

**ПОСІБНИК З ПРАВ ЛЮДИНИ  
ДЛЯ ІНТЕРНЕТ-КОРИСТУВАЧІВ**  
та Пояснювальний меморандум

Рекомендація CM/Rec(2014)6 Ко-  
мітету міністрів Ради Європи  
державам-членам щодо Посіб-  
ника з прав людини для інтернет-  
користувачів та пояснювальний  
меморандум

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE



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

Фінансується  
Європейським Союзом  
та Радою Європи



EUROPEAN UNION

COUNCIL OF EUROPE



CONCEIL DE L'EUROPE

Впроваджується  
Радою Європи

# ПОСІБНИК З ПРАВ ЛЮДИНИ ДЛЯ ІНТЕРНЕТ-КОРИСТУВАЧІВ ТА ПОЯСНЮВАЛЬНИЙ МЕМОРАНДУМ

(Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний меморандум)

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

Посібник з прав людини для Інтернет-користувачів та пояснювальний меморандум (Рекомендація CM/Rec(2014)6 Комітету міністрів країнам-членам щодо посібника з прав людини для Інтернет-користувачів – пояснювальний меморандум). Перекладено українською мовою за виданням Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum – К. : Інжиніринг, 2015. — 56 с.

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

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

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

**Контактна інформація**  
04070, м. Київ, вул. Іллінська, 8,  
бізнес-центр «Іллінський»,  
8-й під'їзд, 5-й поверх  
Тел.: +38 044 3399210

**Автор і видавець оригіналу – Рада Європи**

**Видавець:** ТОВ «Інжиніринг»

**Друк:** ФОП Лесін М. В.

**Наклад:** 400 екз.

<b>ПОСІБНИК З ПРАВ ЛЮДИНИ ДЛЯ ІНТЕРНЕТ-КОРИСТУВАЧІВ .....</b>	<b>4</b>
(Рекомендація CM/REC(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для інтернет-користувачів)	
Вступ .....	6
Доступ і недискримінація .....	7
Свобода вираження поглядів та інформації .....	8
Зібрання, об'єднання та участь .....	9
Приватне життя і захист даних .....	10
Освіта та грамотність .....	11
Діти і молодь .....	11
Ефективні засоби правового захисту .....	12
<b>ПОЯСНЮВАЛЬНИЙ МЕМОРАНДУМ ДО ПОСІБНИКА З ПРАВ ЛЮДИНИ ДЛЯ ІНТЕРНЕТ-КОРИСТУВАЧІВ .....</b>	<b>14</b>
(Керівний комітет із питань ЗМІ та інформаційного суспільства (CDMSI): Рекомендація CM/REC(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для інтернет-користувачів – пояснювальний меморандум)	

# РЕКОМЕНДАЦІЯ СМ/РЕС(2014)6 КОМІТЕТУ МІНІСТРІВ РАДИ ЄВРОПИ ДЕРЖАВАМ- ЧЛЕНАМ ЩОДО ПОСІБНИКА З ПРАВ ЛЮДИНИ ДЛЯ ІНТЕРНЕТ-КОРИСТУВАЧІВ

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

1. Держави-члени Ради Європи зобов'язані забезпечити кожному, хто знаходиться в межах їхньої юрисдикції, права та основоположні свободи, закріплені Європейською конвенцією про захист прав людини (ЗДРЄ №5, Конвенція). Дія цього зобов'язання поширюється й на сферу використання мережі Інтернет. Ці питання врегульовано також іншими конвенціями та документами Ради Європи, якими передбачено захист права на свободу вираження поглядів, доступу до інформації, права на свободу зібрань, захист від кіберзлочинності, а також захист права на приватне життя та захист персональних даних.
2. До зобов'язань держав поважати, захищати та підтримувати права людини належить і нагляд за приватними компаніями. Права людини, які є універсальними та неподільними, а також пов'язані з ними стандарти, мають переважну силу перед загальними вимогами та умовами, що висуваються до Інтернет-користувачів будь-якими суб'єктами приватного сектора.
3. Інтернет є суспільно важливим ресурсом. Люди, спільноти, органи державної влади та приватні компанії здійснюють свою діяльність через Інтернет і законно сподіваються на те, що матимуть доступ до Інтернет-послуг, які будуть надаватися без будь-якої дискримінації, за розумну ціну, а також будуть безпечними, надійними та безперебійними. Крім того, ніхто не повинен підлягати неправомірному, безпідставному або неспівмірному втручанням в реалізацію своїх прав та основоположних свобод при користуванні Інтернетом.
4. Користувачі повинні отримувати підтримку для розуміння та ефективною реалізації ними прав людини в режимі онлайн у разі обмеження або порушення їхніх прав та свобод. Така підтримка повинна включати рекомендації про доступ до ефективних засобів правового захисту. Зважаючи на можливості,

які надає Інтернет для забезпечення прозорості та підзвітності в управлінні державними справами, користувачі повинні мати можливість використовувати Інтернет для участі в демократичному житті.

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

- 5.1.** активно поширювати Посібник з прав людини для Інтернет-користувачів, як це передбачено в Додатку, серед громадян, органів державної влади, суб'єктів приватного сектора та здійснювати конкретні заходи, спрямовані на його застосування, з метою забезпечення реалізації користувачами в повному обсязі своїх прав і основоположних свобод в Інтернеті;
- 5.2.** здійснювати оцінку, періодично переглядати та при необхідності знімати обмеження щодо реалізації прав та свобод в Інтернеті, зокрема у тих випадках, коли вони не відповідають вимогам Конвенції та практиці її застосування Європейським судом з прав людини. Будь-яке обмеження повинно бути передбачене законом, бути необхідним у демократичному суспільстві, мати законну мету, а також бути пропорційним законній меті;
- 5.3.** забезпечувати доступ Інтернет-користувачів до ефективних засобів правового захисту у разі обмеження їхніх прав і свобод або коли вони вважають, що їхні права були порушені. Це потребує поглиблення координації та співпраці між відповідними установами, організаціями та спільнотами. Це також передбачає залучення та ефективну співпрацю з суб'єктами приватного сектора та організаціями громадянського суспільства. Залежно від держави можуть передбачатися механізми відшкодування, забезпечені органами захисту даних, національними правозахисними органами (наприклад, омбудсменами), а також через застосування судових процедур та гарячих ліній;
- 5.4.** розвивати співпрацю з іншими державними і недержавними структурами всередині Ради Європи та поза її межами щодо стандартів і процедур, які мають вплив на захист прав людини й основоположних свобод в Інтернеті;

- 5.5.** заохочувати приватний сектор до повноцінного діалогу з відповідними органами державної влади і громадянським суспільством із питань корпоративної соціальної відповідальності, зокрема, прозорості та підзвітності в своїй діяльності згідно з вимогами «Керівних принципів підприємницької діяльності в аспекті прав людини: реалізуючи курс ООН «Захист, повага і засоби правового захисту». Приватний сектор потрібно заохочувати до сприяння поширенню цього Посібника;
- 5.6.** заохочувати громадянське суспільство до підтримки поширення і застосування Посібника таким чином, щоб воно 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 вас із вашими правами в Інтернеті, їх можливими обмеженнями та доступними засобами правового захисту у випадку таких обмежень. Права людини та основоположні свободи повинні однаковою мірою забезпечуватися в офлайн та онлайн. Цей принцип передбачає повагу до прав і свобод інших Інтернет-користувачів. Посібник надає вам інформацію про те, що на практиці означають права і свободи в контексті використання Інтернету, як ними користуватися, діяти відповідно до них, а також як отримати доступ до засобів правового захисту. Робота над цим документом не припиняється; він залишається відкритим для періодичного оновлення.
- 2.** В основу цього Посібника покладено Європейську конвенцію про захист прав людини, а також інші конвенції та документи Ради Європи, в яких розглянуто різні аспекти захисту прав людини. Всі держави-члени Ради Європи зобов'язані поважати, захищати і забезпечувати дотримання прав і свобод, закріплених у ратифікованих ними документах. У Посібнику також враховано безперервне тлумачення цих прав і свобод Європейським судом з прав людини та у відповідних правових документах Ради Європи.



3. Посібник не запроваджує нові права та основоположні свободи. У ньому викладено чинні стандарти прав людини та механізми їх забезпечення<sup>1</sup>.

## Доступ і недискримінація

1. Доступ до Інтернету – це важливий засіб для реалізації вами своїх прав та свобод, а також для участі в демократичних процесах. Саме тому позбавити вас доступу до Інтернету проти вашої волі можуть лише за рішенням суду. В окремих випадках надання послуг може також припинятися за умовами договору, але це має відбуватися лише після того, як були вичерпані всі інші засоби.
2. Ваш доступ має надаватися за розумну ціну і бути недискримінаційним. Ви повинні мати якомога ширший доступ до 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, спрямованих на сприяння вашому доступу до Інтернету, якщо ви проживаєте у сільській місцевості та географічно віддалених районах, а також якщо ви належите до малозабезпечених верств населення та (або) осіб з особливими потребами чи інвалідністю.
4. При взаємодії з органами державної влади, провайдерами мережі Інтернет та провайдерами Інтернет-контенту чи послуг, а також з іншими користувачами або групами користувачів ви не можете бути об'єктом дискримінації за будь-якими ознаками, такими як стать, раса, колір шкіри, мова, релігія або віра, політичні чи інші переконання, національність або соціальне походження, належність до національної меншини, майновий стан, походження чи будь-який інший статус, зокрема, за етнічною приналежністю, віком або сексуальною орієнтацією.

<sup>1</sup>Цей Посібник є частиною Рекомендації, ухваленої Комітетом міністрів 47 держав-членів Ради Європи. Більш докладну інформацію про цей Посібник можна знайти у пояснювальному меморандумі до Рекомендації.

## Свобода вираження поглядів та інформації

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

- 1.** ви можете вільно висловлюватися в Інтернеті та мати доступ до інформації, поглядів і висловлювань інших осіб. До них належать як політичні заяви, релігійні переконання, погляди і висловлювання, що сприймаються прихильно або вважаються необразливими, так і такі, що можуть завдавати образу, шокувати або виводити інших осіб зі стану рівноваги. Ви повинні приділяти належну увагу репутації та правам інших осіб, зокрема їхньому праву на приватне життя;
- 2.** обмеження можуть накладатися на такі висловлювання, в яких містяться заклики до дискримінації, ненависті або насильства. Такі обмеження повинні бути правомірними, цілеспрямованими і запроваджуватися під контролем суду;
- 3.** ви можете вільно створювати, повторно використовувати і поширювати Інтернет-контент із повагою до права на захист інтелектуальної власності, в тому числі авторського права;
- 4.** органи державної влади зобов'язані поважати і захищати вашу свободу вираження поглядів та свободу інформації. Будь-які обмеження цієї свободи не повинні бути свавільними та мають переслідувати законну мету згідно з вимогами Європейської конвенції про захист прав людини, таку як, зокрема, захист національної безпеки або громадського порядку, охорона здоров'я населення чи моралі, а також відповідати законодавству у сфері прав людини. Крім того, ви повинні бути ознайомлені з такими обмеженнями, а також проінформовані про те, як отримати консультацію та компенсацію; обсяг 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 поважати ваші права та забезпечувати механізми розгляду ваших скарг. Водночас ви маєте знати, що провайдери Інтер-

нет-послуг, такі як соціальні мережі, можуть обмежувати окремі види контенту і поведінки у зв'язку з їхньою політикою щодо контенту. Вам повинні повідомляти про можливі обмеження для того, щоб ви могли прийняти свідоме рішення щодо того, чи варто користуватися такою послугою. Це передбачає надання конкретної інформації про те, що саме провайдер Інтернет-послуги вважає незаконним чи неналежним контентом і поведінкою при користуванні послугою, а також способами реагування провайдера;

6. ви можете вирішити не розкривати свою особу в Інтернеті, наприклад, скористатися псевдонімом. Однак ви маєте 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, що:

1. ви можете вільно обирати будь-який сайт, додаток чи будь-яку іншу послугу з метою створення груп, приєднання, мобілізації та участі в будь-якій соціальній групі та об'єднанні незалежно від їхнього офіційного визнання з боку органів державної влади. Ви також повинні мати можливість використовувати Інтернет для реалізації свого права на створення профспілок та приєднання до них;
2. ви маєте право на мирний протест в Інтернеті. Однак ви повинні знати: якщо ваш онлайн-протест призведе до блокування, перебоїв у наданні послуг та (або) завдасть шкоди майну інших осіб, ви можете зіткнутися з юридичними наслідками;
3. ви можете вільно користуватися доступними онлайн-можливостями для участі в місцевих, національних і глобальних публічних політичних дебатах, законодавчих ініціативах, контролі за прийняттям рішень, зокрема, ви маєте 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 даних і повага до конфіденційності вашої кореспонденції і спілкування. Це означає, що:

1. вам потрібно знати, що при користуванні Інтернетом ваші персональні дані регулярно обробляються. Це відбувається при використанні вами браузерів, електронної пошти, миттєвих повідомлень, передачі голосових повідомлень через Інтернет-протоколи, соціальних мереж, пошукових систем, а також хмарних сервісів для зберігання даних;
2. при обробці ваших персональних даних органи державної влади і приватні компанії зобов'язані дотримуватися певних правил та процедур;
3. ваші персональні дані повинні оброблятися лише у передбачених законом випадках або за умови надання вами згоди. Вам повинні повідомляти про те, які саме ваші персональні дані обробляються та (або) передаються третім сторонам, а також про те, коли, ким та з якою метою здійснюється така обробка. В цілому ви повинні мати можливість здійснювати контроль за своїми персональними даними (перевіряти їх правильність, звертатися з проханням про виправлення, видалення персональних даних або про їх зберігання лише протягом необхідного строку);
4. на вас не повинні поширюватися заходи загального спостереження чи перехоплення інформації. Втручання у ваше приватне життя щодо ваших персональних даних дозволяється лише за виняткових обставин, передбачених законом, наприклад, у разі здійснення кримінального розслідування. Вам повинна надаватися доступна, чітка та точна інформація 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 приватної електронної кореспонденції та спілкування. Ваш роботодавець повинен повідомляти вас про будь-які заходи спостереження та (або) моніторингу;
6. вам можуть надавати допомогу органи захисту даних, які функціонують у більшості європейських держав та 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 контенту державною мовою. Умови такого доступу можуть передбачати винагороду правовласників за їхню роботу. Ви також повинні мати можливість вільного доступу до наукових і культурних здобутків у Інтернеті, що фінансуються державою і перебувають у відкритому доступі в Інтернеті, де це можливо;
2. у частині Інтернет- і медіаграмотності ви повинні мати доступ до інтерактивної освіти і знань для того, щоб користуватися своїми правами та свободами в Інтернеті. Сюди входять уміння, необхідні для розуміння, користування та роботи з широким спектром інструментів Інтернету. Це має навчити вас критично оцінювати точність та достовірність 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. Зокрема, з урахуванням вашого віку ви маєте право на особливий захист і консультування при користуванні Інтернетом. Це означає, що:

