та правові підстави такого відключення, порядок оскарження та звернення з прох відновлення повного доступу до Інтернету. Такі запити повинні розглядатися в розумні строки. Крім Інтернет-користувач при реалізації ним свого права на справедливий судовий розгляд повинен мати м звернутися з проханням про перегляд заходу про відключення компетентним адміністративним та (аб Ці аспекти здійснення правосуддя підсумовано в останньому розділі Посібника під назвою «Ефективн захисту».

35. Ще одним аспектом доступу до Інтернету є позитивні дії та заходи, що вживаються органами держ того, щоб кожен мав доступ до Інтернету. Комітет міністрів Ради Європи рекомендував державам-чле підвищенню цінності Інтернету як суспільної служби[17]. Під цим розуміється «інтенсивне використанн Інтернету в якості найважливішого інструмента в повсякденному житті (спілкування, інформація, зна операції) і пов'язані з цим законні очікування того, що послуги Інтернету надаватимуться за прийнятн будуть доступними, безпечними, надійними і безперервними». Цей розділ інформує користувачів про мати доступ до Інтернету, який має надаватися за прийнятною ціною та на недискримінаційній основі

36. Право на доступ до Інтернет-контенту пов'язане з правом на отримання та поширення інформації передбачено у статті 10 ЄКПЛ[18]. Комітет міністрів Ради Європи заявив, що кожен Інтернет-користува якомога ширший доступ до Інтернет-контенту, програм та послуг на власний вибір, незалежно від того безоплатно чи ні, з застосуванням відповідних пристроїв на власний вибір. Це – загальний принцип, я називають «мережевою нейтральністю» і який повинен застосовуватися незалежно від інфраструктур використовуються для доступу до Інтернету[19].

37. Органи державної влади повинні докладати розумних зусиль у цілях забезпечення доступу до Інте категорій осіб, зокрема тих, що проживають у віддалених районах, та інвалідів, що ґрунтується на пр суспільної служби, закріпленому в Рекомендації №R(99)14 Комітету міністрів щодо нових комунікац інформаційних послуг[20]. У Рекомендації підкреслено, що особи, які проживають у сільських чи геогра районах, малозабезпечені особи або особи з особливими потребами, а також інваліди можуть очікуват

заходи з боку органів державної влади у зв’язку з їхнім доступом до Інтернету.

38. Очікування осіб з обмеженими можливостями мати однаковий з іншими Інтернет-користувачами
недискримінаційний доступ до Інтернету випливає з документів Ради Європи, у яких державам-члена
робити все необхідне для забезпечення особам з обмеженими можливостями доступу до Інтернету та
члени повинні заохочувати невисоку вартість доступу, пам’ятаючи про важливість структури, необхід
рівня обізнаності цих осіб та груп, практичне значення та привабливість доступу до Інтернету і послу
здатність до адаптації та сумісність[22].

39. Принцип недискримінації повинен застосовуватися до взаємодії користувача з органами державно
провайдерами, провайдерами доступу до контенту та іншими організаціями, користувачами або інши
користувачів. Четвертий пункт у дещо перефразованому вигляді викладає статтю 14 ЄКПЛ і статтю 1
ЄКПЛ, що забороняють дискримінацію.

Свобода вираження поглядів та інформації

40. Цей розділ стосується права на свободу вираження поглядів, закріплену у статті 10 ЄКПЛ. Суд у с
практиці підтвердив, що стаття 10 повністю може бути застосована до Інтернету[23]. До права на свобо
поглядів входить право на вільне висловлення своїх думок, переконань, ідей, на пошук, отримання і п
інформації незалежно від державних кордонів. Інтернет-користувачі повинні бути вільними у вираже
переконань, а також своїх релігійних і нерелігійних поглядів. Останнє стосується реалізації права на с
совісті та релігії, закріпленого у статті 9 ЄКПЛ. Свобода вираження поглядів стосується не лише «інф
що сприймаються прихильно або вважаються необразливими чи нейтральними, але також тих, що зав
шокують або виводять зі стану душевної рівноваги[24].

41. Реалізація права на свободу вираження поглядів Інтернет-користувачами повинна врівноважувати
репутації. Суд у низці справ прийняв рішення про те, що це право захищається статтею 8 ЄКПЛ, що з
повагу до приватного життя[25]. Суд постановив, що права, гарантовані статтями 8 і 10, заслуговують н
Він вважає, що коли право на свободу вираження поглядів урівноважене правом на повагу до приват
відповідні критерії такого урівноважування містять такі елементи: внесок в обговорення, які становля
інтерес, ступінь знаменитості конкретної особи, предмет заяви, попередню поведінку відповідної осо
інформації та її достовірність, зміст, форму та наслідки оприлюднення, а також тяжкість застосовуван
в Посібнику зазначено, що Інтернет-користувач повинен приділяти належну увагу репутації інших ос
праву на приватне життя.

42. Існує вираження поглядів, яке не підпадає під захист за статтею 10 ЄКПЛ, зокрема заклики до нен
постановив, що на окремі форми вираження поглядів, які рівнозначні закликам до ненависті або запер
основоположні цінності ЄКПЛ, не поширюється захист, передбачений статтею 10 Конвенції[27]. У зв’яз
застосовує статтю 17 ЄКПЛ. Хоча загальноприйнятого визначення розпалювання ненависті не існує,
Ради Європи заявив, що поняття «розпалювання ненависті» варто розуміти як таке, що охоплює всі ф
поглядів, через які здійснюється поширення, підбурення, сприяння або виправдання расової ненавист
антисемітизму або інших форм ненависті, що ґрунтуються на нетерпимості, яка виявляється через агр
та етноцентризм, дискримінацію та ворожість щодо меншин, мігрантів та осіб іммігрантського походж
цього розділу про свободу вираження поглядів міститься конкретна інформація, викладена простою д
мовою, у якій надано пояснення, що заклики до ненависті не підпадають під дію статті 10 ЄКПЛ. Цей
на те, щоб пояснити з використанням юридичних термінів різні підходи, на підставі яких до розпалюв
можуть застосовуватися статті 10 і 17 ЄКПЛ. Зважаючи на правову природу цієї відмінності, було вир
інформацію буде краще розкрити в пояснювальному меморандумі.

43. Користувачі мають право отримувати і поширювати інформацію в Інтернеті, зокрема, створювати

використовувати і розповсюджувати контент із використанням Інтернету. Суд дослідив взаємозв'язок інтелектуальної власності та свободою вираження поглядів у кримінальних справах про порушення ав думку Суду, обвинувальні вироки у цих справах були втручанням у право на свободу вираження погл перші могли вважатися обґрунтованими, вони повинні бути передбачені законом, переслідувати закон прав інших осіб і вважатися необхідними у демократичному суспільстві[29]. Обмін або надання іншим к обмінюватися файлами в Інтернеті, навіть якщо йдеться про матеріали, захищені авторським правом т вигоди,охоплюються правом отримувати та поширювати інформацію, як це передбачено статтею 10 Є є абсолютним, а тому існує необхідність зважувати, з одного боку, важливість обміну інформацією, а зацікавленість у захисті прав суб'єктів авторського права. Суд підкреслив, що інтелектуальна власніст основі статті 1 Протоколу до ЄКПЛ. Таким чином, питання полягає у збалансуванні двох конкуруючи яких захищаються ЄКПЛ.

44. Рекомендація Комітету міністрів державам-членам про заходи щодо підвищення цінності Інтернет служби містить конкретні рекомендації щодо заходів і стратегій стосовно свободи спілкування і творч незалежно від державних кордонів. Зокрема, у відповідних випадках повинні вживатися заходи щодо «повторному використанню» Інтернет-контенту, що означає використання існуючих цифрових конте створення майбутнього контенту або надання послуг таким чином, щоб вони були сумісними з поваго інтелектуальної власності[31].

45. У пункті 4 надано загальний огляд вимог, яким повинні відповідати обмеження права на свободу в Відповідно до статті 10 ЄКПЛ держави-члени насамперед зобов'язуються не втручатися в обмін інфо особами незалежно від того, будуть це фізичні або юридичні особи. Суд підтвердив, що ефективна ре свободу вираження поглядів також може потребувати позитивних заходів захисту навіть у сфері відно особами. Питання про відповідальність держави може виникнути в результаті того, що остання не пр національне законодавство[32]. Порушення ЄКПЛ може бути встановлене і в тому випадку, коли тлума національними судами юридичного акту, незалежно від того, чи є останній приватним договором, дер документом, нормативним положенням чи адміністративною практикою, є нерозумним, довільним, д або у більш широкому розумінні – таким, що не відповідає основоположним принципам ЄКПЛ[33].

46. Свобода вираження поглядів не є абсолютним правом і може бути предметом обмежень. Втручан вираження поглядів повинно розглядатися як будь-яка форма обмеження з боку будь-якого органу, що повноваження та обов'язки або функціонує у сфері державних послуг, наприклад, до них належать су прокуратури, міліція, будь-які правоохоронні органи, розвідувальні служби, центральні або місцеві ра установи, керівні органи збройних сил та професійні державні структури.