1. ви маєте право на вільне вираження своїх поглядів та участь у житті суспільства, на те, щоб бути почутими та вносити свій вклад у вирішення питань, які торкаються ваших інтересів. Вашим поглядам повинна приділятися належна увага з урахуванням вашого віку, ступеня зрілості та без дискримінації;
2. ви можете очікувати на отримання інформації мовою, що відповідає вашому віку, а також на навчання безпечному користуванню Інтернетом, в тому числі щодо захисту вашого приватного життя, з боку ваших вчителів, вихователів, батьків чи опікунів;

3. ви повинні знати, що контент, який ви створюєте в Інтернеті, або контент про вас, що створюється іншими Інтернет-користувачами, може ставати доступним у будь-якому куточку світу і завдавати шкоду вашій гідності, безпеці, приватному життю або іншим чином шкодити вам та вашим правам у цей час або на наступних етапах вашого життя. На ваш запит такий контент повинен бути вилучений або видалений протягом розумно короткого періоду часу;
4. ви можете очікувати на отримання чіткої інформації про те, який онлайн-контент та поведінка є незаконними (наприклад, домагання в Інтернеті), а також мати можливість повідомити про потенційно незаконний контент. Така інформація має бути адаптована до вашого віку та обставин, а також вам повинні надати поради та підтримку з належною повагою до вашої конфіденційності та анонімності;
5. вам повинен надаватися спеціальний захист від втручання у ваше фізичне, психічне та моральне благополуччя, зокрема, захист від сексуальної експлуатації та насильства в Інтернеті та від інших форм кіберзлочинності. Крім того, ви маєте 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 прав і основоположних свобод. Для отримання правового захисту ви не обов'язково маєте одразу вдаватися до судових засобів. Можливості для звернення по правовий захист повинні бути доступними, відомими, надаватися за прийнятною ціною та здатними забезпечити належне відшкодування. Ефективні засоби правового захисту можна отримати безпосередньо від Інтернет-провайдерів, органів державної влади та (або) національних правозахисних органів. Залежно від порушення ефективним засобом правового захисту може бути розслідування, роз'яснення, відповідь, виправлення, вибачення, поновлення контенту, відновлення доступу та компенсація. На практиці це означає, що:

- 1.1.** ваш Інтернет-провайдер, провайдери доступу до Інтернет-контенту чи послуг або інша компанія та (або) орган державної влади повинні повідомити вас про ваші права, свободи, можливі засоби правового захисту та порядок їх отримання. Таке зобов'язання передбачає забезпечення вас легкодоступною інформацією про порядок повідомлення про втручання у ваші права, звернення з відповідною скаргою та відшкодування завданої шкоди;
  - 1.2.** додаткова інформація та рекомендації повинні надаватися органами державної влади, національними правозахисними органами (наприклад, омбудсменами), органами захисту даних, громадськими консультативними органами, правозахисними асоціаціями чи асоціаціями цифрових прав або організаціями споживачів;
  - 1.3.** органи державної влади зобов'язані захищати вас від кримінальної діяльності або кримінальних злочинів, що вчиняються в Інтернеті або з використанням Інтернету, зокрема, коли це стосується незаконного доступу, втручання, підробки або інших шахрайських маніпуляцій із вашими електронними персональними даними, комп'ютером та даними, які в ньому зберігаються. Відповідні правоохоронні органи зобов'язані розслідувати ці факти та вживати належні заходи, що передбачають застосування санкцій у разі отримання від вас скарги про завдання шкоди або втручання у ваші персональні дані та ваше майно в Інтернеті.
- 2.** При встановленні ваших прав та обов'язків або під час розгляду будь-якого кримінального обвинувачення проти вас, що стосується Інтернету:
- 2.1.** ви маєте право на справедливий судовий розгляд протягом розумного строку незалежним та неупередженим судом;
  - 2.2.** ви маєте право на індивідуальну скаргу до Європейського суду з прав людини після вичерпання всіх існуючих національних засобів правового захисту.

# РЕКОМЕНДАЦІЯ СМ/РЕС(2014)6 КОМІТЕТУ МІНІСТРІВ ДЕРЖАВАМ-ЧЛЕНАМ ЩОДО ПОСІБНИКА З ПРАВ ЛЮДИНИ ДЛЯ ІНТЕРНЕТ- КОРИСТУВАЧІВ – ПОЯСНЮВАЛЬНИЙ МЕМОРАНДУМ

Постійні представники міністрів

Документи КМ

СМ(2014)31 addfinal 16 квітня 2014 р.

**1197-е засідання, 16 квітня 2014 року<sup>2</sup>**

5 ЗМІ

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

в. Рекомендація СМ/Рес(2014)6 Комітету міністрів державам-членам щодо використання посібника з прав людини для Інтернет-користувачів – пояснювальний меморандум

## **Вступ**

1. Інтернет відіграє важливу роль у повсякденному житті людей та у всіх аспектах життя суспільства. Він постійно розвивається і забезпечує громадянам можливість доступу до інформації та послуг, зв'язку та спілкування, а також обміну думками та знаннями на глобальному рівні. Крім того, зростає вплив Інтернету на соціальну, економічну та культурну сфери діяльності.
2. Європейський суд з прав людини (надалі – «Суд<sup>3</sup>») розглядає дедалі більше справ, пов'язаних з Інтернетом. Суд заявляє, що «наразі Інтернет став одним із основних засобів реалізації громадянами свого права на свободу вираження поглядів та інформації, забезпечуючи їх таким чином необхідними механізмами для участі в діяльності та обговореннях політичних питань та питань, що становлять загальний інтерес»<sup>4</sup>.

<sup>2</sup>Цьому документу присвоєно гриф «Для службового користування» до проходження експертизи в Комітеті міністрів.

<sup>3</sup>Див. приклади з практики Європейського суду з прав людини, пов'язані з Інтернетом, у Бюлетені про нові технології за жовтень 2013 року.

<sup>4</sup>Див. справу «Ілдірим проти Туреччини» (Yildirim v. Turkey), №3111/10, §54.



3. У Стратегії Ради Європи щодо управління Інтернетом на 2012-2015 рр. велике значення надається правам Інтернет-користувачів. У главі «Максимальне забезпечення прав і свобод Інтернет-користувачів», спрямованій на покращення доступу до Інтернету та його найоптимальніше використання, у якості напрямку діяльності зазначено: «підготувати зведення існуючих прав людини для Інтернет-користувачів з метою допомоги їм у здійсненні комунікації та забезпеченні ефективного доступу до основних суб'єктів у Інтернеті та до державних установ у тих випадках, коли вони вважають, що їхнім правам і свободам було завдано шкоди – для того щоб повідомити про такий випадок, подати скаргу або отримати 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 засіданні 27-30 квітня 2012 року запропонував Комітету міністрів створити Комітет експертів із прав Інтернет-користувачів (MSI-DUI) та погодив сферу компетенції цього Комітету. За пропозицією CDMSI Комітет міністрів затвердив повноваження Комітету на 1147-му засіданні постійних представників міністрів, що відбулося 6 липня 2012 року<sup>5</sup>. Відповідно до повноважень, наданих MSI-DUI, від нього очікують такі результати:

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

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

<sup>5</sup>Див. CM(2012)91.

6. На форумі з управління Інтернетом (6-9 листопада 2012 року, Баку) під час семінару на тему «Розширення можливостей Інтернет-користувачів – за допомогою яких інструментів?» було проведено консультації із зацікавленими сторонами. Учасники форуму від MSI-DUI скористалися можливістю поспілкуватися з широкою аудиторією на цьому заході, щоб дізнатися думку учасників щодо різноманітних питань, пов'язаних зі Зведенням. Під час обговорень на семінарі з'ясувалися проблеми, що постають перед Інтернет-користувачами, зокрема, видалення контенту, створеного користувачами, без належного судового розгляду, питання, пов'язані з захистом персональних даних, а також відсутність ефективних засобів правового захисту.
7. MSI-DUI провів своє друге засідання 13-14 грудня 2012 року в Страсбурзі. Було розглянуто відповіді, надані різними учасниками на анкету, а також обговорено інформацію, отриману за результатами спілкування з зацікавленими сторонами. Комітет MSI-DUI вирішив на цьому завершити попередній етап своєї роботи та почати працювати над 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-DUI детально розглянув питання, пов'язані з правом на свободу вираження поглядів, правом на приватне життя, свободу зібрань та об'єднань, онлайн-безпеку, правом на освіту, правами дітей, недискримінацією та правом на ефективні засоби правового захисту. Обговорення питань ґрунтувалося на відповідних обов'язкових і необов'язкових стандартах Ради Європи та прецедентному праві Суду. Комітет MSI-DUI також розглянув питання щодо того, який документ міг би бути прийнятий Радою Європи на підтримку Зведення, наприклад, декларація чи рекомендація Комітету міністрів. Такий документ повинен виконувати подвійне завдання: надавати Інтернет-користувачам прості та чіткі рекомендації щодо їх прав онлайн, а також забезпечувати прийняття державами-членами такого документу, що відповідав би їх зобов'язанням за 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 повинне поєднувати офіційну та зрозумілу мову, але при цьому потрібно уникати надмірного спрощення чинних стандартів та

прецедентної практики Суду у сфері прав людини. У ході обговорення було також підкреслено бажаність регулярного оновлення Зведення з метою відображення політики у сфері Інтернету, що постійно змінюється. Для того щоб зрозуміти загальну спрямованість Зведення, Керівний комітет CDMSI вирішив також надати коментарі до проекту Зведення (станом на момент консультацій), зазначивши при цьому, що документ «перебуває на стадії розробки». Отримані відповіді підтвердили підхід Комітету MSI-DUI при підготовці зручного для користувача інформаційного документу, в якому особливу увагу приділено праву на свободу вираження поглядів, праву на приватне життя, праву на освіту, правам дітей і захисту від кіберзлочинності.

- 10.** Проект Зведення був презентований до обговорення зацікавленим сторонам під час Європейського діалогу з управління Інтернетом (EuroDIG, 20-21 червня 2013 року в Лісабоні), зокрема, на семінарі «На шляху до гуманного Інтернету? Правила, права та відповідальність для нашого майбутнього онлайн». Учасники семінару від Комітету MSI-DUI провели неформальну зустріч у Лісабоні. Була висловлена думка про те, що проект Зведення варто скоротити для його більшої доступності Інтернет-користувачам. За результатами цих обговорень та роботи членів Комітету MSI-DUI між сесіями 10 вересня 2013 року в Страсбурзі було проведено спеціальне засідання для тих членів Комітету MSI-DUI, які змогли взяти у ньому участь. На цій зустрічі було розглянуто проект рекомендації Комітету міністрів про права Інтернет-користувачів, який містив у додатку проект Зведення прав людини та основоположних свобод для Інтернет-користувачів. У проекті Зведення автори звертаються безпосередньо до користувача. У зв'язку з таким підходом було прийнято рішення 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-DUI розглянув та остаточно затвердив свої пропозиції для Комітету CDMSI стосовно проекту рекомендації Комітету міністрів щодо використання Посібника з прав людини для Інтернет-користувачів (надалі – «Посібник»). Було вирішено провести багатосторонні консультації, в тому числі з Відкритим форумом Ради Європи, щодо цього Посібника на Форумі з управління Інтернетом (22-25 жовтня 2013 року, Індонезія). До ряду відібраних учасників від приватного сектора, громадянського су-

спільства, технічної та наукової спільнот звернулися з проханням про надання коментарів та пропозицій щодо використання Посібника. Крім того, було запропоновано надати неофіційні коментарі та відгуки щодо проекту рекомендації й іншим відповідним керівним комітетам Ради Європи, у тому числі Керівному комітету з прав людини (CDDH), Європейському комітету з питань правового співробітництва (CDCJ), Європейському комітету з проблем злочинності (CDPC), а також комітетам, пов'язаним із договорами, включно з Консультативним комітетом із питань Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (T-PD), Комітетом із питань кіберзлочинності (T-CY), Комітетом експертів із проблем тероризму (CODEXTER) та Комітетом сторін-учасниць Конвенції про захист дітей від сексуальної експлуатації та сексуального насильства (T-ES). У відповідь комітети CDDH, CDCJ та члени Бюро T-PD надали свої коментарі, які були враховані та увійшли до проекту Рекомендації і проекту Пояснювального меморандуму, підготовлених CDMSI.

- 12.** Крім того, близько 30 відгуків надійшло від представників приватного сектора (телекомунікаційних компаній, провайдерів мережі Інтернет), ключових організацій громадянського суспільства, технічної та наукової спільнот з усіх куточків світу. Вони загалом схвально оцінювали роботу Ради Європи над проектом Посібника та надали чимало коментарів і пропозицій до нього.
- 13.** На своєму четвертому засіданні 3-6 грудня 2013 року Керівний комітет CDMSI розглянув пропозиції MSI-DUI стосовно проекту рекомендації Комітету міністрів щодо використання Посібника з прав людини для Інтернет-користувачів. Було враховано результати консультацій із зазначеними вище зацікавленими сторонами та остаточно затверджено проект рекомендації на основі фінальних коментарів, надісланих електронною поштою.

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

- 14.** Мета цієї Рекомендації полягає в сприянні реалізації та захисту прав людини й основоположних свобод в Інтернеті у всіх державах-членах Ради Європи. Доступ окремих осіб та спільнот до Інтернету і найоптимальніше його використання потребують їхнього інформування та розширення можливостей для реалізації ними своїх права і свобод в онлайні. Цей підхід був підтверджений Комітетом міністрів у Декларації про принципи управління Інтернетом 2011 року, в якій він підкреслив своє бачення Інтернету, орієнтованого на людину і побудованого на засадах поваги до прав людини, з метою підвищення потенціалу Інтернет-користувачів у реалізації ними своїх прав і свобод в Інтернеті як принципу управління Інтернетом.
- 15.** Посібник, що додається до цієї Рекомендації, надає певну базову інформацію щодо окремих прав людини, закріплених у ЄКПЛ та інших відповідних стандартах Ради Європи. Цей документ зосереджує увагу на конкретних правах і свободах та пов'язаних із ними нормах міжнародного права, зокрема, праві на свободу вираження поглядів, свободу зібрань та об'єднань, праві на приватне життя і захист персональних даних, правах дитини, а також праві на ефективні засоби правового захисту. Посібник написаний зрозумілою для користувачів мовою. З метою максимального спрощення тексту Комітет MSI-DUI вирішив не посилатися на суто юридичні формулювання зобов'язань держав-членів за міжнародним правом, у тому числі й на прецедентне право Суду.
- 16.** Права людини та основоположні свободи гарантовано різними документами Ради Європи, дія яких поширюється як в режимі офлайн так і в режимі онлайн, тобто в Інтернеті також. Зокрема, права людини та основоположні свободи закріплені в ЄКПЛ, яка тлумачиться Судом у його прецедентній практиці. Низка конвенцій Ради Європи та інші документи, що не мають обов'язкової юридичної сили, надають додаткові роз'яснення та пояснення для Інтернет-користувачів. Відповідно до позиції Комітету MSI-DUI, для того щоб Інтернет-користувачі розуміли свої права та свободи, їм потріб-

но роз'яснювати їх у простих формулюваннях, що відповідають міжнародно-правовим стандартам Ради Європи та Організації Об'єднаних Націй.