47. Відповідно до п. 2 статті 10 ЄКПЛ будь-яке втручання повинно бути передбачене законом. Це озн законодавство має бути доступним, чітким і достатньо точним для того, щоб особи могли регулювати Законодавство повинно передбачати достатні гарантії від надмірних обмежувальних заходів, зокрема контроль із боку суду чи іншого незалежного судового органу[34]. Втручання також повинно пересліду інтересах національної безпеки, територіальної цілісності або суспільної безпеки з метою запобігання громадського порядку чи злочинам, захисту здоров'я чи моралі, захисту репутації чи прав інших осіб, розголошення отриманої конфіденційної інформації, підтримки авторитетності та безсторонності суд перелік є вичерпним, але його тлумачення і сфера дії розвиваються разом із практикою Суду. Втручан бути необхідним у демократичному суспільстві, а це означає, що потрібно довести його нагальну сусп наявність законної мети, а також того факту, що цей захід є найменш обмежувальним для досягнення вимоги викладені зрозумілою для користувача мовою, тобто будь-які обмеження свободи вираження бути довільними і мають переслідувати законну мету відповідно до ЄКПЛ, наприклад, серед іншого й національної безпеки або громадського порядку, здоров'я населення і моралі, що повинно відповідати сфері прав людини.

48. У наступних пунктах Пояснювального меморандуму більш докладно розглядаються гарантії, які п
Інтернет-користувачам у разі обмеження права на свободу вираження поглядів онлайн. Прикладом по
що можуть розглядатися як порушення свободи вираження поглядів, може бути блокування та фільтр
принципи щодо блокування та фільтрації ґрунтуються на практиці Суду чи інших відповідних станда
Комітетом міністрів[36].

49. Державні органи мають право вдаватися до загальнодержавних заходів блокування або фільтрації
випадках, коли фільтрація стосується конкретного і чітко визначеного контенту за умови наявності рі
компетентного національного органу про його незаконність, яке може бути переглянуте незалежним т
судом або регулюючим органом згідно з вимогами статті 6 ЄКПЛ[37]. Державні органи повинні забезпе
до та під час їх застосування, що забезпечить пропорційність їхніх наслідків меті обмеження, а отже –
демократичному суспільстві, з метою недопущення невиправдного блокування контенту[38].

50. Заходи блокування конкретного Інтернет-контенту не повинні довільно використовуватися як зас
блокування інформації в Інтернеті. Вони не повинні мати побічних наслідків у формі закриття доступ
інформації, що істотно обмежить права Інтернет-користувачів[39]. Вони повинні бути передбачені зако
недопущення зловживання владою повинен забезпечуватися суворий контроль за масштабами блокув
судовим розглядом[40]. У ході судового розгляду подібних заходів потрібно зважувати відповідні конф
урівноважувати їх і з'ясовувати, чи існує менш масштабний захід, який можна застосувати в цілях бл
конкретного Інтернет-контенту[41]. Зазначені вище вимоги та принципи не можуть стати на заваді вста
метою захисту неповнолітніх у конкретних місцях, наприклад, школах, бібліотеках, де останні мають
Інтернету[42].

51. Фільтрація та деіндексація Інтернет-контенту пошуковими системами несе в собі загрозу порушен
вираження поглядів Інтернет-користувачів. Пошукові системи вільно здійснюють загальний пошук та
інформацію, що міститься у Всесвітній мережі. Їх не можна зобов'язувати здійснювати моніторинг св
ініціативно з метою виявлення передбачувано незаконного контенту, і вони не повинні здійснювати б
фільтрацію або блокування, крім тих випадків, коли це передбачено рішенням суду або іншого компе
Деіндексація або фільтрація окремих сайтів на запит державних органів повинні бути прозорими, вузь
також регулярно переглядатися за умови дотримання вимог справедливого судового розгляду[43].

52. Цей розділ також визначає деякі гарантії, що повинні надаватися Інтернет-користувачам у разі зап
обмежень, зокрема, це стосується інформування користувача та надання можливості оскарження таки
йдеться в Рекомендації Комітету міністрів Ради Європи про заходи щодо фільтрації та блокування[44].
користувачам повинна надаватися інформація про активацію фільтрації, причини здійснення фільтра
контенту для розуміння ними того, яким чином та відповідно до яких критеріїв здійснюється фільтра
списки, білі списки, блокування за ключовим словом, рейтинг контенту, деіндексація або фільтрація
контенту пошуковими системами). Їм повинна бути надана точна інформація та рекомендації щодо об
фільтру, зокрема, до кого звертатися, коли існує припущення, що контент був необґрунтовано заблок
допомогою яких засобів можна відключати фільтри щодо конкретного типу контенту або сайту. Кори
забезпечувати ефективними і загальнодоступними засобами оскарження та правового захисту, в тому
призупиненням дії фільтрів у тих випадках, коли користувачі заявляють про необґрунтованість блоку

53. Можуть мати місце випадки, коли компанії, наприклад, такі, що представляють соціальні мережі,
що був створений та розміщений Інтернет-користувачами, облікові записи користувачів (наприклад,
або його присутність в соціальних мережах), обґрунтовуючи свої дії недотриманням вимог користува
послугами. Подібні дії можуть становити втручання в право на свободу вираження поглядів і право на
поширення інформації, крім випадків дотримання вимог п. 2 статті 10 ЄКПЛ у її тлумаченні Судом[45].

54. Згідно з Керівними принципами ООН підприємницької діяльності в аспекті прав людини (які не м

юридичної сили) приватні компанії зобов'язані поважати права людини, що вимагає від них не завдав
людини та не сприяти такій шкоді, а також забезпечувати або співпрацювати щодо компенсації у випа
шкоди. Обов'язок захищати і надавати доступ до ефективних засобів правового захисту – один із най
обов'язків держави, що знайшло своє відображення в п. 5 розділу про свободу вираження поглядів. К
соціальна відповідальність Інтернет-провайдерів передбачає обов'язок боротьби з розпалюванням нен
контентом, що породжує ненависть чи дискримінацію. Провайдери онлайн-послуг повинні виказувати
здійснювати редакційне реагування на висловлювання расового, ксенофобського, антисемітського, не
сексистського (зокрема й ставлення щодо лесбіянок, гомосексуалістів, бісексуалів та транссексуалів)
характеру[46]. Ці провайдери також мають бути готовими надати допомогу Інтернет-користувачам чере
про зміст або вираження поглядів та (або) поведінку, які можуть вважатися незаконними[47].

55. Посібник звертає увагу Інтернет-користувачів на те, що провайдери онлайн-послуг, які розміщують
створений користувачами, мають право на здійснення різних рівнів редакційної оцінки змісту своїх по
для своєї редакційної свободи вони повинні забезпечувати Інтернет-користувачам реалізацію їхнього
отримання та поширення інформації відповідно до статті 10 ЄКПЛ[49]. Це означає, що будь-яке обмеже
створеного користувачем контенту повинно бути конкретним, виправданим з точки зору цілей, для до
було встановлене, і доведеним до відома відповідного Інтернет-користувача.

56. Інтернет-користувач повинен мати змогу приймати поінформоване рішення щодо того, чи користу
послугами онлайн. На практиці Інтернет-користувач повинен бути повною мірою поінформований пр
передбачувані заходи щодо видалення створеного ним контенту або його облікового запису до запров
заходів[50]. Інтернет-користувачам також повинна надаватися доступна (зрозумілою для користувача м
інформація щодо фактів та підстав для вжиття заходів, за допомогою яких передбачено видалення кон
запису. Це передбачає наявність законодавчих положень, на основі яких були вжиті такі заходи, а так
оцінки пропорційності та законності мети, яку вони переслідують. Інтернет-користувачі також повинн
звернутися з проханням про перегляд рішення про видалення контенту та (або) облікового запису в ре
оскаржити рішення в компетентному адміністративному та (або) судовому органі.

57. У шостому підпункті йдеться про анонімність, що ґрунтується на практиці Суду, Будапештській к
документах Комітету міністрів. Суд розглянув питання конфіденційності спілкування в Інтернеті у сп
відмовою однієї з держав-членів Ради Європи змусити Інтернет-провайдера назвати особу, яка розмі
оголошення щодо неповнолітньої особи на сайті знайомств у Інтернеті. Суд постановив, що, незважа
свобода вираження поглядів та конфіденційність спілкування є головними цінностями, а користувачі
Інтернет-послуг повинні мати гарантії поваги до їхнього приватного життя та свободи вираження пог
не можуть бути абсолютними і повинні поступатися місцем у такому випадку іншим законним вимога
запобігання порушенню громадського порядку або злочину чи захист прав і свобод інших осіб. На де
позитивне зобов'язання забезпечувати рамки для поєднання цих конкуруючих інтересів[51].