## Преамбула

- 17.** У преамбулі подано пояснення причини прийняття Комітетом міністрів Рекомендації своїм державам-членам. Насамперед ця Рекомендація виходить з того, що відповідальність за забезпечення прав людини та основоположних свобод людини покладається на держави-члени Ради Європи, що має здійснюватися відповідно до ЄКПЛ у її тлумаченні Судом. Сюди ж належать й інші зобов'язуючі документи Ради Європи, зокрема, Конвенція про кіберзлочинність (надалі – «Будапештська конвенція»), Конвенція про захист дітей від сексуальної експлуатації та сексуального насильства (ЗДРЕ №201, надалі – «Ланцаротська конвенція»), Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (СЕД №108, надалі – «Конвенція 108»).
- 18.** Інші незобов'язуючі стандарти, ухвалені Комітетом міністрів, містять рекомендації державам-членам із питань, пов'язаних з Інтернетом. Серед таких стандартів: Рекомендація CM/Rec(2007)16 Комітету міністрів державам-членам про заходи щодо підвищення цінності Інтернету як суспільно важливого ресурсу; Рекомендація CM/Rec(2008)6 Комітету міністрів державам-членам про заходи з розвитку поваги до свободи слова та інформації у зв'язку з Інтернет-фільтрами; Рекомендація CM/Rec(2010)13 Комітету міністрів державам-членам про захист осіб у зв'язку з автоматизованою обробкою персональних даних у контексті профілювання; Рекомендація CM/Rec(2011)7 Комітету міністрів державам-членам про нове поняття ЗМІ; Рекомендація CM/Rec(2012)4 Комітету міністрів державам-членам про захист прав людини у зв'язку з послугами соціальних мереж та Рекомендація CM/Rec(2012)3 Комітету міністрів державам-членам про захист прав людини щодо пошукових систем.
- 19.** Другий пункт преамбули передбачає, що зобов'язання держав дотримуватися, захищати та сприяти правам людини передбачають зобов'язання здійснювати контроль над приватними компаніями. Це твердження впливає зі статті 1 ЄКПЛ, за якою держави повинні гарантувати кожному, хто перебуває під їхньою юрисдикцією, права і свободи, передбачені Конвен-

цією. Сюди належить і захист від порушень прав людини з боку недержавних суб'єктів, що потребує вживання відповідних кроків для запобігання, розслідування, покарання і відшкодування завданих порушенням збитків за допомогою ефективного законодавства і заходів. Суд у своїх рішеннях підтвердив, що на держави покладається позитивне зобов'язання захищати основні права та свободи осіб в Інтернеті, зокрема ті, що стосуються свободи вираження поглядів<sup>6</sup>, захисту дітей та молоді<sup>7</sup>, захисту моралі та прав інших осіб<sup>8</sup>, боротьби з расистськими та ксенофобськими закликами, а також протидії дискримінації і расовій ненависті<sup>9</sup>. Крім того, Суд поклав на держави відповідальність за відмову захищати своїх громадян від негативного впливу на їхні права та свободи, заподіяні діями приватних компаній<sup>10</sup>. У другому пункті також відображено принцип універсальності та неподільності прав людини, що закріплений у Віденській декларації, прийнятій на Саміті глав держав та урядів держав-членів Ради Європи 9 жовтня 1993 року.

- 20.** У третьому пункті преамбули підтверджено значення Інтернету як суспільно важливого ресурсу, як це передбачено у Рекомендації Комітету міністрів CM/Rec(2007)16<sup>11</sup>. Зважаючи на велику роль Інтернету в повсякденній діяльності користувачів та необхідність забезпечувати захист їхніх прав людини в Інтернеті, у цій рекомендації підкреслено: ніхто не повинен ставати об'єктом неправомірного, безпідставного або неспівмірного втручання в свої права і свободи.
- 21.** У четвертому пункті преамбули визначено мету цієї Рекомендації – розширювати розуміння користувачами своїх прав людини в онлайні та сприяти їх ефективній реалізації, в тому числі завдяки доступу до ефективних засобів правового захисту. Саме тому настільки важливо інформувати користувачів про загрози їхнім основним правам і свободам, а також про

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

<sup>7</sup> Справа «К. У. проти Сполученого Королівства» (K.U. v. UK), №2872/02.

<sup>8</sup> Справа «Пей проти Сполученого Королівства» (Pay v. UK), №32792/05.

<sup>9</sup> Справа «Ферет проти Бельгії» (Féret v. Belgium), №15615/07.

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

<sup>11</sup> Рекомендація CM/Rec(2007)16 Комітету міністрів державам-членам про заходи щодо підвищення цінності Інтернету як суспільно важливого ресурсу.

можливості правового захисту. Заява про можливості, що надаються Інтернетом для транспарентності та підзвітності у суспільних справах, пояснює природу самої основи цієї Рекомендації, яка полягає в тому, щоб дати можливість окремим 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: основні права і свободи однаковою мірою застосовуються в режимі онлайн і офлайн<sup>12</sup>. Цей підхід було підтверджено Радою ООН з прав людини в її Резолюції від 2012 року «Заохочення, захист і дотримання прав людини в Інтернеті». Сприяння застосуванню цього Посібника посилить захист прав людини та основоположних свобод відповідно до чинних стандартів у сфері прав людини.
- 23.** У підпункті 5.1 державам-членам рекомендовано розповсюджувати цей Посібник не лише через органи державної влади, але і залучати приватний сектор. Це може бути його публікація та поширення в друкованій формі або адаптація в електронних форматах. Відповідні державні органи також можуть розміщувати цей Посібник на своїх сайтах. До цього ж можна закликати і приватний сектор.
- 24.** У підпункті 5.2 підтверджено, що здійснення прав людини та основоположних свобод в Інтернеті може підлягати обмеженням, що мають законну мету і є необхідними в демократичному суспільстві, як це передбачено у відповідних статтях ЄКПЛ. З метою забезпечення дотримання цих умов Комітет міністрів рекомендував державам-членам здійснювати оцінку, регулярний огляд та (де необхідно) знімати обмеження на права людини й основоположні свободи в Інтернеті.
- 25.** У підпункті 5.3 містяться заклики до держав-членів розширювати свої зусилля із забезпечення права на ефективний засіб правового захисту, зокрема й завдяки поглибленню координації і співробітництва між існуючими відповідними інститутами, установами (у тому числі й регуляторами

<sup>12</sup> Див. Декларацію Комітету міністрів про принципи управління Інтернетом, принцип 1 «Права людини, демократія та верховенство права».



електронного зв'язку) та спільнотами, які забезпечують правового захисту, наприклад, у контексті обробки скарг, з якими звертаються Інтернет-користувачі. Ця Рекомендація також визнає наявність різноманітних механізмів компенсації в різних державах-членах, що надають такі структури, як органи захисту даних, омбудсмени, суди або гарячі лінії. Держави-члени можуть також здійснювати перевірки існуючих механізмів компенсації у межах своєї юрисдикції й узагальнювати відповідну інформацію в зручних для користувача списках механізмів компенсації. Подібну інформацію можна поширювати разом із цим Посібником, наприклад, у формі додатка. 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 інформацію через кордони і незалежно від них. Це означає, що права людини та основоположні свободи в Інтернеті в державах-членах Ради Європи можуть бути предметом дій із боку державних або недержавних суб'єктів поза їхніми межами Ради Європи; наприклад, може мати місце втручання в свободу вираження поглядів та доступу до інформації, а також щодо поваги приватного життя у зв'язку з персональними даними. З огляду на це у підпункті 5.4 міститься рекомендація координувати діяльність між державами-членами Ради Європи і державами, що не входять до складу цієї організації, а також недержавними суб'єктами.
- 27.** У підпункті 5.5 державам-членам рекомендовано заохочувати повноцінний діалог між приватним сектором та відповідними органами державної влади і громадянським суспільством у тому, що стосується соціальної відповідальності приватного сектору. Основоположний підхід Керівних принципів підприємницької діяльності в аспекті прав людини<sup>13</sup> полягає в тому, що приватні компанії повинні поважати права людини, а це означає, що їм варто уникати порушення прав інших осіб і протидіяти негативно-

<sup>13</sup>«Керівні принципи ООН з питань підприємницької діяльності в аспекті прав людини: реалізація курсу ООН на «захист, повагу і засоби правового захисту» (A/HRC/17/31), ухвалені Резолюцією Ради з прав людини «Права людини, транснаціональні корпорації та інші підприємства (A/HRC/RES/17/4). Зокрема, Керівними принципами передбачено, що держави повинні забезпечувати виконання вимог законів, які спрямовані на гарантування права людини або вимагають від приватних підприємств поважати ці права, а також періодично здійснювати оцінку відповідності подібних законів та усувати будь-які прогалини; забезпечувати, щоб інші закони та нормативи, якими регулюється утворення та функціонування приватних підприємств, наприклад, корпоративне право, не обмежували, а гарантували дотримання у підприємницькій діяльності прав людини; надавати ефективну підтримку, ефективні рекомендації приватним підприємствам із питань поваги прав людини в їхній діяльності; заохочувати і (де необхідно) вимагати від приватних підприємств інформувати про те, як вони вирішують питання впливу своєї діяльності на права людини.

му впливу на права людини, до якого вони причетні. Транспарентність та підзвітність суб'єктів приватного сектора визнаються важливим засобом демонстрації їхньої відповідальності шляхом рекламування та поширення Посібника. Наприклад, провайдери Інтернет-послуг і провайдери доступу до контенту могли б посилатися 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 розповсюдження й застосування Посібника. Таким чином, державам-членам рекомендовано заохочувати організації громадянського суспільства та активістів до розповсюдження і застосування Посібника, а також до посилання на нього, коли вони виступають за імплементацію стандартів у галузі прав людини та їх дотримання.

*Додаток*

## ПОСІБНИК ІЗ ПРАВ ЛЮДИН ДЛЯ ІНТЕРНЕТ-КОРИСТУВАЧІВ

### Вступ

- 29.** Цей Посібник звертається безпосередньо до користувача. Він виступає інструментом для звичайного Інтернет-користувача, який не має спеціальних знань про Інтернет, що ґрунтуються на відповідній освіті або навчанні. Зокрема, йдеться про вміння користувача правильно поводитися в Інтернеті (наприклад, щодо даних про свою ідентичність, персональних даних). Користувачі повинні бути поінформовані в повному обсязі щодо того, як їхній вибір в Інтернеті може впливати на їхні права та свободи, а також про наслідки надання згоди на те, що вони обирають. Вони повинні розуміти обмеження щодо їхніх прав, а також знати про існуючі механізми правового захисту.
- 30.** Посібник ґрунтується на положеннях ЄКПЛ і відповідній прецедентній практиці Суду. У ньому також враховано інші зобов'язуючі документи Ради Європи. Посібник спирається також на інші документи, а саме на окремі декларації та рекомендації Комітету міністрів. Цей Посібник не обмежує дотримання чинних стандартів у сфері прав людини, на основі яких він був

розроблений. Прав і свобод, про які йдеться у Посібнику, потрібно дотримуватися відповідно до юридичних документів, на основі яких вони були розроблені. Посібник містить посилання на чинні стандарти у галузі прав людини та відповідні механізми їх дотримання, при цьому не створюючи нових прав та свобод. Цей Посібник не є ні вичерпним, ні зобов'язуючим роз'ясненням стандартів у сфері прав людини. Наприклад, наступні уточнення про можливі обмеження і втручання у права людини, а також рекомендації з надання допомоги користувачам щодо протидії насильству та образам в Інтернеті заслуговують подальшої уваги з тим, щоб допомогти користувачам краще розуміти свої права, захищати себе та інших. Водночас Посібник лишається відкритим для оновлення та приведення його у відповідність до нових стандартів 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 нерозривно пов'язані й загалом застосовні до всіх прав людини та основоположних свобод, що містяться в ньому, зокрема й до доступу до Інтернету і принципу недискримінації.
32. І хоча доступ до Інтернету досі офіційно не визнаний у якості права людини (враховуючи відмінності у національних контекстах, зокрема й у внутрішньому законодавстві та політиці), він розглядається як умова та фактор сприяння свободі вираження поглядів та іншим правам і свободам<sup>14</sup>. Відповідно позбавлення Інтернет-користувачів доступу може негативно відобразитися на здійсненні ними своїх прав і свобод і навіть означати обмеження права на свободу вираження поглядів, в тому числі права на отримання і поширення інформації. Суд заявив, що в наш час Інтернет став одним із головних засобів реалізації права на свободу вираження поглядів та інформації. Свобода вираження поглядів поширюється не лише на зміст

<sup>14</sup> Спеціальний доповідач ООН із питання про право на свободу поглядів та їх вільне вираження Франк Ла Рю підкреслив, що «Інтернет став необхідним інструментом для реалізації низки прав людини, боротьби з нерівністю та інструментом прискорення розвитку і людського прогресу, при цьому забезпечення доступу до Інтернету має стати першочерговим завданням для всіх держав. Кожна держава, виходячи з цього, повинна розробити конкретну та ефективну політику у ході консультацій із представниками усіх верств суспільства, зокрема й із приватним сектором і відповідними державними установами для того, щоб Інтернет був широко доступним, відкритим та надавався за помірну плату для всіх груп населення». «Будучи каталізатором для людей у здійсненні їхнього права на свободу слова і вираження поглядів, Інтернет також забезпечує можливість 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](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf).

інформації, але також на засоби її поширення, оскільки будь-яке їх обмеження неминуче порушує право на отримання і поширення інформації. Таке втручання може бути прийнятним лише у разі його відповідності умовам, передбаченим у п. 2 статті 10 ЄКПЛ у її тлумаченні Судом<sup>15</sup>. Захід, що може вплинути на доступ осіб до Інтернету, передбачає відповідальність держави згідно зі статтею 10<sup>16</sup>.

- 33.** У зв'язку з цим у Посібнику стверджується, що Інтернет-користувачі не повинні позбавлятися доступу до Інтернету проти їх волі за винятком тих випадків, коли відповідне рішення приймається Судом. Однак це не варто розуміти як заходи законного примусового позбавлення доступу, наприклад, в контексті договірних зобов'язань. Споживачів Інтернету дозволяється відключати від Інтернету у разі несплати за послуги, що їм надаються, але це повинно бути крайньою мірою. Крім того, діти можуть підпадати під обмеження доступу до Інтернету в межах здійснення батьківського контролю за використанням Інтернету залежно від віку та зрілості дитини.
- 34.** Інтернет-користувачі повинні мати ефективні засоби правового захисту у разі їх відключення від Інтернету у випадках, коли на це немає рішення суду. Це передбачає необхідність повідомлення користувача провайдером Інтернет-послуг про причини та правові підстави такого відключення, порядок оскарження та звернення з проханням про відновлення повного доступу до Інтернету. Такі запити повинні розглядатися в розумні строки. Крім того, кожен Інтернет-користувач при реалізації ним свого права на справедливий судовий розгляд повинен мати можливість звернутися з проханням про перегляд заходу про відключення компетентним адміністративним та (або) судовим органом. Ці аспекти здійснення правосуддя підсумовано в останньому розділі Посібника під назвою «Ефективні засоби правового захисту».
- 35.** Ще одним аспектом доступу до Інтернету є позитивні дії та заходи, що вживаються органами державної влади для того, щоб кожен мав доступ до Інтернету. Комітет міністрів Ради Європи рекомендував державам-членам

<sup>15</sup> Див. вище, п. 2, §50. Див. також справу «Аутронік АГ» проти Швейцарії» (Autronic AG v. Switzerland), №12726/87. У справі «Хуршид Мустафа і Тарзібачі проти Швеції» (Khurshid Mustafa and Tarzibachi v. Sweden), №23883/06, Суд встановив, що тлумачення національним судом приватного акту (договору) передбачає відповідальність держави-відповідача, що поширює захист за статтею 10 на обмеження, які встановлювалися приватними особами.

<sup>16</sup> Див. вище, п. 2, §53.

сприяти підвищенню цінності Інтернету як суспільно важливої послуги<sup>17</sup>. Під цим розуміється «інтенсивне використання населенням Інтернету в якості основного засобу в повсякденному житті для спілкування, інформації, знань, комерційних операцій і пов'язані з цим законні очікування того, що послуги Інтернету надаватимуться за прийнятною ціною, а також будуть доступними, безпечними, надійними і безперервними». Цей розділ інформує користувачів про те, що вони повинні 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 в Інтернеті, як це передбачено у статті 10 ЄКПЛ<sup>18</sup>. Комітет міністрів Ради Європи заявив, що кожен Інтернет-користувач повинен мати якомога ширший доступ до Інтернет-контенту, програм та послуг на власний вибір, незалежно від того, надаються вони безоплатно чи ні, з застосуванням відповідних пристроїв на власний вибір. Це – загальний принцип, який, як правило, називають «мережевою нейтральністю» і який повинен застосовуватися незалежно від інфраструктури чи мережі, що використовуються для доступу до Інтернету<sup>19</sup>.

**37.** Органи державної влади повинні докладати розумних зусиль у цілях забезпечення доступу до Інтернету для окремих категорій осіб, зокрема тих, що проживають у віддалених районах, та інвалідів, що ґрунтується на принципі універсальної суспільної послуги, закріпленому в Рекомендації №R(99)14 Комітету міністрів щодо нових комунікаційних та інформаційних послуг<sup>20</sup>. У Рекомендації підкреслено, що особи, які проживають у сільських чи географічно віддалених районах, малозабезпечені особи або особи з особливими потребами, а також інваліди можуть очікувати на конкретні заходи з боку органів державної влади у зв'язку з їхнім доступом до Інтернету.

**38.** Очікування осіб з обмеженими можливостями мати однаковий з інши-

<sup>17</sup> Див. вище, п. 9, CM/Rec(2007)16, розділ II.

<sup>18</sup> Див. вище, п. 2, §50.

<sup>19</sup> Декларація Комітету міністрів про мережеву нейтральність мережі, прийнята Комітетом міністрів 29 вересня 2010 року. Див. також Директиву 2002/21/ЄС Європейського парламенту і Ради ЄС від 7 березня 2002 року про спільні рамки регулювання електронних комунікаційних мереж і послуг, стаття 8(4) г.

<sup>20</sup> Див. вище, п. 9, CM/Rec(2007)16, додаток, розділ II; Рекомендація №R(99)14 Комітету міністрів державам-членам про універсальну суспільну послугу, що стосується нових комунікаційних та інформаційних послуг, принцип 1.

ми Інтернет-користувачами та недискримінаційний доступ до Інтернету впливає з документів Ради Європи, у яких державам-членам рекомендовано робити все необхідне для забезпечення особам з обмеженими можливостями доступу до Інтернету та ІКТ<sup>21</sup>. Держави-члени повинні заохочувати невисоку вартість доступу, пам'ятаючи про важливість структури, необхідність підвищення рівня обізнаності цих осіб та груп, практичне значення та привабливість доступу до Інтернету і послуг, а також про їх здатність до адаптації та сумісність<sup>22</sup>.

- 39.** Принцип недискримінації повинен застосовуватися до взаємодії користувача з органами державної влади, Інтернет-провайдерами, провайдерами доступу до контенту та іншими організаціями, користувачами або іншими групами користувачів. Четвертий пункт у дещо перефразованому вигляді викладає статтю 14 ЄКПЛ і статтю 1 Протоколу 12 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 своїй прецедентній практиці підтвердив, що стаття 10 повністю може бути застосована до Інтернету<sup>23</sup>. До права на свободу вираження поглядів входить право на вільне висловлення своїх думок, переконань, ідей, на пошук, отримання і поширення інформації незалежно від державних кордонів. Інтернет-користувачі повинні бути вільними у вираженні своїх політичних переконань, а також своїх релігійних і нерелігійних поглядів. Останнє стосується реалізації права на свободу думки, совісті та релігії, закріпленого у статті 9 ЄКПЛ. Свобода вираження поглядів стосується не лише «інформації» чи «ідей», що сприймаються прихильно або вважаються необразливими чи нейтральними, але також тих, що завдають образи, шокують або виводять зі стану рівноваги<sup>24</sup>.
- 41.** Реалізація права на свободу вираження поглядів Інтернет-користувачами повинна врівноважуватися правом на захист репутації. Суд у низці справ прийняв рішення про те, що це право захищається статтею 8 ЄКПЛ, що

<sup>21</sup> Там само.

<sup>22</sup> Див. вище, п. 9, CM/Rec(2007)16, додаток, розділ II.

<sup>23</sup> Див. вище, п. 2, §50.

<sup>24</sup> Справа «Хендсайд проти Сполученого Королівства» (Handyside v. UK), рішення від 7 грудня 1976 р., серія А №24, п. 49.

закріплює право на повагу до приватного життя<sup>25</sup>. Суд постановив, що права, гарантовані статтями 8 і 10, заслуговують на однакову повагу. Він вважає, що коли право на свободу вираження поглядів урівноважене правом на повагу до приватного життя, то відповідні критерії такого урівноважування містять такі елементи: внесок в обговорення, які становлять суспільний інтерес, ступінь знаменитості конкретної особи, предмет заяви, попередню поведінку відповідної особи, метод отримання інформації та її достовірність, зміст, форму та наслідки оприлюднення, а також тяжкість застосовуваних санкцій<sup>26</sup>. Отже, в Посібнику зазначено, що Інтернет-користувач повинен приділяти належну увагу репутації інших осіб, зокрема, їхньому праву на приватне життя.

- 42.** Існує вираження поглядів, яке не підпадає під захист за статтею 10 ЄКПЛ, зокрема заклики до ненависті. Суд постановив, що на окремі форми вираження поглядів, які рівнозначні закликам до ненависті або заперечують основоположні цінності ЄКПЛ, не поширюється захист, передбачений статтею 10 Конвенції<sup>27</sup>. У зв'язку з цим Суд застосовує статтю 17 ЄКПЛ. Хоча загальноприйнятого визначення розпалювання ненависті не існує, Комітет міністрів Ради Європи заявив, що поняття «розпалювання ненависті» варто розуміти як таке, що охоплює всі форми вираження поглядів, через які здійснюється поширення, підбурення, сприяння або виправдання расової ненависті, ксенофобії, антисемітизму або інших форм ненависті, що ґрунтуються на нетерпимості, яка виявляється через агресивний націоналізм та етноцентризм, дискримінацію та ворожість щодо меншин, мігрантів та осіб іммігрантського походження<sup>28</sup>. У п. 2 цього розділу про свободу вираження поглядів міститься конкретна інформація, викладена простою для користувача мовою, у якій надано пояснення, що заклики до ненависті не підпадають під дію статті 10 ЄКПЛ. Цей пункт не претендує на те, щоб пояснити з використанням юридичних термінів різні підходи, на підставі яких до розпалювання ненависті можуть застосовуватися статті 10 і 17 ЄКПЛ. Зважаючи на право-

<sup>25</sup>Справи «Шові та інші проти Франції» (Chauvy and Others v. France), №64915/01, §70; «Пфайфер проти Австрії» (Pfeifer v. Austria), №12556/03, §35; «Поланко Торрес і Мовілла Поланко проти Іспанії» (Polanco Torres and Movilla Polanco v. Spain), №34147/06, §40.

<sup>26</sup>Справи «Делфі АС» проти Естонії» (Delfi AS v. Estonia), №64569/09, §78-81 (цю справу передано на розгляд Великої палати Суду); «Аксель Шпрінгер АГ проти Німеччини» (Axel Springer AG v. Germany), №39954/08, §89-95; «Фон Ганновер проти Німеччини» (Von Hannover v. Germany) (№2), №40660/08 і 60641/08, §108-113.

<sup>27</sup>Справи «Ферет проти Бельгії» (Féret v. Belgium), №15615/07; «Гароді проти Франції» (Garaudy v. France), №65831/01, 24.06.2003, рішення про прийнятність; «Лерой проти Франції» (Leroy v. France), №36109/03; «Єрсїлд проти Данії» (Jersild v. Denmark), №15890/89; «Вейделанд та інші проти Швеції» (Vejdeland and Others v. Sweden), №1813/07.

<sup>28</sup>Рекомендація №R(97)20 Комітету міністрів державам-членам щодо розпалювання ненависті.

ву природу цієї відмінності, було вирішено, що таку інформацію буде краще розкрити в пояснювальному меморандумі.

- 43.** Користувачі мають право отримувати і поширювати інформацію в Інтернеті, зокрема, створювати, повторно використовувати і розповсюджувати контент із використанням Інтернету. Суд дослідив взаємозв'язок між захистом інтелектуальної власності та свободою вираження поглядів у кримінальних справах про порушення авторського права. На думку Суду, обвинувальні вироки у цих справах були втручанням у право на свободу вираження поглядів, і для того щоб перші могли вважатися обґрунтованими, вони повинні бути передбачені законом, переслідувати законну мету захисту прав інших осіб і вважатися необхідними у демократичному суспільстві<sup>29</sup>. Обмін або надання іншим можливості обмінюватися файлами в Інтернеті, навіть якщо йдеться про матеріали, захищені авторським правом та у цілях отримання вигоди, охоплюються правом отримувати та поширювати інформацію, як це передбачено статтею 10 ЄКПЛ<sup>30</sup>. Це право не є абсолютним, а тому існує необхідність зважувати, з одного боку, важливість обміну інформацією, а з другого – зацікавленість у захисті прав суб'єктів авторського права. Суд підкреслив, що інтелектуальна власність захищається на основі статті 1 Протоколу до ЄКПЛ. Таким чином, питання полягає у збалансуванні двох конкуруючих інтересів, обидва з яких захищаються ЄКПЛ.
- 44.** Рекомендація Комітету міністрів державам-членам про заходи щодо підвищення цінності Інтернету як суспільної послуги містить конкретні рекомендації щодо заходів і стратегій стосовно свободи спілкування і творчості в Інтернеті незалежно від державних кордонів. Зокрема, у відповідних випадках повинні вживатися заходи щодо сприяння «повторному використанню» Інтернет-контенту, що означає використання існуючих цифрових контентних ресурсів для створення майбутнього контенту або надання послуг таким чином, щоб вони були сумісними з повагою до прав інтелектуальної власності<sup>31</sup>.
- 45.** У пункті 4 надано загальний огляд вимог, яким повинні відповідати обмежен-

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

<sup>30</sup>Там само.

<sup>31</sup>Див. вище, п. 9, CM/Rec(2007)16, додаток, розділ III, абзац 2.



ня права на свободу вираження поглядів. Відповідно до статті 10 ЄКПЛ держави-члени насамперед зобов'язуються не втручатися в обмін інформацією між особами незалежно від того, будуть це фізичні або юридичні особи. Суд підтвердив, що ефективна реалізація права на свободу вираження поглядів також може потребувати позитивних заходів захисту навіть у сфері відносин між окремими особами. Питання про відповідальність держави може виникнути в результаті того, що остання не прийняла відповідне національне законодавство<sup>32</sup>. Порушення ЄКПЛ може бути встановлене і в тому випадку, коли тлумачення національними судами юридичного акту, незалежно від того, чи є останній приватним договором, державним документом, нормативним положенням чи адміністративною практикою, є нерозумним, довільним, дискримінаційним або у більш широкому розумінні – таким, що не відповідає основоположним принципам ЄКПЛ<sup>33</sup>.

- 46.** Свобода вираження поглядів не є абсолютним правом і може бути предметом обмежень. Втручання у свободу вираження поглядів повинно розглядатися як будь-яка форма обмеження з боку будь-якого органу, що здійснює державні повноваження та обов'язки або функціонує у сфері державних послуг, наприклад, до них належать суди, органи прокуратури, міліція/поліція, будь-які правоохоронні органи, розвідувальні служби, центральні або місцеві ради, державні 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 означає, що законодавство має бути доступним, чітким і достатньо точним для того, щоб особи могли регулювати свою поведінку. Законодавство повинно передбачати достатні гарантії від надмірних обмежувальних заходів, зокрема й ефективний контроль із боку суду чи іншого незалежного судового органу<sup>34</sup>. Втручання також повинно переслідувати законну мету в інтересах національної безпеки, територіальної цілісності або суспільної безпеки з метою запобігання порушенням громадського порядку чи злочинам, захисту здоров'я чи моралі, захисту репутації чи прав інших осіб, недопущення розголошення отриманої конфіденційної

<sup>32</sup>Справа «Об'єднання «Ферайн реген Тьєрфабрікен» проти Швейцарії» (VgT Verein gegen Tierfabriken v. Switzerland), №24699/94, §45.

<sup>33</sup>Справи «Хуршид Мустафа і Тарзібачі проти Швеції» (Khurshid Mustafa and Tarzibachi v. Sweden), №23883/06, §33; «Пла і П'юнсерно проти Андорри» (Plaand Puncernau v. Andorra), №69498/01, §59, ЄКПЛ 2004-VIII.

<sup>34</sup>Див. вище, п. 2, §64.