58. Будапештська конвенція не передбачає кримінальну відповідальність за використання комп'ютер
цілях анонімної комунікації. Згідно з пояснювальною доповіддю до цієї Конвенції, «зміна трафіку дан
сприяння анонімним комунікаціям (наприклад, діяльності анонімних систем пересилання електронни
внесення змін до даних із метою реалізації безпеки комунікації (наприклад, шифрування) повинні в пр
розглядатися як законний захист приватного життя, а тому вважатися правомірними. Водночас Сторо
конвенції] можуть виявити бажання криміналізувати окремі зловживання, пов'язані з анонімною кому
наприклад, змінені пакетні дані з метою приховування ідентичності особи при скоєнні злочину»[52].

59. Комітет міністрів Ради Європи підтвердив принцип анонімності в своїй Декларації про свободу сп
Інтернеті[53]. Відповідно з метою забезпечення захисту від стеження онлайн і зміцнення свободи вираж
держави-члени Ради Європи повинні поважати бажання Інтернет-користувачів не розкривати свою ос
повага до анонімності не заважає державам-членам вживати заходів для відстеження осіб, відповідал

кримінальних діянь відповідно до національного законодавства, ЄКПЛ та інших міжнародних догово
правосуддя та діяльності правоохоронних органів.

Зібрання, об'єднання та участь

60. Право на свободу зібрань та об'єднань передбачене у статті 11 ЄКПЛ. Воно також стосується при
Судом щодо захисту політичних заяв, зокрема, в рамках п. 2 ст. 10 ЄКПЛ передбачено мало свободи
контексті політичних заяв або обговорень із питань, що становлять суспільний інтерес[54].

61. Користувач має право на свободу зібрань та об'єднань з іншими особами через використання Інте
формування, приєднання, мобілізацію та участь у суспільних групах та зібраннях, а також профспілка
використанню інструментів, заснованих на Інтернеті. Сюди належить, наприклад, підписання петицій
кампаніях або інших формах громадських акцій. Користувач повинен мати свободу обирати інструме
цих прав, таких як сайти, додатки чи інші послуги. Реалізація цього права не потребує будь-якого фор
соціальної групи та зібрань із боку органів державної влади.

62. Право на протест однаковою мірою застосовується як в режимі онлайн, так і в режимі офлайн. Пр
наслідки для всього суспільства, такі як створення перешкод або блокування доступу до приміщень,
обмеження здійснення права на свободу зібрань відповідно до статті 11 ЄКПЛ. Однак так не обов'язк
кожному випадку, коли подібні дії приводять до порушення послуг онлайн, наприклад, якщо йдеться
несанкціонований доступ до конкретного сайту, до обмеженого онлайн-простору або обробки цифров
дозволу. Врешті, важливо повідомляти користувача про те, що свобода та наслідки протесту онлайн,
порушення, не завжди припустимі.

63. Інтернет став інструментом активної участі громадян у побудові та зміцненні демократичних сусп
міністрів рекомендував державам-членам розробляти та запроваджувати стратегії електронної демокр
участі та електронного врядування з використанням інформаційно-комунікаційних технологій (ІКТ) у
процесах та обговореннях як у відносинах між державними органами та громадянським суспільством
державних послуг[55].

64. Сюди входять свобода участі в публічних політичних дебатах на місцевому, національному і глоб
законодавчі ініціативи, контроль за прийняттям рішень, в тому числі право підписувати петиції з заст
де вони існують. Це ґрунтується на рекомендаціях Комітету міністрів державам-членам про заохочен
громадянами ІКТ (у тому числі онлайн-форумів, онлайн-журналів, політичних чатів, смс-розсилок та
спілкування між громадянами) для участі в демократичних обговореннях, електронних заходах та еле
із метою озвучення своїх проблем, ідей та ініціатив, організації діалогу та обговорень із представника
владою, а також контролю за діяльністю посадових осіб та політиків із питань, що становлять суспіль

<u>Приватне життя і захист даних</u>

65. Право на повагу до сімейного і приватного життя закріплене у статті 8 ЄКПЛ. Це право отримало
тлумачення в практиці Суду, доповнюється і посилюється Конвенцією Ради Європи 108.

66. Приватне життя – це поняття, для означення якого не існує вичерпного визначення. Суд наголоси
8 охоплює широке коло інтересів, зокрема, приватне і сімейне життя, житло і кореспонденцію, зокрем
телефонні переговори[56] та електронну пошту на робочому місці. Приватне життя пов'язане з правом
зображення[57], наприклад, у формі фотографій або відеокліпів. Воно також стосується ідентичності ос
розвитку, права на налагодження та розвиток відносин з іншими людьми. Ним також охоплено діяльн
або підприємницького характеру[58].

67. Багато напрямків діяльності користувачів передбачають певну форму автоматизованої обробки пе
наприклад, використання браузерів електронної пошти, миттєвих повідомлень, передачі голосових по
Інтернет-протоколи, соціальні мережі й пошукові системи, а також хмарні сервіси для зберігання дан
охоплює всі операції, що здійснюються в Інтернеті у зв'язку зі збиранням, зберіганням, зміною, видал
відновленням чи поширенням персональних даних[59].

68. Існують принципи та правила, яких повинні дотримуватися органи державної влади та приватні ко
здійснюють обробку персональних даних. Необхідно, щоб користувач знав і розумів, яким чином обр
та які дії можна вчиняти у зв'язку з цим, наприклад, звернутися з проханням про виправлення або вид
Згідно з Конвенцією 108, персональні дані можуть бути отримані та оброблені справедливо і законно,
визначених та правомірних цілей. Ці процеси повинні бути адекватними, адаптованими і не надмірни
задля яких такі дані зберігаються. Самі дані повинні бути точними і за необхідності оновлюватися, зб
спосіб, що дозволяє ідентифікувати особу, персональні дані якої обробляються, та не довше строку, я
мети, заради якої ці дані зберігаються[60].

69. Наголос робиться на двох конкретних принципах обробки персональних даних: законності такої о
користувача. Користувач повинен бути поінформований про те, що дані можуть оброблятися лише у
законом випадках і за його згоди, яку користувач може надати, наприклад, погодившись з умовами ко
Інтернет-послугою.

70. Вільна, конкретна, інформована та чітка (однозначна) згода особи на обробку персональних даних
предметом обговорення з метою внесення відповідного положення до Конвенції 108[61]. Інформована з
Рекомендації CM/Rec(2012)4 Комітету міністрів державам-членам про захист прав людини у зв'язку з
соціальних мереж. Зокрема, соціальні мережі повинні отримувати інформовану згоду своїх користува
поширенням або обміном їхніми персональними даними з іншими категоріями осіб чи компаній або в
спосіб, інший ніж той, що необхідний для задоволення визначених цілей. Для отримання згоди корист
повинні мати можливість висловитися на користь більш широкого доступу третіх осіб (наприклад, ко
мережах використовуються програми третіх осіб). Користувачі також повинні мати можливість відкл

71. Також варто згадати Рекомендацію CM/Rec(2010)13 Комітету міністрів державам-членам про захи
автоматичною обробкою персональних даних у контексті профілювання. Під цим розуміють методи а
обробки даних шляхом застосування профілю до особи з метою прийняття рішень щодо неї або в ціля
визначення особистих преференцій, поведінки, позицій. Наприклад, персональні дані Інтернет-корист
зібрані та оброблені в контексті його взаємодії з сайтом чи додатком або в контексті використання бр
протягом певного періоду часу або через різні сайти (наприклад, шляхом збору інформації про те, які
відвідує особа, час відвідування, предмет пошуку та залишені коментарі). «Ідентифікаційні маркери»
способів відстеження активності користувача – роблять це шляхом зберігання інформації в апаратурі
подальшого вилучення. Рекомендація передбачає право Інтернет-користувачів надавати свою згоду на
персональних даних із метою профілювання і право на відмову від такої згоди[62].

72. Права Інтернет-користувачів на інформацію у зв'язку з обробкою їхніх персональних даних згадує
документах Ради Європи. Конвенція 108 передбачає, що суб'єкту даних повинна бути надана можлив
факт обробки його персональних даних будь-якою фізичною або юридичною особою, з'ясовувати осн
обробки, а також найменування та фактичну адресу або основне місце розташування органу, який зді
даних, та отримувати в розумні строки і без надмірних затримок чи значних витрат підтвердження фа
персональних даних, а також отримувати повідомлення про такі дані у чіткій формі[63].

73. Інформування користувачів також згадується в Рекомендації CM/Rec(2012)4 Комітету міністрів де
захист прав людини у зв'язку з послугами соціальних мереж. Інтернет-користувачі в соціальних мере
чіткий та зрозумілий спосіб поінформовані про внесення будь-яких змін до умов надання послуг пров

передбачає й інші дії, такі як встановлення додатків третіх сторін, що можуть становити загрозу прив користувачів; законодавство, що не застосовується до надання послуг у соціальних мережах і відпові персональних даних; наслідки відкритого доступу (в часі й географічно) до їхніх профілів і комуніка пояснення різниці між приватними та публічними комунікаціями, а також наслідки публічного досту тому числі необмеженого доступу і збору даних третіми особами; необхідність отримувати попередн перед оприлюдненням їхніх персональних даних, зокрема й відео- та аудіоконтенту у тих випадках, к розширюють доступ за межі самостійно відібраних користувачами контактів. Інтернет-користувачам надавати конкретну інформацію щодо логічного підходу, який лежить в основі обробки персональних використовуються для присвоєння їм профілів та з метою профілювання.