інформації, підтримки авторитетності та безсторонності судової системи. Цей перелік є вичерпним, але його тлумачення і сфера дії розвиваються разом із практикою Суду. Втручання також повинно бути необхідним у демократичному суспільстві, а це означає, що потрібно довести його нагальну суспільну необхідність, наявність законної мети, а також того факту, що цей захід є найменш обмежувальним для досягнення цієї мети<sup>35</sup>. Ці вимоги викладені зрозумілою для користувача мовою, тобто будь-які обмеження свободи вираження поглядів не повинні бути довільними і мають переслідувати законну мету відповідно до ЄКПЛ, наприклад, серед іншого йдеться про захист національної безпеки або громадського порядку, здоров'я населення і моралі, що повинно відповідати законодавству у сфері прав людини.

**48.** У наступних пунктах Пояснювального меморандуму більш докладно розглядаються гарантії, які повинні надаватися Інтернет-користувачам у разі обмеження права на свободу вираження поглядів в режимі онлайн. Прикладом подібних обмежень, що можуть розглядатися як порушення свободи вираження поглядів, може бути блокування та фільтрація. Деякі загальні принципи щодо блокування та фільтрації ґрунтуються на практиці Суду чи інших відповідних стандартах, прийнятих Комітетом міністрів<sup>36</sup>.

**49.** Державні органи мають право вдаватися до загальнодержавних заходів блокування або фільтрації лише в тих випадках, коли фільтрація стосується конкретного і чітко визначеного контенту за умови наявності рішення компетентного національного органу про його незаконність, яке може бути переглянуте незалежним та неупередженим судом або регулюючим органом згідно з вимогами статті 6 ЄКПЛ<sup>37</sup>. Державні органи повинні забезпечити оцінку фільтрів до та під час їх застосування, що забезпечить пропорційність їхніх наслідків меті обмеження, а отже – їх необхідність у демократичному суспільстві, з метою недопущення невідповідного блокування контенту<sup>38</sup>.

**50.** Заходи блокування конкретного Інтернет-контенту не повинні довільно

<sup>35</sup> Там само, §66-70.

<sup>36</sup> Рекомендація CM/Rec(2008)6 Комітету міністрів державам-членам про заходи щодо розвитку поваги до свободи вираження поглядів та інформації у зв'язку з Інтернет-фільтрами; див. додаток, ч. III, ii; див. також вище, п. 1.

<sup>37</sup> Там само, CM/Rec(2008)6, див. додаток, ч. III, iv.

<sup>38</sup> Там само.

використовуватися як засоби загального блокування інформації в Інтернеті. Вони не повинні мати побічних наслідків у формі закриття доступу до великих обсягів інформації, що істотно обмежить права Інтернет-користувачів<sup>39</sup>. Вони повинні бути передбачені законом. У цілях недопущення зловживання повинен забезпечуватися суворий контроль за масштабами блокування а також ефективний судовий розгляд<sup>40</sup>. У ході судового розгляду подібних заходів потрібно зважувати відповідні конфліктні інтереси, урівноважувати їх і з'ясувати, чи існує менш масштабний захід, який можна застосувати в цілях блокування доступу до конкретного Інтернет-контенту<sup>41</sup>. Зазначені вище вимоги та принципи не можуть стати на заваді встановленню фільтрів із метою захисту неповнолітніх у конкретних місцях, наприклад, школах, бібліотеках, де останні мають доступ до Інтернету<sup>42</sup>.

**51.** Фільтрація та деіндексація Інтернет-контенту пошуковими системами несе в собі загрозу порушення свободи вираження поглядів Інтернет-користувачів. Пошукові системи вільно здійснюють загальний пошук та індексують інформацію, що міститься у всесвітній мережі. Їх не можна зобов'язувати здійснювати моніторинг своїх мереж і послуг ініціативно з метою виявлення передбачувано незаконного контенту, і вони не повинні здійснювати будь-яку попередню фільтрацію або блокування, крім тих випадків, коли це передбачено рішенням суду або іншого компетентного органу. Деіндексація або фільтрація окремих сайтів на запит державних органів повинні бути прозорими, вузькоцільовими, а також регулярно переглядатися за умови дотримання вимог справедливого судового розгляду<sup>43</sup>.

**52.** Цей розділ також визначає деякі гарантії, що повинні надаватися Інтернет-користувачам у разі запровадження обмежень, зокрема, це стосується інформування користувача та надання можливості оскарження таких обмежень. Про це йдеться в Рекомендації Комітету міністрів Ради Європи про заходи щодо фільтрації та блокування<sup>44</sup>. Інтернет-користувачам повинна надаватися інформація про активацію фільтрації, причини здійснен-

<sup>39</sup> Див. вище, п. 2, §52, 66-68; див. також Декларацію Комітету міністрів про свободу спілкування в Інтернеті.

<sup>40</sup> Там само, п. 2 вище, §64; справа «Об'єднання «Екін» проти Франції» (Association Ekin v. France), №39288/98.

<sup>41</sup> Там само, п. 2 вище, §64-66.

<sup>42</sup> Див. Декларацію Комітету міністрів про свободу спілкування в Інтернеті, принцип 3.

<sup>43</sup> Див. Рекомендацію CM/Rec(2012)3 Комітету міністрів державам-членам про захист прав людини у зв'язку з пошуковими системами, додаток, ч. III.

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

ня фільтрації конкретного виду контенту для розуміння ними того, яким чином та відповідно до яких критеріїв здійснюється фільтрація (наприклад, чорні списки, білі списки, блокування за ключовим словом, рейтинг контенту, деіндексація або фільтрація окремих сайтів чи контенту пошуковими системами). Їм повинна бути надана точна інформація та рекомендації щодо обходу активного фільтру, зокрема, до кого звертатися, коли існує припущення, що контент був необґрунтовано заблокований, за допомогою яких засобів можна відключати фільтри щодо конкретного типу контенту або сайту. Користувачів потрібно забезпечувати ефективними і загальнодоступними засобами оскарження та правового захисту, в тому числі з призупиненням дії фільтрів у тих випадках, коли користувачі заявляють про необґрунтованість блокування контенту.

- 53.** Можуть мати місце випадки, коли компанії, наприклад, такі, що представляють соціальні мережі, видаляють контент, що був створений та розміщений Інтернет-користувачами, облікові записи користувачів (наприклад, профіль користувача або його присутність в соціальних мережах), обґрунтовуючи свої дії недотриманням вимог користування їхніми послугами. Подібні дії можуть становити втручання в право на свободу вираження поглядів і право на отримання та поширення інформації, крім випадків дотримання вимог п. 2 статті 10 ЄКПЛ у її тлумаченні Судом<sup>45</sup>.
- 54.** Згідно з Керівними принципами ООН підприємницької діяльності в аспекті прав людини (які не мають обов'язкової юридичної сили) приватні компанії зобов'язані поважати права людини, що вимагає від них не завдавати шкоди правам людини та не сприяти такій шкоді, а також забезпечувати або співпрацювати щодо компенсації у випадку завдання такої шкоди. Обов'язок захищати і надавати доступ до ефективних засобів правового захисту – один із найбільш важливих обов'язків держави, що знайшло своє відображення в п. 5 розділу про свободу вираження поглядів. Корпоративна соціальна відповідальність Інтернет-провайдерів передбачає обов'язок боротьби з розпалюванням ненависті та іншим контентом, що породжує ненависть чи дискримінацію. Провайдери онлайн-послуг повинні звертати увагу на висловлювання та редакційне редагування висловлювань,

<sup>45</sup>Рекомендація CM/Rec (2011)7 Комітету міністрів державам-членам про нове поняття ЗМІ, §7, додаток, §15, 44-47, 68-69; Рекомендація CM/Rec(2012)4 Комітету міністрів державам-членам про захист прав людини у зв'язку з послугами соціальних мереж, §3.

мотивованих расовим, ксенофобським, антисемітським, ненависним до жінок, сексистським ставленням (зокрема й ставленням щодо лесбіянок, гомосексуалістів, бісексуалів та транссексуалів) чи іншими мотивами<sup>46</sup>. Ці провайдери також мають бути готовими надати допомогу Інтернет-користувачам через повідомлення їх про зміст або вираження поглядів та (або) поведінку, які можуть вважатися незаконними<sup>47</sup>.

- 55.** Посібник звертає увагу Інтернет-користувачів на те, що провайдери он-лайн-послуг, які розміщують контент, створений користувачами, мають право на здійснення різних рівнів редакційної оцінки змісту своїх послуг<sup>48</sup>. Без шкоди для своєї редакційної свободи вони повинні забезпечувати Інтернет-користувачам реалізацію їхнього права на пошук, отримання та поширення інформації відповідно до статті 10 ЄКПЛ<sup>49</sup>. Це означає, що будь-яке обмеження щодо створеного користувачем контенту повинно бути конкретним, виправданим з точки зору цілей, для досягнення яких воно було встановлене, і доведеним до відома відповідного Інтернет-користувача.
- 56.** Інтернет-користувач повинен мати змогу приймати поінформоване рішення щодо того, чи користуватися йому послугами онлайн. На практиці Інтернет-користувач повинен бути повною мірою поінформований про будь-які передбачувані заходи щодо видалення створеного ним контенту або його облікового запису до запровадження таких заходів<sup>50</sup>. Інтернет-користувачам також повинна надаватися доступна (зрозумілою для користувача мовою), чітка та точна інформація щодо фактів та підстав для вжиття заходів, за допомогою яких передбачено видалення контенту та облікового запису. Це передбачає наявність законодавчих положень, на основі яких були вжиті такі заходи, а також інших елементів оцінки пропорційності та законності мети, яку вони переслідують. Інтернет-користувачі також повинні мати можливість звернутися з проханням про перегляд рішення про видалення контенту та (або) облікового запису в розумні строки й оскаржити рішення в компетентному адміністративному та (або) судовому органі.

<sup>46</sup> Там само, CM/Rec(2011)7, §91.

<sup>47</sup> Там само, CM/Rec(2012)4, II/10.

<sup>48</sup> Там само, CM/Rec(2011)7, §18, 30-31.

<sup>49</sup> Там само, CM/Rec(2011)7, §7, абзац 2.

<sup>50</sup> Див. «Деактивація облікового запису та видалення контенту: Керівні принципи та практика для компаній та користувачів», автори: Еріка Ньюланд, Каролін Нолан, Синтія Вонг, Джиліан Йорк. Режим доступу до ресурсу: [http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final\\_Report\\_on\\_Account\\_Deactivation\\_and\\_Content\\_Removal.pdf](http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pdf).

- 57.** У шостому підпункті йдеться про анонімність, що ґрунтується на практиці Суду, Будапештській конвенції та інших документах Комітету міністрів. Суд розглянув питання конфіденційності спілкування в Інтернеті у справі, пов'язаній із відмовою однієї з держав-членів Ради Європи змусити Інтернет-провайдера назвати особу, яка розмістила непристойне оголошення щодо неповнолітньої особи на сайті знайомств у Інтернеті. Суд постановив, що, незважаючи на те, що свобода вираження поглядів та конфіденційність спілкування є головними цінностями, а користувачі телекомунікацій та Інтернет-послуг повинні мати гарантії поваги до їхнього приватного життя та свободи вираження поглядів, такі гарантії не можуть бути абсолютними і повинні поступатися місцем у такому випадку іншим законним вимогам, таким як запобігання порушенню громадського порядку або злочину чи захист прав і свобод інших осіб. На державу покладається позитивне зобов'язання забезпечувати рамки для поєднання цих конкуруючих інтересів<sup>51</sup>.
- 58.** Будапештська конвенція не передбачає кримінальну відповідальність за використання комп'ютерних технологій у цілях анонімної комунікації. Згідно з пояснювальною доповіддю до цієї Конвенції, «зміна трафіку даних із метою сприяння анонімним комунікаціям (наприклад, діяльності анонімних систем пересилання електронних листів) або внесення змін до даних із метою реалізації безпеки комунікації (наприклад, шифрування) повинні в принципі розглядатися як законний захист приватного життя, а тому вважатися правомірними. Водночас Сторони [Будапештської конвенції] можуть виявити бажання криміналізувати окремі зловживання, пов'язані з анонімною комунікацією, наприклад, змінені пакетні дані з метою приховування ідентичності особи при скоєнні злочину»<sup>52</sup>.
- 59.** Комітет міністрів Ради Європи підтвердив принцип анонімності в своїй Декларації про свободу спілкування в Інтернеті<sup>53</sup>. Відповідно з метою забезпечення захисту від стеження онлайн і зміцнення свободи вираження поглядів держави-члени Ради Європи повинні поважати бажання Інтернет-користувачів не розкривати свою особу. Водночас повага до анонімності не заважає державам-членам вживати заходів для відстеження осіб, відповідальних за вчинення кримінальних діянь відповідно до національ-

<sup>51</sup> Справа «К. У. проти Фінляндії» (K.U. v. Finland), №2872/02, §49.

<sup>52</sup> Будапештська конвенція про кіберзлочинність, ст. 2, пояснювальна доповідь, §62.

<sup>53</sup> Див. Декларацію про свободу спілкування в Інтернеті, принцип 7.

ного законодавства, ЄКПЛ та інших міжнародних договорів у сфері 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 принципів, встановлених Судом щодо захисту політичних заяв, зокрема, в рамках п. 2 ст. 10 ЄКПЛ передбачено мало свободи дій щодо обмежень у контексті політичних заяв або обговорень із питань, що становлять суспільний інтерес<sup>54</sup>.
61. Користувач має право на свободу зібрань та об'єднань з іншими особами через використання Інтернету. Це передбачає формування, приєднання, мобілізацію та участь у суспільних групах та зібраннях, а також профспілках завдяки використанню інструментів, заснованих на Інтернеті. Сюди належить, наприклад, підписання петицій для участі в кампаніях або інших формах громадських акцій. Користувач повинен мати свободу обирати інструменти для реалізації цих прав, таких як сайти, додатки чи інші послуги. Реалізація цього права не потребує будь-якого формального визнання 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. Протести, що мають наслідки для всього суспільства, такі як створення перешкод або блокування доступу до приміщень, є в межах здійснення права на свободу зібрань відповідно до статті 11 ЄКПЛ. Однак так не обов'язково відбувається в кожному випадку, коли подібні дії приводять до порушення послуг онлайн, наприклад, якщо йдеться про несанкціонований доступ до конкретного сайту, до обмеженого онлайн-простору або обробки цифрового контенту без дозволу. Врешті, важливо повідомляти користувача про те, що свобода та наслідки протесту онлайн, результатом яких є порушення, не завжди можуть бути вільно сприйняті.
63. Інтернет став інструментом активної участі громадян у побудові та зміцненні демократичних суспільств. Комітет міністрів рекомендував державам-членам розробляти та запроваджувати стратегії електронної демократії, електронної участі та електронного врядування з використанням

<sup>54</sup>Справа «Вінгроув проти Сполученого Королівства» (Wingrove v. UK), 25 листопада 1996 р., §58, протоколи 1996-V.

інформаційно-комунікаційних технологій (ІКТ) у демократичних процесах та обговореннях як у відносинах між державними органами та громадянським суспільством, так і при наданні державних послуг<sup>55</sup>.

- 64.** Сюди входять свобода участі в публічних політичних дебатах на місцевому, національному і глобальному рівнях, законодавчі ініціативи, контроль за прийняттям рішень, в тому числі право підписувати петиції з застосуванням ІКТ там, де вони існують. Це ґрунтується на рекомендаціях Комітету міністрів державам-членам про заохочення використання громадянами ІКТ (у тому числі онлайн-форумів, онлайн-журналів, політичних чатів, смс-розсилок та інших форм спілкування між громадянами) для участі в демократичних обговореннях, електронних заходах та електронних кампаніях із метою озвучення своїх проблем, ідей та ініціатив, організації діалогу та обговорень із представниками громадян і владою, а також контролю за діяльністю посадових осіб та політиків із питань, що становлять суспільний інтерес.

## Приватне життя і захист даних

- 65.** Право на повагу до сімейного і приватного життя закріплене у статті 8 ЄКПЛ. Це право отримало подальше тлумачення в практиці Суду, доповнюється і посилюється Конвенцією Ради Європи 108.
- 66.** Приватне життя – це поняття, для означення якого не існує вичерпного визначення. Суд наголосив на тому, що стаття 8 охоплює широке коло інтересів, зокрема, приватне і сімейне життя, житло і кореспонденцію, зокрема й пошту, телефонні переговори<sup>56</sup> та електронну пошту на робочому місці. Приватне життя пов'язане з правом особи на своє зображення<sup>57</sup>, наприклад, у формі фотографій або відеокліпів. Воно також стосується ідентичності особи та особистого розвитку, права на налагодження та розвиток відносин з іншими людьми. Ним також охоплено діяльність професійного або підприємницького характеру<sup>58</sup>.

<sup>55</sup> Див. п. 9 вище, CM/Rec(2007)16, додаток, ч. I.

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

<sup>57</sup> Справи «Фон Ганновер проти Німеччини» (Von Hannover v. Germany) (№2), №40660/08 і 60641/08, §108-113; «Шіакка проти Італії» (Sciaccia v. Italy), №50774/99, §29.

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



- 67.** Багато напрямків діяльності користувачів передбачають певну форму автоматизованої обробки персональних даних, наприклад, використання браузерів, електронної пошти, миттєвих повідомлень, передачі голосових повідомлень через Інтернет-протоколи, соціальні мережі й пошукові системи, а також хмарні сервіси для зберігання даних. Конвенція 108 охоплює всі операції, що здійснюються в Інтернеті у зв'язку зі збиранням, зберіганням, зміною, видаленням та відновленням чи поширенням персональних даних<sup>59</sup>.
- 68.** Існують принципи та правила, яких повинні дотримуватися органи державної влади та приватні компанії, що здійснюють обробку персональних даних. Необхідно, щоб користувач знав і розумів, яким чином оброблюються його дані та які дії можна вчиняти у зв'язку з цим, наприклад, звернутися з проханням про виправлення або видалення даних. Згідно з Конвенцією 108, персональні дані можуть бути отримані та оброблені справедливо і законно, зберігатися для визначених та правомірних цілей. Ці процеси повинні бути адекватними, адаптованими і не надмірними щодо тих цілей, задля яких такі дані зберігаються. Самі дані повинні бути точними і за необхідності оновлюватися, зберігатися у такий спосіб, що дозволяє ідентифікувати особу, персональні дані якої обробляються, та не довше строку, який потрібен для тієї мети, заради якої ці дані зберігаються<sup>60</sup>.
- 69.** Наголос робиться на двох конкретних принципах обробки персональних даних: законності такої обробки та згоди користувача. Користувач повинен бути поінформований про те, що дані можуть оброблятися лише у передбачених законом випадках і за його згоди, яку користувач може надати, наприклад, погодившись з умовами користування Інтернет-послугою.
- 70.** Вільна, конкретна, інформована та чітка (однозначна) згода особи на обробку персональних даних в Інтернеті наразі є предметом обговорення з метою внесення відповідного положення до Конвенції 108<sup>61</sup>. Інформована згода згадується в Рекомендації CM/Rec(2012)4 Комітету міністрів дер-

<sup>59</sup> Див. Конвенцію 108, ст. 2.

<sup>60</sup> Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS №108).

<sup>61</sup> Консультативний комітет Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS №108) надав низку пропозицій щодо модернізації цієї Конвенції (T-PD(2012)4Rev3\_en). Одна з пропозицій стосується згоди особи, персональні дані якої обробляються, у якості передумови такої обробки: «Кожна Сторона забезпечує обробку даних на засадах вільної, конкретної, інформованої та [чіткої, однозначної] згоди суб'єкта даних або за передбачених законодавством підстав».

жавам-членам про захист прав людини у зв'язку з послугами соціальних мереж. Зокрема, соціальні мережі повинні отримувати інформовану згоду своїх користувачів перед поширенням або обміном їхніми персональними даними з іншими категоріями осіб чи компаній або використанням їх у спосіб, інший ніж той, для якого вони збиралися. Для отримання згоди користувачів останні повинні мати можливість висловитися на користь більш широкого доступу третіх осіб (наприклад, коли в соціальних мережах використовуються програми третіх осіб). Користувачі також повинні мати можливість відкликати свою згоду.

**71.** Також варто згадати Рекомендацію CM/Rec(2010)13 Комітету міністрів державам-членам про захист осіб у зв'язку з автоматичною обробкою персональних даних у контексті профілювання. Під цим розуміють методи автоматичної обробки даних шляхом застосування профілю до особи з метою прийняття рішень щодо неї або в цілях аналізу чи визначення особистих преференцій, поведінки, позицій. Наприклад, персональні дані Інтернет-користувача можуть бути зібрані та оброблені в контексті його взаємодії з сайтом чи додатком або в контексті використання браузера в Інтернеті протягом певного періоду часу або через різні сайти (наприклад, шляхом збору інформації про те, які сторінки та контент відвідує особа, час відвідування, предмет пошуку та зроблені кліки). «Ідентифікаційні маркери» («cookies») – один із способів відстеження активності користувача – роблять це шляхом зберігання інформації в апаратурі користувача для її подальшого вилучення. Рекомендація передбачає право Інтернет-користувачів надавати свою згоду на використання персональних даних із метою профілювання і право на відмову від такої згоди<sup>62</sup>.

**72.** Права Інтернет-користувачів на інформацію у зв'язку з обробкою їхніх персональних даних згадуються в різних документах Ради Європи. Конвенція 108 передбачає, що суб'єкту даних повинна бути надана можливість встановлювати факт обробки його персональних даних будь-якою фізичною або юридичною особою, з'ясувати основні цілі такої обробки, а також найменування та фактичну адресу або основне місце розташування органу, який здійснює обробку даних, та отримувати в розумні строки і без

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

надмірних затримок чи значних витрат підтвердження факту зберігання його персональних даних, а також отримувати повідомлення про такі дані у чіткій формі<sup>63</sup>.

- 73.** Інформування користувачів також згадується в Рекомендації CM/Rec(2012)4 Комітету міністрів державам-членам про захист прав людини у зв'язку з послугами соціальних мереж. Інтернет-користувачі в соціальних мережах повинні бути в чіткий та зрозумілий спосіб поінформовані про внесення будь-яких змін до умов надання послуг провайдерами. Це також передбачає й інші дії, такі як встановлення додатків третіх сторін, що можуть становити загрозу приватному життю користувачів; законодавство, що застосовується до надання послуг у соціальних мережах і відповідної обробки їхніх персональних даних; наслідки відкритого доступу (в часі й географічно) до їхніх профілів і комунікацій, зокрема, пояснення різниці між приватними та публічними комунікаціями, а також наслідки публічного доступу до інформації, в тому числі необмеженого доступу і збору даних третіми особами; необхідність отримувати попередню згоду інших осіб перед оприлюдненням їхніх персональних даних, зокрема й відео- та аудіоконтенту у тих випадках, коли вони розширюють доступ за межі самостійно відібраних користувачами контактів. Інтернет-користувачам також варто надавати конкретну інформацію щодо логічного підходу, який лежить в основі обробки персональних даних, що використовуються для присвоєння їм профілів та з метою профілювання.
- 74.** Інтернет-користувачі повинні мати можливість здійснювати контроль за своїми персональними даними відповідно до Конвенції 108, зокрема, у тому, що стосується права на виправлення або стирання даних, що були оброблені незаконно, а також права на засоби правового захисту у тому випадку, коли підтвердження або (залежно від контексту) повідомлення, виправлення чи стирання, про які йшлося вище, не були здійснені<sup>64</sup>.
- 75.** Рекомендація CM/Rec(2012)3 Комітету міністрів державам-членам про захист прав людини щодо пошукових систем стосується низки заходів, які можуть вживати провайдери з метою захисту приватного життя своїх користувачів. Сюди входить захист персональних даних від незаконного до-

<sup>63</sup> Конвенція 108, ст. 8.

<sup>64</sup> Див. п. 60 вище, ст. 8.

ступу третіх осіб і схеми повідомлення про порушення даних. До заходів також повинні належати абонентське шифрування повідомлень між користувачами і провайдером пошукової системи. Взаємна кореляція даних, що походять від різних послуг/платформ і належать провайдеру пошукової системи, може мати місце лише у разі надання користувачем однозначної згоди на цю конкретну послугу. Користувачі повинні мати можливість доступу, виправлення та видалення своїх даних, зібраних у ході користування такими послугами, в тому числі щодо будь-якого створеного профілю, наприклад, у цілях прямого маркетингу<sup>65</sup>.

**76.** Соціальні мережі повинні також допомагати користувачам управляти своїми даними та захищати їх, зокрема, за допомогою:

- *шаблонних налаштувань приватності за замовчуванням, якими обмежується доступ до визначених і відібраних користувачем контактів. Це передбачає адаптацію до їхніх умов забезпечення приватного життя та відбір рівня публічного доступу до їхніх даних;*
- *поширеного захисту чутливих даних, таких як доступ до біометричних даних або розпізнавання облич, який не повинен активуватися автоматично;*
- *убезпечення даних від незаконного доступу до персональних даних користувача третіх осіб, у тому числі абонентське шифрування між користувачем і соціальними мережами. Користувачів необхідно інформувати про порушення безпеки їхніх персональних даних із метою вживання ними запобіжних заходів у вигляді зміни пароля, а також для уважного ставлення до своїх фінансових операцій (наприклад, коли соціальні мережі мають доступ до банківської інформації або реквізитів кредитної картки);*
- *захисту приватного життя на рівні технологічного рішення: коли потреба в захисті даних враховується на етапі розробки послуг або продуктів, а зміни в наявних послугах постійно оцінюються на предмет впливу на приватне життя;*

<sup>65</sup> Див. CM/Rec(2012)3, зокрема, додаток, ч. II.

- захисту тих, хто не є користувачами соціальних мереж, шляхом відмови від збору та обробки їхніх персональних даних, наприклад, адрес електронної пошти та біометричних даних. Користувачі повинні знати про свої зобов'язання перед іншими особами, зокрема, що публікація персональних даних, пов'язаних з іншими особами, повинна відповідати дотриманню прав цих інших осіб<sup>66</sup>.

- 77.** Перед закриттям облікового запису користувача в соціальній мережі він повинен мати можливість просто та вільно перенести свої дані на інший сервіс чи пристрій у зручному для нього форматі. Після цього всі дані користувача та про користувача повинні бути назавжди видалені із носіїв зберігання служби соціальної мережі. Крім того, Інтернет-користувачі повинні мати можливість робити свідомий вибір щодо своєї ідентичності онлайн, в тому числі щодо використання псевдоніма. Якщо соціальна мережа потребує реєстрації із зазначенням дійсних особистих даних, то публікація дійсних особистих даних в Інтернеті повинна бути здійснена на вибір користувача. Це не заважає правоохоронним органам отримувати доступ до дійсних особистих даних користувача у разі необхідності та за умови надання відповідних правових гарантій, що забезпечують дотримання основних прав і свобод.
- 78.** У контексті профілювання користувач також повинен мати можливість заперечувати проти використання своїх персональних даних із метою профілювання і проти рішення, яке приймається виключно на основі профілювання, що має правові наслідки для користувача або істотно торкається його інтересів, за винятком тих випадків, коли це передбачено законом, у якому вказано заходи із забезпечення законних інтересів користувачів, зокрема, дозволяється їм викласти свою точку зору, за винятком тих випадків, коли рішення приймається у ході виконання договору і при цьому передбачено, що існують заходи із забезпечення законних інтересів Інтернет-користувача<sup>67</sup>.
- 79.** Права Інтернет-користувачів не є абсолютними, саме тому у третьому підпункті є посилання на слово «в цілому». Винятки дозволяються, коли вони передбачені законом і у тих випадках, коли вони є необхідною мірою в де-

<sup>66</sup> Там само.

<sup>67</sup> Рекомендація CM/Rec(2010)13 Комітету міністрів державам-членам про захист осіб у зв'язку з автоматизованою обробкою персональних даних у контексті профілювання, розділ 5.

мократичному суспільстві в інтересах: а) захисту державної безпеки; громадської безпеки, фінансових інтересів держави або для боротьби зі злочинами; б) захисту суб'єкта даних або прав і свобод інших осіб. Обмеження здійснення передбачених прав можуть міститися в законі щодо автоматизованих досє персональних даних, що використовуються в статистичних цілях або наукових досліджень у тих випадках, коли відсутня явна загроза порушення приватного життя суб'єкта даних<sup>68</sup>.

**80.** Перехоплення, пов'язане з прослуховуванням, моніторингом або спостереженням за змістом повідомлень, забезпеченням змісту даних через доступ і використання комп'ютерної системи або непрямо з використанням електронного прослуховування чи пристроїв для прослуховування. Перехоплення може також передбачати запис<sup>69</sup>. Право на повагу до конфіденційності кореспонденції та повідомлень закріплене у статті 8 ЄКПЛ з її подальшим тлумаченням Судом. Поняття кореспонденції охоплює поштові і телекомунікаційні повідомлення<sup>70</sup>, а також повідомлення електронною поштою на робочому місці<sup>71</sup>. Очікується, що тлумачення цього поняття буде змінюватися, щоб відповідати розвитку технологій, завдяки яким можуть з'являтися нові форми спілкування в Інтернеті, такі як електронні листи (у широкому розумінні), миттєві повідомлення тощо, які потрапляють під дію статті 8.

**81.** Далі розглянуто деякі загальні принципи, підтверджені практикою Суду, щодо перехоплення і спостереження за повідомленнями у справах, не пов'язаних з Інтернетом, а також у справах, що стосуються втручання органів державної влади. Ці принципи надають загальні рекомендації та посилення для можливого застосування їх у майбутньому до Інтернет-спілкування.