74. Інтернет-користувачі повинні мати можливість здійснювати контроль за своїми персональними да Конвенції 108, зокрема, у тому, що стосується права на виправлення або стирання даних, що були обр також права на засоби правового захисту у тому випадку, коли підтвердження або (залежно від конте виправлення чи стирання, про які йшлося вище, не були здійснені[64].

75. Рекомендація CM/Rec(2012)3 Комітету міністрів державам-членам про захист прав людини щодо стосується низки заходів, які можуть вживати провайдери з метою захисту приватного життя своїх ко входить захист персональних даних від незаконного доступу третіх осіб і схеми повідомлення про по заходів також повинні належати абонентське шифрування повідомлень між користувачами і провайде системи. Взаємна кореляція даних, що походять від різних послуг/платформ і належать провайдеру п може мати місце лише у разі надання користувачем однозначної згоди на цю конкретну послугу. Кор мати можливість доступу, виправлення та видалення своїх даних, зібраних у ході користування таким числі щодо будь-якого створеного профілю, наприклад, у цілях прямого маркетингу[65].

76. Соціальні мережі повинні також допомагати користувачам управляти своїми даними та захищати допомогою:

- *шаблонних налаштувань приватності за замовчуванням,* якими обмежується доступ до визна користувачем контактів. Це передбачає адаптацію до їхніх умов забезпечення приватного житт публічного доступу до їхніх даних;

- *посиленого захисту чутливих даних,* таких як доступ до біометричних даних або розпізнаван повинен активуватися автоматично;

- *убезпечення даних від незаконного доступу до персональних даних користувача* третіх осіб, у абонентське шифрування між користувачем і соціальними мережами. Користувачів необхідно порушення безпеки їхніх персональних даних із метою вживання ними запобіжних заходів у в а також для уважного ставлення до своїх фінансових операцій (наприклад, коли соціальні мере банківської інформації або реквізитів кредитної картки);

- *захисту приватного життя на рівні технологічного рішення:* коли потреба в захисті даних в розробки послуг або продуктів, а зміни в наявних послугах постійно оцінюються на предмет в життя;

- *захисту тих, хто не є користувачами соціальних мереж,* шляхом відмови від збору та обробк персональних даних, наприклад, адрес електронної пошти та біометричних даних. Користувач свої зобов'язання перед іншими особами, зокрема, що публікація персональних даних, пов'яза особами, повинна відповідати дотриманню прав цих інших осіб[66].

77. Перед закриттям облікового запису користувача в соціальній мережі він повинен мати можливість

перенести свої дані на інший сервіс чи пристрій у зручному для нього форматі. Після цього всі дані ко користувача повинні бути назавжди видалені із носіїв зберігання служби соціальної мережі. Крім того користувачі повинні мати можливість робити свідомий вибір щодо своєї ідентичності онлайн, в тому використання псевдоніма. Якщо соціальна мережа потребує реєстрації із зазначенням дійсних особис публікація дійсних особистих даних в Інтернеті повинна бути здійснена на вибір користувача. Це не з правоохоронним органам отримувати доступ до дійсних особистих даних користувача у разі необхідн надання відповідних правових гарантій, що забезпечують дотримання основних прав і свобод.

78. У контексті профілювання користувач також повинен мати можливість заперечувати проти викор персональних даних із метою профілювання і проти рішення, яке приймається виключно на основі пр правові наслідки для користувача або істотно торкається його інтересів, за винятком тих випадків, ко законом, у якому вказано заходи із забезпечення законних інтересів користувачів, зокрема, дозволяєт точку зору, за винятком тих випадків, коли рішення приймається у ході виконання договору і при цьо існують заходи із забезпечення законних інтересів Інтернет-користувача[67].

79. Права Інтернет-користувачів не є абсолютними, саме тому у третьому підпункті є посилання на сл Винятки дозволяються, коли вони передбачені законом і у тих випадках, коли вони є необхідною міро демократичному суспільстві в інтересах: а) захисту державної безпеки; громадської безпеки, фінансов держави або для боротьби зі злочинами; б) захисту суб'єкта даних або прав і свобод інших осіб. Обме передбачених прав можуть міститися в законі щодо автоматизованих досьє персональних даних, що в статистичних цілях або наукових досліджень у тих випадках, коли відсутня явна загроза порушення п суб'єкта даних[68].

80. Зазначено, що існує перехоплення, пов'язане з прослуховуванням, моніторингом або спостережен повідомлень, забезпеченням змісту даних через доступ і використанням комп'ютерної системи або не використанням електронного прослуховування чи пристроїв для прослуховування. Перехоплення мож передбачати запис[69]. Право на повагу до конфіденційності кореспонденції та повідомлень закріплене подальшим тлумаченням Судом. Поняття кореспонденції охоплює поштові і телекомунікаційні повід повідомлення електронною поштою на робочому місці[71]. Очікується, що тлумачення цього поняття бу щоб відповідати розвитку технологій, завдяки яким можуть з'являтися нові форми спілкування в Інте електронні листи (у широкому розумінні), миттєві повідомлення тощо, які потрапляють під дію статт

81. Далі розглянуто деякі загальні принципи, підтверджені практикою Суду, щодо перехоплення і спо повідомленнями у справах, не пов'язаних з Інтернетом, а також у справах, що стосуються втручання влади. Ці принципи надають загальні рекомендації та посилання для можливого застосування їх у май Інтернет-спілкування.

82. Перехоплення кореспонденції та телекомунікацій є втручанням у право на приватне життя й обме закріпленими у п. 2 ст. 8 ЄКПЛ. Сам факт існування законодавства, яке дозволяє здійснювати спостер телекомунікаціями, може вважатися втручанням у право на приватне життя. Законодавство, яке запро спостереження, в рамках якої всі особи у відповідній державі потенційно можуть стати об'єктом моні їхньої поштової переписки і повідомлень, безпосередньо стосується всіх користувачів або потенційни поштових і телекомунікаційних послуг у цій державі. У зв'язку з цим Суд підтвердив право кожної ос заявляти про те, що вона стала жертвою порушення, спричиненого самим фактом існування секретни законодавства, яким вони дозволяються, і при цьому вона не повинна заявляти про те, що подібні захо застосовані до неї[72].

83. Перехоплення повинно мати законодавчу підставу та бути необхідним у демократичному суспільс національної безпеки, громадської безпеки або економічного добробуту країни, запобігання заворуше для захисту здоров'я чи моралі або захисту прав і свобод інших осіб, як це передбачено статтею 8 ЄК

такі загальні принципи, що, зокрема, стосуються тих вимог, яким повинно відповідати законодавство,
приховані заходи спостереження за кореспонденцією і повідомленнями з боку органів державної влад

- *Передбачуваність* – законодавство повинно бути доступним для відповідної особи, яка повин
передбачити наслідки його застосування щодо неї. Законодавство має бути сформульовано дос
для того, щоб громадяни мали чітке уявлення про те, за яких умов і обставин влада має право в
таємного і потенційно небезпечного втручання в право на повагу до приватного життя і кореспо

- *Мінімальні гарантії у сфері дискреційних повноважень органів державної влади* – законодавс
детальні норми щодо і) характеру правопорушень, які можуть передбачати віддання наказу пр
визначення категорій осіб, повідомлення яких можуть підлягати моніторингу; ііі) граничної тр
моніторингу; iv) порядку аналізу, використання і зберігання отриманих даних; та v) запобіжни
повідомленні даних іншим особам; а також щодо обставин, за яких отримані дані можуть або п
а записи знищено[74].

- *Нагляд та перегляд компетентними органами влади* – Суд вимагає наявності адекватних і еф
щодо недопущення зловживань[75].

84. У практиці Суду щодо приватного життя на робочому місці було встановлено, що телефонні дзвін
приміщенні підприємства підпадають під категорію приватного життя і кореспонденції. Електронна п
надсилається з робочого місця, а також інформація, отримана за результатами моніторингу особистог
Інтернету, повинні захищатися за статтею 8 ЄКПЛ. У разі відсутності повідомлення працівника про т
може підлягати моніторингу, останній має розумні підстави сподіватися на повагу до приватного жит
телефонних дзвінків, електронної пошти та користування Інтернетом на робочому місці[76]. Користувач
допомога з боку органів, відповідальних за захист даних, або інших компетентних органів у державах

85. Органи, що відповідають за захист даних та існують в більшості держав-членів, відіграють важлив
розслідуванні, участі, наданні інформації або участі в іншій формі втручання з метою виправлення си
персональних даних. Це все забезпечується додатково до першочергової ролі держави у забезпеченні
персональних даних у більш широкому розумінні зобов'язання держав гарантувати право на приватне

Освіта і грамотність

86. Право на освіту закріплене в статті 2 Протоколу 1 до ЄКПЛ. Рекомендація CM/Rec(2007)16 Коміте
державам-членам про заходи підвищення цінності Інтернету як суспільної служби закликає до створе
доступу до навчального, культурного та наукового контенту в цифровій формі з наданням можливост
самовираження всім культурам і доступу до Інтернету всіма мовами включно з мовами нечисленних н
користувачі повинні мати можливість вільного доступу до наукових і культурних здобутків у Інтернет
державою[78]. Також у рамках розумних обмежень має бути забезпечений доступ до цифрових матеріал
надбанням. В окремих випадках дозволяється запроваджувати умови платного доступу до знань із мет
винагороди правовласникам за їхню роботу в межах допустимих винятків у сфері захисту прав інтеле

87. Інтернет-користувачі повинні мати можливість отримувати в Інтернеті базову інформацію, освіту,
метою реалізації своїх прав людини і основоположних свобод. Це відповідає стандартам Комітету мін
у сфері забезпечення комп'ютерної грамотності як основної передумови доступу до інформації, реалі
прав і права на освіту із застосуванням ІКТ[79].

88. Програми та ініціативи у сфері Інтернет-грамотності дозволяють Інтернет-користувачам критично
точність і достовірність Інтернет-контенту. Комітет міністрів рекомендував державам-членам Ради Є
доступу до засобів ІКТ і заохочувати освіту для того, щоб всі особи, і особливо діти, здобували навич

роботи з найрізноманітнішими ІКТ, і критично оцінювали якість інформації, зокрема тієї, що може бу
шкідливою[80].

Діти і молодь

89. Діти та молодь мають право висловлювати свої погляди, брати участь у житті суспільства і прийня
торкаються їхніх інтересів, через використання Інтернету та інших ІКТ. Це ґрунтується на стандартах
якими проголошено право всіх дітей і молоді віком до 18 років мати засоби, простір, можливості й (ко
підтримку для того, щоб вільно висловлювати свої погляди, бути почутими і вносити свій вклад у при
питань, які торкаються їхніх інтересів. При цьому їхній думці повинна приділятися належна увага з ур
віку, зрілості та рівня розуміння. Право дітей і молоді на участь повною мірою поширене на Інтернет
дискримінації за будь-якими ознаками, в тому числі за ознаками расової приналежності, етнічного по
шкіри, статі, мови, релігійних, політичних або інших переконань, національного чи соціального похо
інвалідності, народження, сексуальної орієнтації чи іншого статусу[81].

90. Дітям і молоді потрібно надавати відповідну їхньому віку та обставинам інформацію, в тому числі
мережі, ЗМІ, про те, які можливості вони мають для реалізації власних прав. Вони мають бути повно
поінформовані про масштаби своєї участі, зокрема про відповідні обмеження, очікувані та фактичні р
також про те, яким чином була врахована їхня думка[82]. У тих випадках, коли вони вважають, що мало
їхнього права на участь, їм повинні надаватися ефективні засоби компенсації і правового захисту, так
дітей способи звернення зі скаргою, судові та адміністративні процедури, а також допомога та підтри
застосуванні[83].

91. Інтернет-користувачі діти і молодь повинні мати можливість безпечного користування Інтернетом
бути забезпечена належна повага до їхнього приватного життя. Вчителі, вихователі та батьки повинні
надавати інформацію. Їхня інформаційна грамотність означає компетентне використання інструменті
інформації, вміння критично аналізувати контент, розвиток комунікаційних навичок, що сприяють ви
громадянської позиції і творчого підходу, а також навчання дітей та їхніх вихователів позитивному та
використанню Інтернету й інформаційно-комунікаційних технологій[84].

92. Право дітей на приватне життя було предметом розгляду у ряді справ у Європейському суді. Фізич
добробут дітей належить до найважливіших аспектів їхнього права на приватне життя. На держави-чл
позитивні зобов'язання щодо забезпечення ефективного дотримання цього права[85]. Суд вважає, що еф
тяжким діянням, які можуть підривати основоположні цінності та найважливіші аспекти приватного ж
закріплення дієвих положень у кримінальному законодавстві й проведення розслідування[86].

93. Важливо розуміти, що контент, який створюється або використовується дітьми та молоддю в Інтер
про них, що створюється іншими особами (наприклад, фотографії, відеозаписи, текстовий або інший
цього контенту (журнали реєстрації, архіви та обробка даних) можуть надовго або назавжди стати дос
загрожувати їхній гідності, безпеці, приватному життю або іншим чином робити їх уразливими в цей
наступних етапах їхнього життя. Вони самі, їхні батьки, опікуни, вчителі та вихователі повинні мати м
адаптуватися до цих реалій та захищати своє приватне життя онлайн. Саме тому важливо, щоб існува
рекомендації про те, як можна стерти персональну інформацію. Комітет міністрів розробив для держа
рекомендації та заявив, що за винятком прямих приписів закону не повинно бути довгострокових або
записів контенту, створеного дітьми в Інтернеті, який загрожує їхній гідності, безпеці, приватному жи
чином робить їх уразливими в цей момент або на наступних етапах їхнього життя[87]. Відповідно держа
запропоновано дослідити (там, де це доречно) разом з іншими зацікавленими сторонами можливість в
стирання такого контенту та його слідів (журналів реєстрації, архівів та обробки даних) у розумні стр
підпункт 3 не поширюється на контент, що стосується дітей або молоді та був створений у пресі або в
першому реченні цього положення Посібника зазначено, що в ньому розглядаються ситуації, пов'язан

створеним дітьми або молоддю чи іншими Інтернет-користувачами про них.

94. Щодо шкідливого контенту і поведінки онлайн діти мають право на особливу увагу та допомогу, ї
їхньому віку та обставинам, зокрема, у зв'язку з ризиком завдання шкоди, що може виникнути у зв'яз
онлайн, принизливим і стереотипним зображенням жінок, зображенням та схваленням насильства і за
зокрема у тому, що стосується самогубств, принизливих, дискримінаційних або расистських висловл
подібної поведінки, домагання з метою сексуального насильства, вербування дітей-жертв торгівлі лю
переслідування чи інших форм домагання, що можуть мати тяжкі наслідки для фізичного, емоційного
благополуччя дитини[89].

Таким чином, дітям та молоді, що користуються Інтернетом, потрібно надавати відповідну їхньому ві
іншим конкретним обставинам інформацію про види незаконного контенту та поведінки.

95. Діти та молодь також повинні мати можливість повідомляти про контент або поведінку, які створ
завдання шкоди, а також отримувати консультації та підтримку з належною увагою до їхньої конфіде
анонімності. Це особливо актуально для контенту в соціальних мережах. Комітет міністрів рекоменду
членам вдатися до активних дій щодо цього[90] та, зокрема, захищати дітей і молодь від шкідливого ко

- надання чіткої інформації про види контенту, обмін контентом або поведінку, які можуть суп
юридичним нормам;

- розробки редакційної політики таким чином, щоб відповідний контент або поведінку можна б
«неприпустимі» в умовах використання послуг соціальних мереж, забезпечувати при цьому, щ
обмежував право на свободу вираження поглядів та інформації;

- створення легкодоступних механізмів для повідомлення про неналежний або явно незаконни
поведінку в соціальних мережах;

- належної перевірки та реагування на скарги про кіберзнущання чи кіберзалицяння[91].

96. Дітей та молодих користувачів також варто інформувати про ризики втручання в їхнє фізичне і мо
благополуччя, в тому числі про сексуальну експлуатацію та насильство у віртуальному середовищі, ш
особливого захисту. Про це йдеться в Ланцаротській конвенції Ради Європи і відповідній практиці Су
на держави покладається позитивне зобов'язання забезпечувати захист дітей в Інтернеті[92].

97. Відповідно до Ланцаротської конвенції діти повинні бути захищені від вербування, схиляння або
участі в порнографічних матеріалах, які розміщуються або пропонуються в Інтернеті (наприклад, із за
камер, чатів, онлайн-ігор)[93]. Вони також повинні бути захищені від домагань із використанням Інтерн
метою залучення до участі в сексуальних дійствах із дитиною (залицяння), яка відповідно до національ
не досягла юридичного віку статевої зрілості, або з метою створення дитячої порнографії[94].

98. Дітей потрібно заохочувати до участі в формуванні та втіленні державної політики, програм або ін
сфері боротьби з сексуальною експлуатацією та сексуальним насильством над дітьми в Інтернеті[95]. Їм
зручні та доступні для дитини засоби для повідомлення про факти сексуального насильства та експлу
також для подання скарг через інформаційні служби, такі як гарячі лінії телефонного або Інтернет-зв'
надавати консультації та підтримку з питань користування цими послугами з належною увагою до пи
анонімності[96].