**82.** Перехоплення кореспонденції та телекомунікацій є втручанням у право на приватне життя й обмежується умовами, закріпленими у п. 2 ст. 8 ЄКПЛ. Сам факт існування законодавства, яке дозволяє здійснювати спо-

<sup>68</sup> Конвенція 108, ст. 9.

<sup>69</sup> Див. пояснювальну доповідь до Будапештської конвенції, п. 53.

<sup>70</sup> Справи «Асоціація за євроінтеграцію і права людини та Екміджієв проти Болгарії» (Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria), №62540/00, §58; «Класс та інші проти Німеччини» (Klass and Others v. Germany), №5029/71; «Малоун проти Сполученого Королівства» (Malone v. UK), №8691/79; «Вебер і Саравія проти Німеччини» (Weber and Saravia v. Germany), №54934/00.

<sup>71</sup> Див. справу «Копленд проти Сполученого Королівства» (Copland v. UK), №62617/00.

стерезення за телекомунікаціями, може вважатися втручанням у право на приватне життя. Законодавство, яке запроваджує систему спостереження, в рамках якої всі особи у відповідній державі потенційно можуть стати об'єктом моніторингу на предмет їхньої поштової переписки і повідомлень, безпосередньо стосується всіх користувачів або потенційних користувачів поштових і телекомунікаційних послуг у цій державі. У зв'язку з цим Суд підтвердив право кожної особи за певних умов заявляти про те, що вона стала жертвою порушення, спричиненого самим фактом існування секретних заходів або законодавства, яким вони дозволяються, і при цьому вона не повинна скаржитися про те, що подібні заходи були фактично застосовані до неї самої<sup>72</sup>.

**83.** Перехоплення повинно мати законодавчу підставу та бути необхідним у демократичному суспільстві в інтересах національної безпеки, громадської безпеки або економічного добробуту країни, запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або захисту прав і свобод інших осіб, як це передбачено статтею 8 ЄКПЛ. Суд розробив такі загальні принципи, що, зокрема, стосуються тих вимог, яким повинно відповідати законодавство, що регулює приховані заходи спостереження за кореспонденцією і повідомленнями з боку органів державної влади.

- *Передбачуваність* – законодавство повинно бути доступним для відповідної особи, яка повинна мати можливість передбачити наслідки його застосування щодо неї. Законодавство має бути сформульоване достатньо чітко і точно для того, щоб громадяни мали чітке уявлення про те, за яких умов і обставин влада має право вдатися до такого таємного і потенційно небезпечного втручання в право на повагу до приватного життя і кореспонденції<sup>73</sup>.

- *Мінімальні гарантії у сфері дискреційних повноважень органів державної влади* – законодавство повинно містити детальні норми щодо

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

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

i) характеру правопорушень, які можуть передбачати віддання наказу про перехоплення; ii) визначення категорій осіб, повідомлення яких можуть підлягати моніторингу; iii) граничної тривалості такого моніторингу; iv) порядку аналізу, використання і зберігання отриманих даних; v) запобіжних заходів при повідомленні даних іншим особам; а також щодо обставин, за яких отримані дані можуть або повинні бути стерті, а записи знищено<sup>74</sup>.

- *Нагляд та перегляд компетентними органами влади* – Суд вимагає наявності адекватних і ефективних гарантій щодо недопущення зловживань<sup>75</sup>.

**84.** У практиці Суду щодо приватного життя на робочому місці було встановлено, що телефонні дзвінки працівника у приміщенні підприємства підпадають під категорію приватного життя і кореспонденції. Електронна пошта, яка надсилається з робочого місця, а також інформація, отримана за результатами моніторингу особистого використання Інтернету, повинні захищатися за статтею 8 ЄКПЛ. У разі відсутності повідомлення працівника про те, що його діяльність може підлягати моніторингу, останній має розумні підстави сподіватися на повагу до приватного життя в контексті телефонних дзвінків, електронної пошти та користування Інтернетом на робочому місці<sup>76</sup>. Користувачу може бути надана допомога з боку органів, відповідальних за захист даних, або інших компетентних органів у державах-членах.

**85.** Органи, що відповідають за захист даних та існують в більшості держав-членів, відіграють важливу роль у розслідуванні, втручанні, підвищенні поінформованості або участі в іншій формі для надання правової допомоги виправлення ситуації у ході обробки персональних даних. Це все забезпечується додатково до першочергової ролі держави у забезпеченні захисту персональних даних у більш широкому розумінні своїх зобов'язань гарантувати право на приватне та сімейне життя.

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

<sup>75</sup> Справа «Асоціація за євроінтеграцію і права людини та Екміджієв проти Болгарії» (Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria), №62540/00), §77.

<sup>76</sup> Справа «Копленд проти Сполученого Королівства» (Copland v. UK), №62617/00, §41-42.



## Освіта і грамотність

- 86.** Право на освіту закріплене в статті 2 Протоколу 1 до ЄКПЛ. Рекомендація СМ/Rec(2007)16 Комітету міністрів державам-членам про заходи підвищення цінності Інтернету як суспільно важливого ресурсу закликає до створення і розвитку доступу до навчального, культурного та наукового контенту в цифровій формі з наданням можливостей для самовираження всім культурам і доступу до Інтернету всіма мовами включно з мовами корінних/нечисленних народів<sup>77</sup>. Інтернет-користувачі повинні мати можливість вільного доступу до наукових і культурних здобутків у Інтернеті, що фінансуються державою<sup>78</sup>. Також у рамках розумних обмежень має бути забезпечений доступ до цифрових матеріалів, що є суспільним надбанням. В окремих випадках дозволяється запроваджувати умови доступу до знань із метою виплати винагороди правовласникам за їхню роботу в межах допустимих винятків у сфері захисту прав інтелектуальної власності.
- 87.** Інтернет-користувачі повинні мати можливість отримувати в Інтернеті базову інформацію, освіту, знання та навички з метою реалізації своїх прав людини і основоположних свобод. Це відповідає стандартам Комітету міністрів Ради Європи у сфері забезпечення комп'ютерної грамотності як основної передумови доступу до інформації, реалізації культурних прав і права на освіту із застосуванням ІКТ<sup>79</sup>.
- 88.** Програми та ініціативи у сфері Інтернет-грамотності дозволяють Інтернет-користувачам критично аналізувати точність і достовірність Інтернет-контенту. Комітет міністрів рекомендував державам-членам Ради Європи сприяти доступу до засобів ІКТ і заохочувати освіту для того, щоб всі особи, і особливо діти, здобували навички, необхідні для роботи з найрізноманітнішими ІКТ, і критично оцінювали якість інформації, зокрема тієї, що може бути для них шкідливою<sup>80</sup>.

<sup>77</sup> Див. також п. 8 вище, СМ/Rec(2007)16, розділ IV.

<sup>78</sup> Там само.

<sup>79</sup> Декларація Комітету міністрів про права людини і верховенство права в інформаційному суспільстві, СМ(2005)56 доопрацьована 13 травня 2005 року.

<sup>80</sup> Там само.

## Діти і молодь

- 89.** Діти та молодь мають право висловлювати свої погляди, брати участь у житті суспільства і прийнятті рішень, які торкаються їхніх інтересів, через використання Інтернету та інших ІКТ. Це ґрунтується на стандартах Комітету міністрів, якими проголошено право всіх дітей і молоді віком до 18 років мати засоби, простір, можливості й (коли це необхідно) підтримку для того, щоб вільно висловлювати свої погляди, бути почутими і вносити свій вклад у прийняття рішень із питань, які торкаються їхніх інтересів. При цьому їхній думці повинна приділятися належна увага з урахуванням їхнього віку, зрілості та рівня розуміння. Право дітей і молоді на участь повною мірою поширене на Інтернет без будь-якої дискримінації за будь-якими ознаками, в тому числі за ознаками расової приналежності, етнічного походження, кольору шкіри, статі, мови, релігійних, політичних або інших переконань, національного чи соціального походження, майна, інвалідності, народження, сексуальної орієнтації чи іншого статусу<sup>81</sup>.
- 90.** Дітям і молоді потрібно надавати відповідну їхньому віку та обставинам інформацію, в тому числі через соціальні мережі, ЗМІ, про те, які можливості вони мають для реалізації власних прав. Вони мають бути повною мірою поінформовані про масштаби своєї участі, зокрема, про відповідні обмеження, очікувані та фактичні результати участі, а також про те, яким чином була врахована їхня думка<sup>82</sup>. У тих випадках, коли вони вважають, що мало місце порушення їхнього права на участь, їм повинні надаватися ефективні засоби компенсації і правового захисту, такі як адаптовані для дітей способи звернення зі скаргою, судові та адміністративні процедури, а також допомога та підтримка у їх застосуванні<sup>83</sup>.
- 91.** Інтернет-користувачі діти і молодь повинні мати можливість безпечного користування Інтернетом, при цьому повинна бути забезпечена належна повага до їхнього приватного життя. Вчителі, вихователі та батьки повинні їх навчати і надавати інформацію. Їхня інформаційна грамотність означає компетентне використання інструментів доступу до інформації,

<sup>81</sup>Рекомендація CM/Rec(2012)2 Комітету міністрів державам-членам щодо участі дітей і молоді віком до 18 років.

<sup>82</sup>Там само.

<sup>83</sup>Див. Рекомендацію CMRec(2011)12 Комітету міністрів державам-членам про права дітей та соціальні послуги, адаптовані для дітей і сімей; Керівні принципи Ради Європи про правосуддя, адаптовані для дітей.

вміння критично аналізувати контент, розвиток комунікаційних навичок, що сприяють вихованню громадянської позиції і творчого підходу, а також навчання дітей та їхніх вихователів позитивному та відповідальному використанню Інтернету й інформаційно-комунікаційних технологій<sup>84</sup>.

**92.** Право дітей на приватне життя було предметом розгляду у ряді справ у Європейському суді. Фізичний і духовний добробут дітей належить до найважливіших аспектів їхнього права на приватне життя. На держави-члени покладено позитивні зобов'язання щодо забезпечення ефективного дотримання цього права<sup>85</sup>. Суд вважає, що ефективна протидія тяжким діям, які можуть підривати основоположні цінності та найважливіші аспекти приватного життя, потребує закріплення дієвих положень у кримінальному законодавстві й проведення розслідування<sup>86</sup>.

**93.** Важливо розуміти, що контент, який створюється або використовується дітьми та молоддю в Інтернеті, або контент про них, що створюється іншими особами (наприклад, фотографії, відеозаписи, текстовий або інший контент), чи сліди цього контенту (журнали реєстрації, архіви та обробка даних) можуть надовго або назавжди стати доступними. Це може загрожувати їхній гідності, безпеці, приватному життю або іншим чином робити їх уразливими в цей час або на наступних етапах їхнього життя. Вони самі, їхні батьки, опікуни, вчителі та вихователі повинні мати можливість знати й адаптуватися до цих реалій та захищати своє приватне життя в режимі онлайн. Саме тому важливо, щоб існували практичні рекомендації про те, як можна стерти персональну інформацію. Комітет міністрів Ради Європи розробив для держав-членів відповідні рекомендації та заявив, що за винятком правоохоронної діяльності не повинно бути довгострокових або завжди доступних записів контенту, створеного дітьми в Інтернеті, який загрожує їхній гідності, безпеці, приватному життю або іншим чином робить їх уразливими в цей момент або на наступних етапах їхнього життя<sup>87</sup>. Відповідно державам-членам було запропоновано дослідити (там, де це доречно) разом з іншими зацікавленими сторонами можливість видален-

<sup>84</sup> Рекомендація Res(2006)12 Комітету міністрів щодо створення можливостей для дітей у новому інформаційному та комунікаційному середовищі.

<sup>85</sup> Справа «К. У. проти Фінляндії» (K.U. v. Finland), №2872/02, §40-41.

<sup>86</sup> Справи «X та Y проти Нідерландів» (X and Y v. the Netherlands), §23-24 і 27; «Огест проти Сполученого Королівства» (August v. UK), №36505/02; «М.С. проти Болгарії» (M.C. v. Bulgaria), №39272/98, §150; «К. У. проти Фінляндії» (K.U. v. Finland), №2872/02, §46.

<sup>87</sup> Декларація Комітету міністрів про захист гідності, безпеки та приватного життя дітей в Інтернеті.

ня або стирання такого контенту та його слідів (журналів реєстрації, архівів та обробки даних) у розумні строки<sup>88</sup>. Однак підпункт 3 не поширюється на контент, що стосується дітей або молоді та був створений у пресі або видавцями. В першому реченні цього положення Посібника зазначено, що в ньому розглядаються ситуації, пов'язані з контентом, створеним дітьми або молоддю чи іншими Інтернет-користувачами про них.

**94.** Щодо шкідливого контенту і поведінки в режимі онлайн діти мають право на особливу увагу та допомогу, що відповідають їхньому віку та обставинам, зокрема, у зв'язку з ризиком завдання шкоди, що може виникнути у зв'язку з порнографією онлайн, принизливим і стереотипним зображенням жінок, зображенням та схваленням насильства і завдання шкоди собі, зокрема, у тому, що стосується самогубств, принизливих, дискримінаційних або расистських висловлювань, виправдання подібної поведінки, домагання з метою сексуального насильства, вербування дітей-жертв торгівлі людьми, знуцання, переслідування чи інших форм домагання, що можуть мати тяжкі наслідки для фізичного, емоційного та психологічного благополуччя дитини<sup>89</sup>. Таким чином, дітям та молоді, що користуються Інтернетом, потрібно надавати відповідну їхньому віку та будь-яким іншим конкретним обставинам інформацію про види незаконного контенту та поведінки.

**95.** Діти та молодь також повинні мати можливість повідомляти про контент або поведінку, які створюють загрозу завдання шкоди, а також отримувати консультації та підтримку з належною увагою до їхньої конфіденційності та анонімності. Це особливо актуально для контенту в соціальних мережах. Комітет міністрів рекомендував своїм державам-членам вдатися до активних дій щодо цього<sup>90</sup> та, зокрема, захищати дітей і молодь від шкідливого контенту шляхом:

- надання чіткої інформації про види контенту, обмін контентом або поведінку, які можуть суперечити чинним юридичним нормам;
- розробки редакційної політики таким чином, щоб відповідний кон-

<sup>88</sup> Там само.

<sup>89</sup> Рекомендація CM/Rec(2009)5 Комітету міністрів державам-членам про заходи захисту дітей від шкідливого контенту та поведінки і сприяння їхній активній участі в новому інформаційному та комунікаційному середовищі.

<sup>90</sup> Див. CM/Rec(2012)4, додаток, II, §10.

тент або поведінку можна було визначати як «неприпустимі» в умовах використання послуг соціальних мереж, забезпечувати при цьому, щоб такий підхід не обмежував право на свободу вираження поглядів та інформації;

- створення легкодоступних механізмів для повідомлення про неналежний або явно незаконний контент чи поведінку в соціальних мережах;

- належної перевірки та реагування на скарги про кіберзнущання чи кіберзалицяння<sup>91</sup>.