Ефективні засоби правового захисту

99. Право на ефективний засіб правового захисту закріплене у статті 13 ЄКПЛ. Кожна особа, чиї прав
чи порушуються в Інтернеті, має право на ефективний засіб правового захисту.

100. Стаття 13 ЄКПЛ гарантує наявність на національному рівні засобу правового захисту, спрямован
реалізації по суті передбачених у ЄКПЛ прав і свобод незалежно від того, в якій формі вони можуть з
внутрішньому правопорядку. Це потребує забезпечення національного засобу правового захисту для р
скарги, поданої на основі ЄКПЛ, і для надання відповідної компенсації[97]. На держави-члени покладає
зобов'язання щодо невідкладного, ретельного і ефективного розслідування заяв про порушення прав
процедури повинні давати можливість компетентному органу приймати рішення по суті скарги про по
і не лише призначати санкції за будь-яке встановлене порушення, але також забезпечувати виконання
рішення[98].

101. Має бути створений національний орган, на який покладено завдання щодо прийняття рішень за
розгляду заяв про порушення прав, гарантованих ЄКПЛ[99]. Потрібно забезпечити окремий порядок, із
особа може подати скаргу на безпідставне затягування провадження у справі про визначення її прав[10
має бути судовий орган, головне, щоб він надавав гарантії незалежності та неупередженості. Водночас
повноваження та процесуальні гарантії повинні дозволяти йому встановлювати ефективність кожного
правового захисту[101].

102. Порядок роботи компетентного національного органу повинен дозволяти йому виконувати ефект
порушення. Він повинен дозволяти компетентному органу приймати рішення по суті скарги щодо пор
передбачених ЄКПЛ[102], призначати санкції за будь-яке порушення і давати потерпілій особі гарантії в
відповідного рішення[103]. Засіб правового захисту повинен бути ефективним на практиці й за законом
залежати від ступеня визначеності сприятливого для позивача результату[104]. Хоча жоден засіб правов
сам по собі повністю задовольнити вимоги статті 13, передбачена законодавством сукупність засобів
виконати це завдання[105].

103. Ефективні засоби правового захисту повинні бути в наявності, про них повинні знати, вони мають
надаватися за помірну плату і забезпечувати належне відшкодування. Ефективні засоби правового зах
отримати безпосередньо від провайдерів Інтернет-послуг (хоча вони можуть і не мати такого рівня не
відповідав би вимогам статті 13 ЄКПЛ), органів державної влади та (або) інших національних правоза
можливостей компенсації входять проведення розслідування, надання пояснення провайдером послуг
надання права відповісти на заяву, що вважається дифамаційною або образливою, відновлення створе
контенту, що був видалений провайдером Інтернет-послуг, а також відновлення доступу до Інтернету
користувача і відповідна компенсація.

104. У частині своїх позитивних зобов'язань щодо захисту осіб від порушення прав людини приватни
держави повинні вживати відповідних заходів, які забезпечать у разі вчинення подібних порушень мо
використання потерпілими судових і позасудових механізмів[106]. Керівні принципи ООН підприємниц
аспекті прав людини потребують від компаній запровадження таких механізмів подачі скарг, які були
прогнозованими (запроваджували чітку і зрозумілу процедуру із зазначенням строків на кожному ета
прозорість щодо типів процесів та наявних результатів, а також засобів моніторингу їхньої реалізації)
(доступ до джерела інформації, консультації та експертиза), прозорими та здатними забезпечити такі
захисту, що цілковито відповідали б міжнародним стандартам у сфері прав людини, що застосовують
конкретних осіб[107].

105. Інтернет-користувачам повинна бути надана чітка та прозора інформація щодо наявних засобів п
інформація повинна частиною умов користування та (або) надання послуг, інших інформаційних мате
провайдерами Інтернету/Інтернет-послуг. Інтернет-користувачам повинні бути надані практичні й дос
що дозволять їм звертатися до провайдерів Інтернету/Інтернет-послуг із проблемними питаннями. Во

можливість звертатися з запитами на інформацію і клопотаннями про компенсацію. Прикладом засоб
що може бути наданий Інтернет-користувачам, є лінії довіри або гарячі лінії, які створюють провайде
чи асоціації захисту споживачів, до яких можуть звертатися Інтернет-користувачі у разі порушення їх
інших осіб. Консультації можуть надавати органи державної влади та (або) інші національні правозах
(омбудсмени), органи захисту даних, регулятори електронного зв'язку, громадські консультативні ор
асоціації чи асоціації цифрових прав або організації споживачів.

106. Інтернет-користувачі повинні бути захищені від кіберзлочинності. Держави, що підписали Будап
взяли на себе зобов'язання захищати громадян від кримінальної діяльності й злочинів у Інтернеті. Інт
цілком обґрунтовано можуть розраховувати на захист від кримінальної діяльності або кримінальних з
вчиняються в Інтернеті або з використанням Інтернету.

107. У центрі уваги перебувають злочини проти конфіденційності та цілісності комп'ютерних даних і
злочини, пов'язані з комп'ютерами. Тут не розглядаються злочини, пов'язані з контентом (дитяча пор
порушення авторських прав), оскільки вважається, що вони частково розглядаються в тих частинах П
присвячені правам дітей. Захист правовласників розглядається як такий, що стосується інтересів цієї к
не інтересів Інтернет-користувачів. Питання перехоплення і спостереження за повідомленнями також
розділі про приватне життя і захист даних.

108. Інтернет-користувачі мають законний інтерес у безперешкодному управлінні, функціонуванні та
комп'ютерними системами. Вони повинні бути захищені від незаконного доступу до комп'ютерних с
їх окремих частин, включаючи апаратну частину, компоненти, дані, що зберігаються, та встановлену
директорію, трафік і пов'язані з контентом дані. Це також передбачає захист від несанкціонованого вт
комп'ютерні системи і дані (хакерство, злом або інші форми вторгнення в комп'ютер), яке може ство
для користувачів систем в Інтернеті і для використання даних, таких як доступ до конфіденційних дан
інформація, таємниці тощо)[108].

109. Інтернет-користувачі повинні бути захищені від втручання в комп'ютерні дані, зокрема, від вико
кодів (наприклад, вірусів і троянських програм)[109]. Вони також повинні бути захищені від втручання
комп'ютерних або телекомунікаційних систем шляхом внесення, передачі, пошкодження, видалення,
знищення комп'ютерних даних[110], наприклад, програм, що викликають атаки «відмова в обслуговуван
кодів, таких як віруси, які перешкоджають або значно сповільнюють роботу системи чи програми, що
обсяги електронних листів отримувачу з метою блокування комунікаційних функцій системи (спам).
адміністративним чи кримінальним правопорушенням – залежить від національного законодавства.

110. Інтернет-користувачі повинні бути захищені від комп'ютерного шахрайства, пов'язаного з несан
створенням або зміною даних таким чином, що вони набувають нової доказової сили у ході юридичн
ґрунтуються на автентичності інформації, що міститься в даних[111].

111. Інтернет-користувачі мають законний інтерес щодо захисту активів, які надаються або управляю
системах (електронні фонди, депозити). Вони повинні бути захищені від шахрайських комп'ютерних
завдають пряму економічну або майнову шкоду майну Інтернет-користувача (гроші, матеріальні та не
що мають економічну цінність), як, наприклад, шахрайство з кредитними картками[112].

112. Будь-які заходи безпеки, спрямовані на захист Інтернет-користувачів від кіберзлочинності, повин
відповідати стандартам ЄКПЛ і, зокрема, вимогам щодо права на приватне і сімейне життя та права н
поглядів[113].

113. Інтернет-користувачі мають право на справедливий суд, закріплений статтею 6 ЄКПЛ. Це передб
громадянських прав і обов'язків або кримінальної відповідальності у зв'язку з діяльністю Інтернет-ко

це стосується ключових принципів, проголошених Судом, а саме: права на справедливий та публічни
розумні строки незалежним і неупередженим судом; права на звернення до суду, остаточне вирішенн
обґрунтоване судове рішення і його виконання; права на змагальне провадження в суді та рівні можл

114. Суд у справах, не пов'язаних з Інтернетом, встановив загальні принципи щодо якості здійснення
(незалежність, неупередженість, компетентність суду), захисту прав сторін (справедливе слухання, рі
сторін, публічне слухання), а також щодо ефективного здійснення правосуддя (в розумні строки).

115. Інтернет-користувач має право звернутися до Суду з індивідуальною скаргою після вичерпання в
засобів правового захисту, що були доступними та чинними протягом шести місяців[114] із дати прийня
рішення.

[1] Цей Посібник є частиною Рекомендації, ухваленої Комітетом міністрів 47 держав-членів Ради Європ
інформацію про цей Посібник можна знайти у пояснювальному меморандумі до Рекомендації.

[2] Цьому документу присвоєно гриф «Для службового користування» до проходження експертизи в Ко

[3] Див. приклади з практики Європейського суду з прав людини, пов'язані з Інтернетом, у Бюлетені пр
жовтень 2013 року.

[4] Див. справу «Їлдирим проти Туреччини» (*Yildirim v. Turkey*), №3111/10, §54.

[5] Див. CM(2012)91.

[6] Див. справу «Озгюр Гюндем проти Туреччини» (*Özgür Gündem v. Turkey*), №23144/93, §42-46.

[7] Справа «К. U. проти Сполученого Королівства» (*K.U. v. UK*), №2872/02.

[8] Справа «Пей проти Сполученого Королівства» (*Pay v. UK*), №32792/05.

[9] Справа «Ферет проти Бельгії» (*Féret v. Belgium*), №15615/07.

[10] Справи «Лопез Остра проти Іспанії» (*López Ostra v. Spain*), №16798/90, §44-58; «Ташкін та ін. проти
and Others v. Turkey); «Фадєєва проти Російської Федерації» (*Fadeyeva v. the Russian Federation*). У сп
Мустафа і Тарзібачі проти Швеції» (*Khurshid Mustafa and Tarzibachi v. Sweden*), №23883/06, Суд встан
тлумачення національним судом приватного акту (договору) передбачає відповідальність держави-від
поширює захист за статтею 10 на обмеження, які встановлювалися приватними особами.

[11] Рекомендація CM/Rec(2007)16 Комітету міністрів державам-членам про заходи щодо підвищення ц
суспільної служби.

[12] Див. Декларацію Комітету міністрів про принципи управління Інтернетом, принцип 1 «Права люди
верховенство права».

[13] «Керівні принципи ООН підприємницької діяльності в аспекті прав людини: реалізація курсу ООН
засоби правового захисту» (A/HRC/17/31), ухвалені Резолюцією Ради з прав людини «Права людини,
корпорації та інші підприємства (A/HRC/RES/17/4). Зокрема, Керівними принципами передбачено, що
забезпечувати виконання вимог законів, які спрямовані на гарантування права людини або вимагають
підприємств поважати ці права, а також періодично здійснювати оцінку відповідності подібних закон
які прогалини; забезпечувати, щоб інші закони та нормативи, якими регулюється утворення та функці

підприємств, наприклад, корпоративне право, не обмежували, а гарантували дотримання у підприємн
прав людини; надавати ефективну підтримку, ефективні рекомендації приватним підприємствам із пи
людини в їхній діяльності; заохочувати і (де необхідно) вимагати від приватних підприємств інформу
вирішують питання впливу своєї діяльності на права людини.

[14] Спеціальний доповідач ООН із питання про право на свободу поглядів та їх вільне вираження Фран
що «Інтернет став необхідним інструментом для реалізації низки прав людини, боротьби з нерівністю
прискорення розвитку і людського прогресу, при цьому забезпечення доступу до Інтернету має стати
завданням для всіх держав. Кожна держава, виходячи з цього, повинна розробити конкретну та ефект
консультацій із представниками усіх верств суспільства, зокрема й із приватним сектором і відповідн
установами для того, щоб Інтернет був широко доступним, відкритим та надавався за помірну плату д
населення». «Будучи каталізатором для людей у здійсненні їхнього права на свободу слова і виражен
також забезпечує можливості для реалізації низки інших прав людини». Режим доступу до ресурсу:
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

[15] Див. вище, п. 2, §50. Див. також справу «Аутронік АГ» проти Швейцарії» (*Autronic AG v. Switzerlan*
справі «Хуршид Мустафа і Тарзібачі проти Швеції» (*Khurshid Mustafa and Tarzibachi v. Sweden*), №23
встановив, що тлумачення національним судом приватного акту (договору) передбачає відповідальніс
відповідача, що поширює захист за статтею 10 на обмеження, які встановлювалися приватними особа

[16] Див. вище, п. 2, §53.

[17] Див. вище, п. 9, CM/Rec(2007)16, розділ II.

[18] Див. вище, п. 2, §50.

[19] Декларація Комітету міністрів про мережеву нейтральність мережі, прийнята Комітетом міністрів 2
Див. також Директиву 2002/21/ЄС Європейського парламенту і Ради ЄС від 7 березня 2002 року про с
регулювання електронних комунікаційних мереж і послуг, стаття 8(4) g.

[20] Див. вище, п. 9, CM/Rec(2007)16, додаток, розділ II; Рекомендація №R(99)14 Комітету міністрів дер
універсальну суспільну службу, що стосується нових комунікаційних та інформаційних послуг, прин

[21] Там само.

[22] Див. вище, п. 9, CM/Rec(2007)16, додаток, розділ II.

[23] Див. вище, п. 2, §50.

[24] Справа «Хендісайд проти Сполученого Королівства» (*Handyside v. UK*), рішення від 7 грудня 1976 р
п. 49.

[25] Справи «Шові та інші» (*Chauvy and Others*), №64915/01, §70; «Пфайфер проти Австрії» (*Pfeifer v. Au*
§35; «Поланко Торрес і Мовілла Поланко проти Іспанії» (*Polanco Torres and Movilla Polanco v. Spain*),

[26] Справи «Делфі АС» проти Естонії» (*Delfi AS v. Estonia*), №64569/09, §78-81 (цю справу передано на
палати Суду); «Аксель Шпрінгер АГ» проти Німеччини» (*Axel Springer AG v. Germany*), №39954/08, §
Ганновер проти Німеччини» (*Von Hannover v. Germany*) (№2), №40660/08 і 60641/08, §108-113.

[27] Справи «Ферет проти Бельгії» (*Féret v. Belgium*), №15615/07; «Гароді проти Франції» (*Garaudy v. Fr*

24.06.2003, рішення про прийнятність; «Лерой проти Франції» (*Leroy v. France*), №36109/03; «Єрсілд
v. Denmark), №15890/89; «Вейделанд та інші проти Швеції» (*Vejdeland and Others v. Sweden*), №1813/0

[28] Рекомендація №R(97)20 Комітету міністрів державам-членам щодо розпалювання ненависті.

[29] Справа «Ней та Сунде Колмісоппі проти Швеції» (*Neij and Sunde Kolmisoppi v. Sweden*), №40397/12;
Доналд та інші проти Франції» (*Ashby Donald and others v. France*), №36769/08, §34.

[30] Там само.

[31] Див. вище, п. 9, CM/Rec(2007)16, додаток, розділ III, абзац 2.

[32] Справа «Об'єднання «Ферайн геген Тьерфабрікен» проти Швейцарії» (*VgT Verein gegen Tierfabriker*
№24699/94, §45.

[33] Справи «Хуршид Мустафа і Тарзібачі проти Швеції» (*Khurshid Mustafa and Tarzibachi v. Sweden*), №
і П'юнсерно проти Андорри» (*Plaand Puncernau v. Andorra*), №69498/01, §59, ЄКПЛ 2004-VIII.

[34] Див. вище, п. 2, §64.

[35] Там само, §66-70.

[36] Рекомендація CM/Rec(2008)6 Комітету міністрів державам-членам про заходи щодо розвитку повагі
вираження поглядів та інформації у зв'язку з Інтернет-фільтрами, див. додаток, ч. III, ii; див. також ви

[37] Там само, CM/Rec(2008)6, див. додаток, ч. III, iv.

[38] Там само.

[39] Див. вище, п. 2, §52, 66-68; див. також Декларацію Комітету міністрів про свободу спілкування в Ін

[40] Там само, п. 2 вище, §64; справа «Об'єднання «Екін» проти Франції» (*Association Ekin v. France*), №

[41] Там само, п. 2 вище, §64-66.

[42] Див. Декларацію Комітету міністрів про свободу спілкування в Інтернеті, принцип 3.

[43] Див. Рекомендацію CM/Rec(2012)3 Комітету міністрів державам-членам про захист прав людини у
пошуковими системами, додаток, ч. III.

[44] Див. п. 34 вище; CM/Rec(2008)6, див. додаток, ч. I; там само, CM/Rec(2012)3, додаток, ч. III.

[45] Рекомендація CM/Rec (2011)7 Комітету міністрів державам-членам про нове поняття ЗМІ, §7, додат
Рекомендація CM/Rec(2012)4 Комітету міністрів державам-членам про захист прав людини у зв'язку
соціальних мереж, §3.

[46] Там само, CM/Rec(2011)7, §91.

[47] Там само, CM/Rec(2012)4, II/10.

[48] Там само, CM/Rec(2011)7, §18, 30-31.

[49] Там само, CM/Rec(2011)7, §7, абзац 2.

[50] Див. «Деактивація облікового запису та видалення контенту: Керівні принципи та практика для ком
користувачів», автори: Еріка Ньюланд, Каролін Нолан, Синтія Вонг, Джиліан Йорк. Режим доступу д
http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_

[51] Справа «K. U. проти Фінляндії» (*K.U. v. Finland*), №2872/02, §49.

[52] Будапештська конвенція про кіберзлочинність, ст. 2, пояснювальна доповідь, §62.

[53] Див. Декларацію про свободу спілкування в Інтернеті, принцип 7.

[54] Справа «Вінгроув проти Сполученого Королівства» (*Wingrove v. UK*), 25 листопада 1996 р., §58, про

[55] Див. п. 9 вище, CM/Rec(2007)16, додаток, ч. I.

[56] Справа «Класс та інші проти Німеччини» (*Klass and Others v. Germany*), №5029/71, §41.

[57] Справи «Фон Ганновер проти Німеччини» (*Von Hannover v. Germany*) (№2), №40660/08 і 60641/08, §
проти Італії» (*Sciacca v. Italy*), №50774/99, §29.

[58] Справи «Ротару проти Румунії» (*Rotaru v. Romania*), №28341/95; «P.G. and J.H. проти Сполученого К
and J.H. v. UK), №44787/98; «Пек проти Сполученого Королівства» (*Peck v. UK*), №44647/98; «Перрі п
Королівства» (*Perry v. UK*), №63737/00; «Аманн проти Швейцарії» (*Amann v. Switzerland*), №27798/95

[59] Див. Конвенцію 108, ст. 2.

[60] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS №108).

[61] Консультативний комітет Конвенції про захист осіб у зв'язку з автоматизованою обробкою персона
№108) надав низку пропозицій щодо модернізації цієї Конвенції (T-PD(2012)4Rev3_en). Одна з пропо
згоди особи, персональні дані якої обробляються, у якості передумови такої обробки: «Кожна Сторон
обробку даних на засадах вільної, конкретної, інформованої та [чіткої, однозначної] згоди суб'єкта да
передбачених законодавством підстав».

[62] Рекомендація CM/Rec(2010)13 Комітету міністрів державам-членам про захист осіб у зв'язку з авто
обробкою персональних даних у контексті профілювання, розділ 5.

[63] Конвенція 108, ст. 8.

[64] Див. п. 60 вище, ст. 8.

[65] Див. CM/Rec(2012)3, зокрема, додаток, ч. II.

[66] Там само.

[67] Рекомендація CM/Rec(2010)13 Комітету міністрів державам-членам про захист осіб у зв'язку з авто

обробкою персональних даних у контексті профілювання, розділ 5.

[68] Конвенція 108, ст. 9.

[69] Див. пояснювальну доповідь до Будапештської конвенції, п. 53.

[70] Справи «Асоціація за євроінтеграцію і права людини та Екміджиєв проти Болгарії» (*Association for E and Human Rights and Ekmidzhiev v. Bulgaria*), №62540/00, §58; «Класс та інші проти Німеччини» (*Klas Germany*), №5029/71; «Малоун проти Сполученого Королівства» (*Malone v. UK*), №8691/79; «Вебер і С Німеччини» (*Weber and Saravia v. Germany*), №54934/00.

[71] Див. справу «Копленд проти Сполученого Королівства» (*Copland v. UK*), №62617/00.

[72] Справи «Класс та інші проти Німеччини» (*Klass and Others v. Germany*), №5029/71, §30-38; «Малоун Королівства» (*Malone v. UK*), №8691/79, §64; «Вебер і Саравія проти Німеччини» (*Weber and Saravia v* №54934/00, §78-79, «Асоціація за євроінтеграцію і права людини та Екміджиєв проти Болгарії» (*Assoc Integration and Human Rights and Ekmidzhiev v. Bulgaria*), №62540/00, §58, 69-70.

[73] Справи «Малоун проти Сполученого Королівства» (*Malone v. UK*), №8691/79, §67; «Валенсуела Кон (*Valenzuela Contreras v. Spain*), рішення від 30 липня 1998 року, звіти 1998-V, с. 1925, §46 (iii); «Хан п Королівства» (*Khan v. UK*), №35394/97, §26; «Асоціація за євроінтеграцію і права людини та Екміджи (*Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria*), №62540/00, §71.

[74] Див. справи «Круслін проти Франції» (*Kruslin v. France*), №11801/85, §33; «Ювіг проти Франції» (*H* №11105/84, §32; «Аманн проти Швейцарії» (*Amann v. Switzerland*), №/95, §56; «Вебер і Саравія проти *and Saravia v. Germany*), №54934/00, §93; «Асоціація за євроінтеграцію і права людини та Екміджиєв (*Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria*), №62540/00, §76.

[75] Там само, №62540/00), §77.

[76] Справа «Копленд проти Сполученого Королівства» (*Copland v. UK*), №62617/00, §41-42.

[77] Див. також п. 8 вище, CM/Rec(2007)16, розділ IV.

[78] Там само.

[79] Декларація Комітету міністрів про права людини і верховенство права в інформаційному суспільств доопрацьована 13 травня 2005 року.

[80] Там само.

[81] Рекомендація CM/Rec(2012)2 Комітету міністрів державам-членам щодо участі дітей і молоді віком

[82] Там само.

[83] Див. Рекомендацію CMRec(2011)12 Комітету міністрів державам-членам про права дітей та соціаль адаптовані для дітей і сімей; Керівні принципи Ради Європи про правосуддя, адаптовані для дітей.

[84] Рекомендація Rec(2006)12 Комітету міністрів щодо створення можливостей для дітей у новому інф

комунікаційному середовищі.

[85] Справа «К. U. проти Фінляндії» (*K.U. v. Finland*), №2872/02, §40-41.

[86] Справи «X та Y проти Нідерландів» (*X and Y v. the Netherlands*), §23-24 і 27; «Огест проти Сполучен (*August v. UK*), №36505/02; «M.C. проти Болгарії» (*M.C. v. Bulgaria*), №39272/98, §150; «К. U. проти Ф *Finland*), №2872/02, §46.

[87] Декларація Комітету міністрів про захист гідності, безпеки та приватного життя дітей в Інтернеті.

[88] Там само.

[89] Рекомендація CM/Rec(2009)5 Комітету міністрів державам-членам про заходи захисту дітей від шкі поведінки і сприяння їхній активній участі в новому інформаційному та комунікаційному середовищі

[90] Див. CM/Rec(2012)4, додаток, II, §10.

[91] Там само.

[92] Справа «К. U. проти Фінляндії» (*K.U. v. Finland*), №2872/02.

[93] Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства С див. також пояснювальну доповідь до цих статей.

[94] Там само, ст. 23.

[95] Там само, ст. 9/1.

[96] Там само, ст. 13; див. також Рекомендацію CM/Rec(2011)12 Комітету міністрів державам-членам пр соціальні послуги, адаптовані для дітей і їхніх сімей; Керівні принципи Ради Європи про правосуддя, дітей.

[97] Справа «Кая проти Туреччини» (*Kaya v. Turkey*), №22729/93, §106.

[98] Справа «Сміт і Грейді проти Сполученого Королівства» (*Smith and Grady v. UK*), №33985/96, 33986/

[99] Справи «Сілвер та інші проти Сполученого Королівства» (*Silver and Others v. UK*), №5947/72, 6205/ 7107/75, 7113/75, 7136/75, §113; «Кая проти Туреччини» (*Kaya v. Turkey*), №22729/93, §106.

[100] Справа «Кудла проти Польщі» (*Kudla v. Poland*), №30210/96, §157.

[101] Справи «Сілвер та інші проти Сполученого Королівства» (*Silver and Others v. UK*), №5947/72, 6205 7107/75, 7113/75, 7136/75, §113; «Кая проти Туреччини» (*Kaya v. Turkey*), №22729/93, §106.

[102] Справа «Сміт і Грейді проти Сполученого Королівства» (*Smith and Grady v. UK*), №33985/96, 33986

[103] Справа «Іатрідіс проти Греції» (*Iatridis v. Greece*), №31107/96, §60.

[104] Справа «Кудла проти Польщі» (*Kudla v. Poland*), №30210/96, §158.

[105] Справи «Сілвер та інші проти Сполученого Королівства» (*Silver and Others v. UK*), №5947/72, 6205/
7107/75, 7113/75, 7136/75, §113; «Кудла проти Польщі» (*Kudla v. Poland*), №30210/96, §157.

[106] Питання корпоративної соціальної відповідальності і позитивних зобов'язань держав щодо захисту
роз'яснюються в п.19 і 28 Пояснювального меморандуму.

[107] Див. «Керівні принципи ООН підприємницької діяльності в аспекті прав людини: реалізація курсу
повагу і засоби правового захисту» (A/HRC/17/31), ухвалені Резолюцією Ради з прав людини «Права
транснаціональні корпорації та інші підприємства (A/HRC/RES/17/4), гл. III, принципи 28-31.

[108] Будапештська конвенція про кіберзлочинність, ст. 2, Пояснювальна доповідь, §44-50.

[109] Там само, ст. 4, Пояснювальна доповідь, §60-61.

[110] Там само, ст. 5, Пояснювальна доповідь, §65-69.

[111] Там само, ст. 7, Пояснювальна доповідь, §81.

[112] Там само, ст. 8, Пояснювальна доповідь, §86-88.

[113] Там само, ст. 15.

[114] Після набуття чинності Протоколу №15 до ЄКПЛ цей строк буде складати чотири місяці.