- 96.** Дітей та молодих користувачів також варто інформувати про ризики втручання в їхнє фізичне і моральне благополуччя, в тому числі про сексуальну експлуатацію та насильство у віртуальному середовищі, що потребує особливого захисту. Про це йдеться в Ланцаротській конвенції Ради Європи і відповідній практиці Суду, який визнає, що на держави покладається позитивне зобов'язання забезпечувати захист дітей в Інтернеті<sup>92</sup>.
- 97.** Відповідно до Ланцаротської конвенції діти повинні бути захищені від вербування, схиляння або примушування до участі в порнографічних матеріалах, які розміщуються або пропонуються в Інтернеті (наприклад, із застосуванням веб-камер, чатів, онлайн-ігор)<sup>93</sup>. Вони також повинні бути захищені від домагань із використанням Інтернету або інших ІКТ із метою залучення до участі в сексуальних діях із дитиною (залицяння), яка відповідно до національного законодавства не досягла юридичного віку статевої зрілості, або з метою створення дитячої порнографії<sup>94</sup>.
- 98.** Дітей потрібно заохочувати до участі в формуванні та втіленні державної політики, програм або інших ініціатив у сфері боротьби з сексуальною експлуатацією та сексуальним насильством над дітьми в Інтернеті<sup>95</sup>. Їм повинні надаватися зручні та доступні для дитини засоби для повідомлення про факти сексуального насильства та експлуатації в Інтернеті, а також для подання скарг через інформаційні служби, такі як гарячі лінії телефонного

<sup>91</sup> Там само.

<sup>92</sup> Справа «К. У. проти Фінляндії» (К.У. v. Finland), №2872/02.

<sup>93</sup> Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства СДРС, №201, ст. 2, 21; див. також пояснювальну доповідь до цих статей.

<sup>94</sup> Там само, ст. 23.

<sup>95</sup> Там само, ст. 9/1.

або Інтернет-зв'язку. Їм потрібно надавати консультації та підтримку з питань користування цими послугами з належною увагою до питань приватності та анонімності<sup>96</sup>.

## Ефективні засоби правового захисту

- 99.** Право на ефективний засіб правового захисту закріплене у статті 13 ЄКПЛ. Кожна особа, чиї права і свободи обмежені чи порушуються в Інтернеті, має право на ефективний засіб правового захисту.
- 100.** Стаття 13 ЄКПЛ гарантує наявність на національному рівні засобу правового захисту, спрямованого на забезпечення реалізації по суті передбачених у ЄКПЛ прав і свобод незалежно від того, в якій формі вони можуть забезпечуватися у внутрішньому правопорядку. Це потребує забезпечення національного засобу правового захисту для розгляду по суті скарги, поданої на основі ЄКПЛ, і для надання відповідної компенсації<sup>97</sup>. На держави-члени покладається позитивне зобов'язання щодо невідкладного, ретельного і ефективного розслідування заяв про порушення прав людини. Відповідні процедури повинні давати можливість компетентному органу приймати рішення по суті скарги про порушення Конвенції і не лише призначати санкції за будь-яке встановлене порушення, але також забезпечувати виконання прийнятого рішення<sup>98</sup>.
- 101.** Має бути створений національний орган, на який покладено завдання щодо прийняття рішень за результатами розгляду заяв про порушення прав, гарантованих ЄКПЛ<sup>99</sup>. Потрібно забезпечити окремий правовий порядок, із дотриманням якого особа може подати скаргу на безпідставне затягування провадження у справі про визначення її прав<sup>100</sup>. Це не обов'язково має бути судовий орган, головне, щоб він надавав гарантії незалежності та неупередженості. Водночас надані йому повноваження та процесуальні гарантії повинні дозволяти йому встановлювати ефективність кожного конкретного засобу правового захисту<sup>101</sup>.

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

<sup>97</sup> Справа «Кая проти Туреччини» (Kaya v. Turkey), №22729/93, §106.

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

<sup>99</sup> Справи «Сілвер та інші проти Сполученого Королівства» (Silver and Others v. UK), №5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, §113; «Кая проти Туреччини» (Kaya v. Turkey), №22729/93, §106.

<sup>100</sup> Справа «Кудла проти Польщі» (Kudla v. Poland), №30210/96, §157.

<sup>101</sup> Справи «Сілвер та інші проти Сполученого Королівства» (Silver and Others v. UK), №5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, §113; «Кая проти Туреччини» (Kaya v. Turkey), №22729/93, §106.

- 102.** Порядок роботи компетентного національного органу повинен дозволяти йому виконувати ефективне розслідування порушення. Він повинен дозволяти компетентному органу приймати рішення по суті скарги щодо порушення прав, передбачених ЄКПЛ<sup>102</sup>, призначати санкції за будь-яке порушення і давати потерпілій особі гарантії виконання відповідного рішення<sup>103</sup>. Засіб правового захисту повинен бути ефективним на практиці й за законом та не завжди залежати від ступеня визначеності сприятливого для позивача результату<sup>104</sup>. Хоча жоден засіб правового захисту не може сам по собі повністю задовольнити вимоги статті 13, передбачена законодавством сукупність засобів такого захисту може виконати це завдання<sup>105</sup>.
- 103.** Ефективні засоби правового захисту повинні бути в наявності, про них повинні знати, вони мають бути доступними, надаватися за помірну плату і забезпечувати належне відшкодування. Ефективні засоби правового захисту можна також отримати безпосередньо від провайдерів Інтернет-послуг (хоча вони можуть і не мати такого рівня незалежності, що відповідав би вимогам статті 13 ЄКПЛ), органів державної влади та (або) інших національних правозахисних установ. До можливостей правового захисту входять проведення розслідування, надання пояснення провайдером послуг або Інтернету, надання права відповісти на заяву, що вважається дифамаційною або образливою, відновлення створеного користувачем контенту, що був видалений провайдером Інтернет-послуг, а також відновлення доступу до Інтернету у разі відключення користувача і відповідна компенсація.
- 104.** У частині своїх позитивних зобов'язань щодо захисту осіб від порушення прав людини приватними компаніями держави повинні вживати відповідних заходів, які забезпечать у разі вчинення подібних порушень можливість використання потерпілими судових і позасудових механізмів<sup>106</sup>. Керівні принципи ООН з питань підприємницької діяльності в аспекті прав людини потребують від компаній запровадження таких механізмів подачі скарг, які були б доступними і прогнозованими (запроваджували чітку і зрозумілу процедуру із зазначенням строків на кожно-

<sup>102</sup>Справа «Сміт і Грейді проти Сполученого Королівства» (Smith and Grady v. UK), №33985/96, 33986/96, §138.

<sup>103</sup>Справа «Іатрідіс проти Греції» (Iatridis v. Greece), №31107/96, §60.

<sup>104</sup>Справа «Кудла проти Польщі» (Kudla v. Poland), №30210/96, §158.

<sup>105</sup>Справи «Сілвер та інші проти Сполученого Королівства» (Silver and Others v. UK), №5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, §113; «Кудла проти Польщі» (Kudla v. Poland), №30210/96, §157.

<sup>106</sup>Питання корпоративної соціальної відповідальності і позитивних зобов'язань держав щодо захисту прав людини роз'яснюються в п.19 і 28 Пояснювального меморандуму.

му етапі процесу, прозорість щодо типів процесів та наявних результатів, а також засобів моніторингу їхньої реалізації), справедливими (доступ до джерела інформації, консультації та експертиза), прозорими та здатними забезпечити такі засоби правового захисту, що цілковито відповідали б міжнародним стандартам у сфері прав людини, що застосовуються безпосередньо до фізичних осіб<sup>107</sup>.

- 105.** Інтернет-користувачам повинна бути надана чітка та прозора інформація щодо наявних засобів правового захисту. Ця інформація повинна бути частиною умов користування та (або) надання послуг, інших інформаційних матеріалів і політики провайдерів Інтернету/Інтернет-послуг. Інтернет-користувачам повинні бути надані практичні й доступні інструменти, що дозволять їм звертатися до провайдерів Інтернету/Інтернет-послуг із проблемними питаннями. Вони повинні мати можливість звертатися з запитом на інформацію і клопотаннями про компенсацію. Прикладом засобу правового захисту, що може бути наданий Інтернет-користувачам, є лінії довіри або гарячі лінії, які створюють провайдери Інтернет-послуг чи асоціації захисту споживачів, до яких можуть звертатися Інтернет-користувачі у разі порушення їхніх прав та прав інших осіб. Консультації можуть надавати органи державної влади та (або) інші національні правозахисні установи (омбудсмени), органи захисту даних, регулятори електронного зв'язку, громадські консультативні органи, правозахисні асоціації чи асоціації цифрових прав або організації споживачів.
- 106.** Інтернет-користувачі повинні бути захищені від кіберзлочинності. Держави, що підписали Будапештську конвенцію, взяли на себе зобов'язання захищати громадян від кримінальної діяльності й злочинів у Інтернеті. Інтернет-користувачі цілком обґрунтовано можуть розраховувати на захист від кримінальної діяльності або кримінальних злочинів, що вчиняються в Інтернеті або з використанням Інтернету.
- 107.** У центрі уваги перебувають злочини проти конфіденційності та цілісності комп'ютерних даних і систем, а також злочини, пов'язані з комп'ютерами. Тут не розглядаються злочини, пов'язані з контентом (дитяча пор-

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



нографія, порушення авторських прав), оскільки вважається, що вони частково розглядаються в тих частинах Посібника, які присвячені правам дітей. Захист правовласників розглядається як такий, що стосується інтересів цієї конкретної групи, а не інтересів Інтернет-користувачів. Питання перехоплення і спостереження за повідомленнями також розглядаються в розділі про приватне життя і захист даних.

- 108.** Інтернет-користувачі мають законний інтерес у безперешкодному управлінні, функціонуванні та контролі над їхніми комп'ютерними системами. Вони повинні бути захищені від незаконного доступу до комп'ютерних систем у цілому або їх окремих частин, включаючи апаратну частину, компоненти, дані, що зберігаються, та встановлену систему, директорію, трафік і пов'язані з контентом дані. Це також передбачає захист від несанкціонованого вторгнення в комп'ютерні системи і дані (хакерство, злом або інші форми вторгнення в комп'ютер), яке може створювати перешкоди для користувачів систем в Інтернеті і для використання даних, таких як доступ до конфіденційних даних (паролі, інформація, таємниці тощо)<sup>108</sup>.
- 109.** Інтернет-користувачі повинні бути захищені від втручання в комп'ютерні дані, зокрема, від використання шкідливих кодів (наприклад, вірусів і троянських програм)<sup>109</sup>. Вони також повинні бути захищені від втручання в роботу комп'ютерних або телекомунікаційних систем шляхом внесення, передачі, пошкодження, видалення, змінення або знищення комп'ютерних даних<sup>110</sup>, наприклад, програм, що викликають атаки «відмова в обслуговуванні», шкідливих кодів, таких як віруси, які перешкоджають або значно сповільнюють роботу системи чи програми, що надсилають великі обсяги електронних листів отримувачу з метою блокування комунікаційних функцій системи (спам). Буде це адміністративним чи кримінальним правопорушенням – залежить від національного законодавства.
- 110.** Інтернет-користувачі повинні бути захищені від комп'ютерного шахрайства, пов'язаного з несанкціонованим створенням або зміною даних таким чином, що вони набувають нової доказової сили у ході юридичних процедур, які ґрунтуються на автентичності інформації, що міститься в даних<sup>111</sup>.

<sup>108</sup>Будапештська конвенція про кіберзлочинність, ст. 2, Пояснювальна доповідь, §44-50.

<sup>109</sup>Там само, ст. 4, Пояснювальна доповідь, §60-61.

<sup>110</sup>Там само, ст. 5, Пояснювальна доповідь, §65-69.

<sup>111</sup>Там само, ст. 7, Пояснювальна доповідь, §81.

- 111.** Інтернет-користувачі мають законний інтерес щодо захисту активів, які надаються або управляються в комп'ютерних системах (електронні фонди, депозити). Вони повинні бути захищені від шахрайських комп'ютерних маніпуляцій, що завдають пряму економічну або майнову шкоду майну Інтернет-користувача (гроші, матеріальні та нематеріальні активи, що мають економічну цінність), як, наприклад, шахрайство з кредитними картками<sup>112</sup>.
- 112.** Будь-які заходи безпеки, спрямовані на захист Інтернет-користувачів від кіберзлочинності, повинні повною мірою відповідати стандартам ЄКПЛ і, зокрема, вимогам щодо права на приватне і сімейне життя та права на свободу вираження поглядів<sup>113</sup>.
- 113.** Інтернет-користувачі мають право на справедливий суд, закріплений статтею 6 ЄКПЛ. Це передбачає визначення громадянських прав і обов'язків або кримінальної відповідальності у зв'язку з діяльністю Інтернет-користувачів. Зокрема, це стосується ключових принципів, проголошених Судом, а саме: права на справедливий та публічний розгляд справи в розумні строки незалежним і неупередженим судом; права на звернення до суду, остаточне вирішення спору, обґрунтоване судові рішення і його виконання; права на змагальне провадження в суді та рівні можливості сторін тощо.
- 114.** Суд у справах, не пов'язаних з Інтернетом, встановив загальні принципи щодо якості здійснення правосуддя (незалежність, неупередженість, компетентність суду), захисту прав сторін (справедливе слухання, рівні можливості 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 всіх внутрішніх засобів правового захисту, що були доступними та чинними протягом шести місяців<sup>114</sup> із дати прийняття остаточного рішення.

<sup>112</sup> Там само, ст. 8, Пояснювальна доповідь, §86-88.

<sup>113</sup> Там само, ст. 15.

<sup>114</sup> Після набуття чинності Протоколу №15 до ЄКПЛ цей строк буде складати чотири місяці.



**Посібник з прав людини для інтернет-користувачів** допоможе дізнатися про права людини в інтернеті, їх можливі обмеження і доступні засоби правового захисту. Посібник не встановлює нові права – він ґрунтується на нормативно-правових документах Ради Європи, передусім

Європейській конвенції з прав людини. Основний принцип посібника – права та основоположні свободи людини діють однаковою мірою офлайн та онлайн.

Більше інформації про посібник – <http://www.coe.int/en/web/internet-users-rights/guide>

**Рада Європи** є провідною організацією із захисту прав людини континенту. Вона включає в себе 47 держав-членів, 28 з яких є членами Європейського союзу. Усі держави-члени Ради Європи підписалися під Європейською конвенцією з прав людини – угоду, спрямовану на захист прав людини, демократії та верховенства закону. Європейський суд з прав людини контролює здійснення Конвенції у державах-членах.

<http://www.coe.int/en/web/kyiv>

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

Більше інформації про ЄС: <http://eeas.europa.eu/delegations/ukraine>

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE