Генеральний Секретаріат

Генеральний директорат
з прав людини та верховенства права

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DGI(2014) 31
4 грудня 2014 року

ПОРУШЕННЯ ПРАВ ЛЮДИНИ ОНЛАЙН

Підготовлено
міжнародною неприбутковою асоціацією
«Європейські цифрові права» (EDRi)

Автори та редактори:

Джо Макнеймі, виконавчий директор, EDRi
Маріант Фернандес Перес, молодший менеджер з адвокації, EDRi

За підтримки:

Міжнародної мережі з прав дитини, CRIN, https://www.crin.org/
Дієго Наранжо, менеджера з адвокації, EDRi
Поліни Малаї, стажера, EDRi
Ангели Собольчакової, стажера, EDRi

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

Фінансується Європейським Союзом та Радою Європи

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Впроваджується Радою Європи

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

Дослідження «Порушення прав людини онлайн» є практичним роз'ясненням Рекомендації CM/Rec(2014)6 Комітету міністрів державам-членам щодо «Посібника з прав людини для інтернет користувачів» та Пояснювального меморандуму CM(2014)31.

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

ЗМІСТ

ВСТУП

Дане дослідження присвячене аналізу репрезентативних, на думку авторів, **труднощів, пов'язаних із реалізацією європейськими Інтернет-користувачами своїх прав та основоположних свобод**, а також доступних механізмів їх відновлення. Ми посилаємося на практику європейських і національних судів, де це видається доцільним, а також до відповідних доповідей та звітів[1].

Дослідження є практичним роз'ясненням Рекомендації CM/Rec(2014)6 Комітету міністрів державам-членам щодо «Посібника з прав людини для інтернет користувачів»[2] (надалі – «Посібник») та Пояснювального меморандуму CM(2014)31[3] (надалі – «Пояснювальний меморандум»).

Дане дослідження складається з семи розділів.

Розділи 1-6 присвячені онлайн порушенням прав людини, що вказані у Посібнику та пов'язані з доступом та принципом недискримінації (1), свободою вираження поглядів та інформації (2), свободою зібрань, об'єднань та участі (3), захистом приватного життя та персональних даних (4), освітою та грамотністю (5), а також правами дітей і молоді (6). Кожен розділ, **в свою чергу, містить три підрозділи,** а саме: *вступ*, у якому надається загальне бачення ситуації; *дослідження судових справ* на предмет наявності правових викликів та засобів відновлення порушених прав і свобод; та *висновок*.

Розділ 7 підсумовує дослідження та робить короткий загальний аналіз **засобів правового захисту**, спрямованих на боротьбу з порушеннями прав людини в онлайн середовищі. У дослідженні показано, що у деяких випадках дійсно існують доступні для європейських Інтернет-користувачів засоби правового захисту. Інші випадки, навпаки, свідчать про необхідність внесення відповідних змін на законодавчому та практичному рівнях. Зрештою, деякі приклади свідчать про необхідність формування нового способу мислення з метою оцінки впровадження міжнародного законодавства щодо прав людини, яке традиційно орієнтується на рівень держави, у приватному суспільному просторі, яким є Інтернет.

[1] Остання дата доступу до усіх посилань - 28 листопада 2014 року.

[2] Рада Європи, Рекомендація CM/Rec(2014)6 Комітету міністрів державам-членам «Посібник з прав людини для Інтернет-користувачів» від 16 квітня 2014 року [Електронний ресурс]. – Режим доступу: https://wcd.coe.int/ViewDoc.jsp?id=2184807.

[3] Рада Європи, Пояснювальний меморандум до Рекомендації CM/Rec(2014)6 Комітету міністрів державам-членам «Посібник з прав людини для інтернет-користувачів» від 16 квітня 2014 року [Електронний ресурс]. – Режим доступу: https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282014%2931&Language=lanEnglish&Ver=addfinal&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864.

1 ДОСТУП ТА НЕДИСКРИМІНАЦІЯ

1.1. Вступ

Як зазначається в Пояснювальному меморандумі до Посібника, концепція доступу до Інтернету як фундаментального права людини обговорювалася протягом досить тривалого часу.

Питання доступу до Інтернету як права людини, хоча і є важливим обговоренням саме по собі , створює ризики залишити поза увагою увесь комплекс прав, які охоплює визначення «доступ та недискримінація».

Сучасний Інтернет 2014 року суттєво відрізняється від того, яким він був у 2004 році, коли відбувся перший прорив у масовому підключенні, а також від далекого 1994 року, коли він лише починав набувати популярності. «Право людини на доступ» саме по собі не має великого значення – питання полягає в тому, до чого саме надається відповідний доступ. На відміну від 1994 року наразі Інтернет є частиною повсякденного життя величезної кількості людей та сприяє реалізації ними своїх демократичних і економічних прав. З іншого боку, цілком обґрунтовано можна заперечити, що право на підтримання належного рівня функціональності Інтернету є навіть більш вагомим для суспільства, ніж доступ сам по собі. Адже доступ втратить свою важливість, якщо мережа більше не сприятиме та не захищатиме здійснення фундаментальних прав людини.

Свобода отримувати та передавати інформацію, зокрема в так званій всесвітній павутині «Веб 2.0», складається з принаймні трьох окремих частин. По-перше, для отримання інформації особі необхідно отримати доступ до мережі, що зазвичай надається через Інтернет-провайдера (*скорочено ІП*). По-друге, для передачі інформації повідомлення особи не повинні бути об'єктом блокування та/або видалення провайдером з боку отримувача. По-третє, будь-яка онлайн платформа, що використовується для комунікації, не повинна встановлювати надмірних обмежень.

У даному розділі розглядається випадок, пов'язаний з позбавленням доступу до Інтернету в Ірландії, що став наслідком самовільного, позасудового покарання за повторювані звинувачення у незаконному завантаженні контенту.

1.2. Судова практика - справа *Eircom*

Відключення від Інтернету

Посібник пояснює, що відключення від мережі Інтернет, яке, серед іншого, може припинятися за умовами договору, повинне застосовуватися в останню чергу. Більш детально дане положення викладене у Пояснювальному меморандумі, де зазначається, що будь-яке подібне втручання повинне відповідати умовам, закріпленим у пункті 2 статті 10 Конвенції. Далі наводиться важливе уточнення, що «захід, який може вплинути на доступ осіб до Інтернету, передбачає відповідальність держави згідно зі статтею 10».

Колишній ірландський монопольний оператор *Eircom* прийняв рішення впровадити «добровільну» систему посилення захисту авторських прав, що може призводити до одностороннього відключення доступу до Інтернету. Ступінь «добровільності» (як це часто трапляється у випадках приватного правозастосування в онлайн середовищі) викликає чимало запитань з огляду на те, що дану систему було запроваджено в рамках вирішення судової справи.

Відповідно до запровадженого механізму підрядники, які працюють у музичній індустрії, повинні збирати IP адреси користувачів *Eircom* в однорангових (peer-to-peer) мережах та встановлювати ті адреси, які, на їхню думку, причетні до піратського обміну контентом. Після цього такі адреси передаються компанії *Eircom*[4].

Eircom, в свою чергу, автоматично розглядає такі звинувачення як обґрунтовані, та визначає осіб, які, на його думку, користувалися зазначеними IP адресами на момент заявлених порушень, та оголошує «попередження» користувачам, закликаючи їх припинити протиправну діяльність. Після трьох попереджень абонент позбавляється доступу до мережі на тиждень, після чотирьох – на рік.

Правові виклики

Керуючись угодою сторін у справі, яка призвела до запровадження такої системи, Верховний суд Ірландії мав прийняти рішення про відповідність угоди нормам про захист персональних даних. На підставі цього рішення ірландський орган захисту даних видав «виконавчий наказ»[5].

У даному рішенні головуючий суддя спростував аргументи про те, що Інтернет є «аморфним неземним утворенням, що регулюється нормами, які суперечать фундаментальним принципам прав людини»[6]. Він також заперечив аргумент про те, що Інтернет «переписав правові норми кожної країни, через яку він проходить». Окрім того, з більш ніж незрозумілих причин, суддя зазначив, що «дитяча порнографія, наприклад, залишається дитячою порно-

[4] Текст угоди, що став відомим внаслідок витоку інформації, було опубліковано на веб-сайті Torrentfreak у 2009 році [Електронний ресурс]. – Доступний за посиланням: http://torrentfreak.com/leaked-document-reveals-eircom-deal-with-irish-riaa-090808/.

[5] *EMI Records та Ors проти EircomLtd*

[6] *EMI Records та Ors проти EircomLtd*, пункт 5

графією незалежно від того, чи її було надіслано поштою, чи передано за допомогою цифрових засобів»[7].

Зрештою, перейшовши до деталей справи, суддя зробив некоректну заяву про те, що «програмне забезпечення для однорангового нелегального завантаження контенту, з іншого боку, надається сайтами на зразок *Pirate Bay*». Неправильно стверджувати, що однорангове завантаження програмного забезпечення є важливою функцією сайтів на зразок *Pirate Bay*. Окрім того, некоректно посилатися на «програмне забезпечення для однорангового незаконного завантаження», оскільки існує лише «однорангове програмне забезпечення», яке може бути використане для законних і незаконних цілей[8]. Той факт, що суддя дійшов однозначного висновку про відсутність законних цілей використання однорангового програмного забезпечення, викликає значні сумніви щодо розуміння ним підстав, на основі яких було зроблено попередження та позбавлено доступу.

У країні, 73% населення якої проживає у сільській місцевості[9], де *Eircom* є оператором, що надає універсальне обслуговування, - за словами судді, людині потрібно лише «прогулятися до центра свого міста, щоб отримати доступ до Інтернету за приблизно 1.50 євро на годину»[10].

Встановлено законом

Суддя описав квазісудовий процес, наслідком результатом якого стало позбавлення користувача доступу до Інтернету наступним чином:

> «За 14 днів до позбавлення доступу до мережі користувачу надсилається повідомлення . Протягом цього часу користувач має право зробити заяву компанії *Eircom* як Інтернет-провайдеру по телефону або через мережу Інтернет. *Eircom* розглядає заяву користувача, не консультуючись з позивачами, відповідно до пункту 2.8 протоколу. Компанія має взяти до уваги індивідуальні умови, які передбачають пом'якшувальні обставини, для того, щоб встановити, чи не підпадає даний випадок під категорію винятків, або перевірити матеріал, який містить факти на користь відсутності порушення як такого. Якщо виконання зазначених вище дій не призведе до скасування чи відхилення протоколу, користувач позбавляється доступу до Інтернету»[11].

Проте в Ірландії немає закону, який би містив процедури, описані суддею. Зазначені процедури не були предметом демократичного обговорення з точки зору їх необхідності або пропорційності. Окрім того, не застосовувалася презумпція невинуватості. Дані, які були отримані від підрядників позивачів, автоматично вважалися правильними. Процедура повністю перебуває під

[7] *EMI Records ma Ors nponu EircomLtd,* пункт 6

[8] *EMI Records ma Ors nponu EircomLtd*, пункт 7

[9] Прес-реліз служби Євростат: Близько 40% населення 27 держав-членів ЄС живуть у міській місцевості, 30 березня 2012 року, [Електронний ресурс]. – Режим доступу: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/1-30032012-BP/EN/1-30032012-BP-EN.PDF.

[10] *EMI Records ma Ors nponu EircomLtd*, пункт 9

[11] *EMI Records ma Ors nponu EircomLtd,* пункт 13

контролем компанії *Eircom*, яка виконує роль судді, присяжних та відповідає за позбавлення доступу.

Припущення про достовірність звинувачень також викликає багато сумнівів. У 2010 році, незадовго після впровадження даного механізму, компанія *Eircom* помилково надіслала 400 листів з попередженнями особам, які, як виявилося, не використовували відповідні IP адреси. Неможливо встановити, скільки всього подібних листів було надіслано. Газета «*The Sunday Times*» повідомила, що помилково обвинуваченим користувачам було надано знижку в розмірі 50 євро від суми їхніх рахунків за користування Інтернетом, що, будучи позитивним кроком, все ж змусило *Eircom* задуматись над уникненням публічного визнання подібних помилок у майбутньому[12].

Суд відзначив обов'язки абонента за контрактом з *Eircom*, а також той факт, що «однією з основних функцій судів відповідно до Конституції є забезпечення виконання законних угод»[13]. Крім того, суд наголосив на основних положеннях контракту з *Eircom*, не звернувши жодної уваги, серед іншого, на доведення, принцип передбачуваності чи презумпцію невинуватості, зокрема у пунктах 5.5, 5.6 та 5.10.

У пункті 5.6 зазначається

> «користувачі не мають права користуватися послугою з метою створення, розміщення або передачі контенту, який порушує права інтелектуальної власності, зокрема, але не виключно, авторські права іншої особи чи організації».

У свою чергу, у пункті 7.1 зазначено, що угоду може бути тимчасово призупинено або розірвано компанією *Eircom* у випадку порушення її умов.

Суд дійшов висновку, що контракт був «законною угодою». Наприклад, питання відповідності несправедливих умов контракту законодавству (зокрема, обов'язку, закріпленого Статутом 27/1995 про несправедливі умови контракту, який вимагає уникати «укладання угод, що є зобов'язуючими для споживача, якщо надання послуг продавцем або постачальником залежить від умови, реалізація якої залежить виключно від його волі») було просто проігноровано.

Право на приватне життя та захист персональних даних

Стаття 1.2. а) Додаткового протоколу до Конвенції Ради Європи № 108 (яка була підписана Ірландією у 2001 році та набрала чинності в цій країні у 2009 році) встановлює, що сторони повинні мати один чи більше органів нагляду, уповноважених брати участь у судовому розгляді або повідомляти компетентним судовим органам про порушення положень внутрішньодержавного права. Уповноважений із захисту персональних даних Ірландії не мав повноважень для участі в даному судовому розгляді або для привернення уваги компетентних судових органів до помічених ним порушень законодавства про захист персональних даних. Відповідно до заяв суду,

[12] *Mark Tighe, Eircom investigated after falsely accusing customers of piracy,* 5 червня 2011 року [Електронний ресурс]. – Режим доступу: http://www.thesundaytimes.co.uk/sto/news/ireland/article642095.ece.

[13] *EMI Records ma Ors protu EircomLtd,* пункт 15

він був позбавлений таких повноважень з огляду на «стурбованість щодо відшкодування його витрат»[14]. Таким чином, існують значні сумніви щодо того, чи Ірландія порушила – і продовжує порушувати – свої зобов'язання за Додатковим протоколом.

Ключовим питанням щодо захисту даних було право представників музичної індустрії в першу чергу та право *Eircom* у другу чергу здійснювати обробку IP адрес користувачів послуг Eircom. З цієї точки зору необхідно було визначити, чи є IP адреси персональними даними. Європейське законодавство не залишає місця для сумнівів. Стаття 2 (а) Директиви 1995/46/ЄС визначає «персональні дані» як «будь-яку інформацію, що пов'язана з ідентифікацією або можливою ідентифікацією фізичної особи («суб'єкта даних»); *особою, яку можна встановити, є така, яка може бути встановлена прямо чи опосередковано*».

За відсутності експертного висновку органу захисту персональних даних Верховний суд Ірландії постановив, що дані, зібрані позивачами, *щоб надати компанії Eircom можливість ідентифікувати відповідних осіб*, не дозволяли встановити особу до того, як вони були передані у власність *Eircom*. Суд також постановив, що після отримання таких даних *Eircom* має законний інтерес діяти у відповідності до, «а також розглядатися іншими як орган, що дотримується законів та Конституції».

Встановлений законом, необхідний та пропорційний

Як було зазначено вище, в Ірландії немає закону, який би регулював порядок відключення фізичних осіб від Інтернету. Не було проведено жодної оцінки щодо того, чи було необхідним покарання, встановлене приватною компанією. Міра покарання (відключення на тиждень, а згодом - на рік) не була розглянута з точки зору її необхідності та пропорційності.

Альтернативи

Суд зазначив, що існували альтернативи послугам *Eircom* передбачаючи, що фізична особа проживала в місті. Проте, для використання функціонально подібних послуг необхідно прийняти умови надання послуг іншого провайдера. При цьому передбачуваність змін у наданні послуг іншими операторами ірландського ринку видається такою ж обмеженою та несправедливою, як і у випадку з *Eircom*. Нижче наводимо декілька прикладів:

> *Vodafone:* «Компанія *Vodafone* може змінювати або призупиняти надання послуг повністю або частково, надаючи або не надаючи відповідне повідомлення, якщо такий захід є на її думку необхідним»[15].
>
> *UPC*: «Компанія *UPC* зберігає за собою право на власний розсуд видаляти матеріали зі своїх серверів і припиняти доступ до Інтернету користувачам, які, на її думку, порушили умови цих Правил для користувачів»[16].

[14] *EMI Records ma Ors проти EircomLtd,* пункт 2

[15] Vodafone, *Terms and conditions for bill pay services* [Електронний ресурс]. – Режим доступу: http://www.vodafone.ie/terms/paymonthly/.

[16] Розділ 17: *Removal of Materials of UPC's «Acceptable Usage Policy»* [Електронний ресурс]. – Режим доступу: http://www.upc.ie/terms/usage-policy/.

Sky Ireland: «Ми маємо право вжити нагальних заходів для контролю, обмеження або припинення (залежно від обставин) надання Послуг у будь-який час (зокрема протягом Мінімального періоду):

(a) без попередження, якщо:

(I) у нас є обґрунтовані підстави вважати, що Послугу було використано у спосіб, заборонений вашим Контрактом (вашими Контрактами) або нашими Правилами користування» .

Можливість уникнути самовільних «правил», які дають змогу (або потенційно дають можливість) Інтернет-провайдерам відключати доступ користувача від мережі на власний розсуд, є обмеженою або взагалі відсутня на ірландському ринку (*Sky* є певним винятком з правила, оскільки компанія принаймні посилається на «обґрунтовані підстави»).

Зрештою, необхідно також звернути увагу на зобов'язання *Eircom* щодо універсального надання послуг: велика кількість абонентів компанії не зможе скористатися послугами альтернативних провайдерів у випадку відключення.

1.3. Висновок

Дана справа свідчить про наявність значних проблем у сфері нормативно-правового регулювання фундаментальних прав доступу та недискримінації в Ірландії. Позиція Верховного суду Ірландії нівелює сутність основних гарантій:

- обмеження накладаються за відсутності чіткого й передбачуваного закону, з очевидним порушенням статті 10(2) Європейської конвенції про захист прав людини та основоположних свобод;
- не було дотримано зобов'язання щодо необхідності та пропорційності обмежень;
- дані, які чітко підпадають під визначення персональних даних відповідно до Конвенції Ради Європи («будь-яка інформація, яка стосується фізичної особи») та Директиви ЄС 1995/46/ЄС, позбавляються захисту за рішенням Верховного суду Ірландії;
- фінансування органу захисту даних в Ірландії позбавило (та, ймовірно, продовжує позбавляти) його можливості втручатися у подібні справи, що порушує Додатковий протокол до Конвенції Ради Європи про захист персональних даних;
- ігноруючи незбалансованість прав, закріплених відповідно до контрактів компанії *Eircom* з клієнтами, Суд постановив, що контракт є «законною угодою»;
- ігноруючи вимогу про те, що обмеження права на приватне життя повинні здійснюватися «згідно із законом» (Стаття 8 Європейської конвенції про захист прав людини (ЄКПЛ), Верховний суд Ірландії, вочевидь, вважає, що діяльність або «сприйняття іншими» діяльності як такої, що спрямована на виконання вимог законодавства, є достатньою правовою підставою для обробки персональних даних.

[17] *Sky Ireland,* «Ваші контракти», Частина I, пункт 9.4 [Електронний ресурс]. – Режим доступу: http://www.sky.com/ireland/__PDF/Broadband_and_Talk_subscription_contract.pdf.

2 СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ ТА ІНФОРМАЦІЇ

2.1. Вступ

Свобода вираження поглядів, як зазначено у статті 10 ЄКПЛ, вважається основою демократичного суспільства. Як було відзначено Європейським судом з прав людини (надалі – «ЄСПЛ»), свобода вираження поглядів є однією з головних умов розвитку демократичного суспільства та самореалізації кожної особи[18]. Користувачі повинні мати право вільно висловлювати свої думки, погляди та ідеї, зокрема політичні переконання та релігійні і нерелігійні погляди, а також шукати, отримувати та передавати інформацію незалежно від кордонів. ЄСПЛ також визнав особливу важливість Інтернету для реалізації фізичними особами їх права на свободу вираження шляхом надання необхідних інструментів для участі у діяльності та обговореннях, що становлять суспільний інтерес[19].

Однак, це право не є абсолютним: репутація інших осіб, право на приватне життя та майнові права повинні поважатися. Мова ворожнечі тією чи іншою мірою заборонена у багатьох країнах: погляди, які спонукають, поширюють, пропагують або виправдовують расову ненависть, ксенофобію, антисемітизм або інші форми ненависті на основі нетолерантності, не підпадають під захист статті 10[20].

2.2. Судова практика – справа *Delfi*

Зобов'язання щодо моніторингу заборонено де-юре, але заохочується де-факто.

Існуючі механізми правозастосування, що застосовуються для боротьби з мовою ворожнечі, дифамацією та іншими порушеннями в онлайн середовищі, які часто підтримуються та заохочуються судами, можуть заходити занадто далеко та мати побічний ефект у вигляді порушення законних прав Інтернет-користувачів.

Такий підхід особливо чітко прослідковується на прикладі процедури «повідомити та вилучити», тобто повідомлення про незаконне розміщення з вимогою вилучити контент (*notice and take down)*, що була запроваджена Директивою ЄС «Про електронну комерцію»[21]. Відповідно до так званих положень «безпечної гавані» для Інтернет-провайдерів (ІП), хостинг-провайдер, серед іншого, захищається від відповідальності за контент третіх сторін, якщо йому невідомо про незаконну діяльність або інформацію, що зберігається на його серверах, та

[18] ЄСПЛ, *Animal Defenders International v. the United Kingdom,* 48876/08, 22 квітня 2013 року, пункт 100.

[19] ЄСПЛ, *Ahmet Yildirim v. Turkey,* 3111/10, 18 грудня 2012 року, пункт 54.

[20] Рада Європи, Рекомендація R (97) 20 Комітету міністрів державам-членам «Про мову ненависті» від 30 жовтня 1997 року.

якщо після того, як йому стало відомо про них, він вживає невідкладних заходів для видалення або унеможливлення доступу до такої інформації.

Крім того, відповідно до статті 15 Директиви «Про електронну комерцію» на провайдерів послуг не накладається загальний обов'язок щодо моніторингу інформації, яку вони передають чи зберігають, включаючи загальний обов'язок здійснювати активний пошук фактів чи обставин, що вказують на незаконну діяльність.

Проте, незважаючи на пряму заборону, закріплену в Директиві, розуміння положення «коли постачальнику стало відомо» поступово розширилося до фактичного заохочення моніторингу та активного пошуку фактів незаконної діяльності з метою уникнення відповідальності за дії третіх сторін в онлайн середовищі. Це створює дисбаланс стимулів для Інтернет-компаній: з одного боку, існує чіткий стимул (відповідальність) для обмеження спілкування, але при цьому відсутній будь-який стимул, крім обслуговування користувачів і зв'язків з громадськістю, для збереження контенту онлайн. Цей дисбаланс підриває принцип передбачуваності, та, відповідно, перешкоджає свободі спілкування.

Здійснення загального моніторингу інформації, яка надається інтернет-користувачами до її розміщенням на веб-сайті *Delfi*, було заохочене Верховним судом Естонії у справі «*Леедо* проти *Delfi*»[22]. Справа стосувалася незаконних коментарів дифамаційного характеру, які були розміщені анонімним Інтернет-користувачем на інформаційному веб-сайті *Delfi* у відповідь на законно опубліковану статтю, яка не містила жодного дифамаційного матеріалу. Компанія *Delfi* дозволяла користувачам коментувати статті та створила власні «правила щодо мови ненависті», якими заборонялися коментарі, що містили погрози, образи, нецензурні висловлювання та непристойності, у тому числі певні ключові слова, а також підбурювання до ворожнечі, насилля і незаконної діяльності. В основу процедури «повідомити та вилучити» була покладена активна участь користувачів, які могли повідомити компанію *Delfi* про неналежні коментарі, які після цього оперативно видалялися. Незважаючи на великою мірою проактивний підхід, компанію було звинувачено у завданні моральної шкоди В. Леедо, який став об'єктом незаконних коментарів до статті, опублікованої *Delfi*.

Верховний суд Естонії постановив, що положення «безпечної гавані», встановлені Директивою «Про електронну комерцію», не застосовувалися до *Delfi* як хостингового сервісу для коментарів. Суд керувався пунктом 42 Преамбули Директиви «Про електронну комерцію», яка встановлює, що положення «безпечної гавані» стосуються лише тих випадків, коли діяльність постачальників

[21] Директива 2000/31/ЕС Європейського парламенту та Ради від 8 червня 2000 року «Про деякі правові аспекти інформаційних послуг, зокрема електронної комерції, на внутрішньому ринку» («Директива про електронну комерцію»).

[22] Вищий суд Естонії, Vjatļeslav Leedo v. AS Delfi, 3-2-1-43-09, 10 червня 2009 року.

інформаційних послуг обмежена технічним процесом дії та наданням доступу до мережі передачі даних[23]. Відповідно до рішення Верховного суду Естонії, на компанію *Delfi* не поширювалася дія положень «безпечної гавані», оскільки вона здійснювала контроль за змістовним наповненням інформації, яка передавалася чи зберігалася, інтегрувала секцію коментарів у свій портал новин і заохочувала користувачів до коментування, а також була економічно зацікавлена в кількості отриманих коментарів[24].

Верховний суд розтлумачив використання положень «безпечної гавані» надзвичайно вузько й повністю проігнорував критерій «коли йому стало відомо» у визначенні хостинг-провайдера, який вважався однією з основних вимог для звільнення Інтернет-провайдерів від відповідальності.

По-перше, компанія *Delfi* оперативно видалила коментарі дифамаційного характеру після отримання повідомлення від пана Леедо і, таким чином, діяла відповідно до Директиви «Про електронну комерцію». По-друге, очевидно, що компанія не закликала користувачів розміщувати коментарі, сповнені ненависті, оскільки у відповідній дисклеймер, розміщеній на сервері, було чітко зазначено, що такі коментарі будуть видалятися. Крім того, компанія встановила автоматичну систему фільтрації для видалення коментарів, які містили певну ненормативну лексику, а також систему «повідомити та вилучити», що також не було визнано Судом достатнім заходом. У тому ж рішенні Верховний суд пішов ще далі і постановив, що в силу функціонування такої системи під час видалення коментарів після отримання повідомлення про їхню невідповідність, компанія *Delfi* здійснювала над ними контроль і, таким чином, могла приймати рішення щодо того, які коментарі публікувати, а які – ні[25]. Такий аналіз виходить із припущення, що рішення компанії щодо (не)законності завжди буде правильним. Той факт, що на практиці компанія зможе лише захистити себе від відповідальності свідомо видаляючи будь-який контент, який у майбутньому може бути визнаний незаконним, означає, що позиція Суду практично *вимагає* від компанії видаляти законний контент.

Крім того, Верховний суд прямо заохочував здійснювати моніторинг контенту та активний пошук (потенційно) незаконного контенту перед його публікацією, зазначивши, що «той факт, що вона [*Delfi*] не використала таку можливість [(не визначила, які коментарі необхідно публікувати, а які - ні)], не означає, що вона не мала жодного контролю над публікацією коментарів»[26]. Така інтерпретація положень «безпечної гавані» Директиви «Про електронну комерцію» суперечить закріпленій у ній забороні вимагати здійснення загального моніторингу, що міститься у статті 15, оскільки Суд прямо заохочує Інтернет-провайдерів здійсню-

[23] *Leedo v. Delfi*, пункт 13.

[24] Там само.

[25] Там само.

[26] Там само.

вати моніторинг та піддавати цензурі контент перед його публікацією як єдині способи уникнути відповідальності за поведінку третіх осіб. Крім того, таке тлумачення є несумісним з Принципом 6 Декларації Ради Європи про свободу спілкування в Інтернеті, відповідно до якої у випадках, коли Інтернет-провайдери зберігають контент, який походить від інших сторін, держави можуть притягнути їх до спільної відповідальності, якщо вони *негайно не видалять або не припинять доступ до відповідної інформації чи послуг після виявлення* їхнього незаконного характеру або, у випадку вимог про відшкодування, після виявлення фактів чи *обставин, які свідчать про незаконну діяльність або інформацію*[27].

Результатом такого вузького тлумачення положень «безпечної гавані» може стати попередня цензура з боку Інтернет-провайдерів та масштабне видалення контенту з метою уникнення відповідальності за дії третіх сторін в онлайн середовищі, що у свою чергу може призвести до незаконного втручання у свободу вираження поглядів користувачами, а також сприяти розвитку культури «вилучення» *(«Web takedown» culture)*.

Складовою цієї проблеми є передбачуваний вплив таких рішень на «реальний світ» – компаніям доведеться адаптуватися, і не обов'язково через використання «найменш обмежувального підходу», що означає, що наслідком такого рішення може стати більш обмежувальна політика, зокрема запровадження попередньої цензури, автоматичного видалення контенту, заборони коментування як такого, реєстрації, які накладатимуть надмірні обмеження на можливість анонімного висловлювання тощо.

ЄСПЛ дійшов висновку, що системи автоматичного фільтрування і «повідомити та вилучити», впроваджені *Delfi*, були недостатніми для гарантування того, що коментарі, опубліковані на Інтернет-порталі, не будуть порушувати особисті права третіх осіб[28]. Дані системи не забезпечували достатнього захисту прав третіх осіб, враховуючи економічний інтерес, що стає очевидним з огляду на кількість коментарів та технічні можливості Інтернет-провайдера[29]. Важко знайти засоби, які становили б альтернативу *попередньому* блокуванню та фільтруванню контенту з метою попередження порушень з боку третіх сторін, які витікають з такого тлумачення. Крім того, незрозуміло, чому Суд надав абсолютну перевагу правам третіх осіб над свободою слова коментаторів.

2.3. Висновок

Зобов'язання здійснювати моніторинг або фільтрувати контент перед його публікацією суперечить вимозі надання ефективних засобів правового захисту. Той факт, що посередники, які мають зобов'язання діяти (тобто ви-

[27] Комітет міністрів Ради Європи, Декларація «Про свободу спілкування в Інтернеті», прийнята 28 травня 2003 року.

[28] ЄСПЛ, *Delfi AS v. Estonia,* 64569/09, 10 жовтня 2013 року. Справа перебуває на розгляді Великої Палати.

[29] Там само, пункт 89.

даляти *потенційно* незаконні повідомлення), майже не мають відповідної зацікавленості у збереженні контенту онлайн, скасовує презумпцію невинуватості, право на компенсацію та тією чи іншою мірою, залежно від ролі посередника в онлайн обговореннях, свободу спілкування.

Відповідно до статті 13 ЄКПЛ кожна особа, чиї права та свободи є обмеженими або порушеними, має право на ефективний засіб правового захисту. Таке право передбачає можливість вимагати компенсації в національних органах у випадку порушення фундаментальних прав. Насправді, національний орган у розумінні статті 13 не обов'язково повинен бути судовим[30]. Проте, для того, щоб захист, який він забезпечує, був насправді ефективним, такий орган має бути незалежним. Приватні сторони, як, наприклад, компанія *Delfi* у зазначеній справі, не зобов'язані зберігати контент онлайн та, як правило, мають власні умови надання послуг, які дозволяють довільну поведінку з їхнього боку.

Крім того, ефективні засоби правового захисту повинні бути в наявності, про них повинні знати, вони мають бути доступними, надаватися за помірну плату та забезпечувати належне відшкодування. Видається малоймовірним, щоб таким незалежним органом влади, спроможним проводити належні розслідування порушень прав людини став Інтернет-провайдер, який сам боїться відповідальності. Результати такого процесу прийняття рішень не будуть ні об'єктивними, ні повністю незалежними, оскільки посередник переслідуватиме власні комерційні інтереси та небезпідставно може заявити про право керувати послугами на власний розсуд. У справі *Telekabel*, що розглядалася Судом Європейського Союзу (СЄС)[31], Суд виходив із припущення, що примушування (припис) Інтернет-посередника обмежити доступ врівноважувалося іншими неконкретизованими зобов'язаннями з дотримання фундаментальних прав користувачів.

Крім того, важливо пам'ятати, що держави мають першочергове зобов'язання забезпечувати, щоб їхні правові системи надавали адекватні й ефективні гарантії реалізації свободи вираження поглядів, які можуть бути виконані примусово[32]. Це означає, що, якщо припущення у справі *Telekabel* є неправильним, правова система повинна бути оновлена. Небезпечно залишати на розсуд приватного сектору встановлення належного балансу між фундаментальними правами, оскільки це призводить до прийняття самовільних рішень, що найчастіше відбувається у випадку незбалансованості стимулів. Також залишається сумнівним питання про те, чи можна обґрунтовано вимагати у посередників прийняття дискреційних рішень щодо (не)законності висловів третіх осіб ще до того, як будь-хто встигне висловити заперечення проти них.

[30] ЄСПЛ, *Kudla v. Poland,* 30210/96, 26 жовтня, пункт 157.

[31] *«UPC Telekabel Wien GmbH проти Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH»,* C-314/12, 27 березня 2014 року.

[32] КПЛ, Звіт Джона Раггі, Спеціального представника Генерального секретаря на тему прав людини і транснаціональних корпорацій та інших підприємств. Керівні принципи підприємницької діяльності в аспекті прав людини: реалізуючи курс ООН «Захист, повага і засоби правового захисту». A/HRC/12/31, 21 березня 2011 року. Див принцип 25.

3 ЗІБРАННЯ, ОБ'ЄДНАННЯ ТА УЧАСТЬ

3.1. Вступ

Кожен має право на свободу мирних зібрань і об'єднань використовуючи Інтернет. Крім того, кожен має право обирати засоби для здійснення цих прав. Дані права закріплені у статті 11 (1) ЄКПЛ. У Пояснювальному меморандумі також зазначається, що «у п. 2 статті 10 ЄКПЛ передбачено мало свободи дій щодо обмежень у контексті політичних заяв або обговорень із питань, що становлять суспільний інтерес»[33]. Пояснювальний меморандум визначає права, які підлягають виконанню за цією статтею: право на онлайн протест, підписання петицій он-лайн, участь у кампаніях та обговореннях, а також право на створення суспільних груп або професійних спілок. Крім того, право на свободу мирних зібрань та об'єднань передбачає також обов'язок держави надавати громадянам засоби електронного врядування для того, щоб останні могли скористатися суспільними послугами.

З точки зору окремого індивіда, Інтернет надає можливість мобілізуватися та проводити демонстрації онлайн без додаткових витрат або необґрунтованих обмежень. Проте, наразі найбільші труднощі викликає забезпечення однакового рівня захисту таких класичних прав онлайн та офлайн.

У даному розділі розглядаються приклади використання державними органами Інтернету та телекомунікаційних мереж з *метою впровадження попереджувальних заходів нагляду*, що порушує право на свободу мирних зібрань та об'єднань онлайн як безпосередньо, так і через «охолоджувальний ефект». Ми вважаємо, що здійснення через Інтернет основоположного права, закріпленого у статті 11, обмежується через надто часте посилання органами державної влади на доволі розмите виключення «з міркувань національної безпеки». Зрештою, невідповідними є й самі засоби правового захисту, доступні користувачам мережі.

3.2. Судова практика – онлайн зібрання та об'єднання в соціальні групи

Добровільні заходи, що запроваджуються соціальними медіа

Соціальні медіа платформи (наприклад, *Twitter, Facebook, YouTube, LinkedIn*, форуми для обговорень або веб-сайти онлайн кампаній) є приватними організаціями, бізнес-модель яких заснована на наданні безкоштовного місця для проведення зібрань та розширення можливостей для участі в обмін

[33] Пояснювальний меморандум, пункт 60.

на право використання персональних даних користувачів для рекламних цілей. Проте, відіграючи надзвичайно важливу роль у реалізації онлайн прав, соціальні медіа платформи також розглядаються органами державної влади як ключові суб'єкти для здійснення нагляду та накладення різноманітних обмежень на осіб, яких навіть не було звинувачено чи визнано винними в порушенні закону.

Яскравим прикладом є Стандарти громади *Facebook* щодо насильства та погроз, у яких зазначено, що:

> «організації, задіяні у терористичній або насильницькій кримінальній діяльності, не можуть бути представлені на нашому веб-сайті». Ми також забороняємо просування, планування або святкування будь-яких ваших дій, якщо вони призвели або могли призвести до завдання фінансової шкоди іншим особам, включаючи крадіжки та вандалізм»[34].

Таке поєднання заборон, пов'язаних із порушенням кримінального та цивільного законодавства, а також просто неналежної поведінки, викликає питання про те яким чином і як це підсилює державне законодавство, а також відповідальність приватної компанії, яка є домінуючою на ринку. В умовах постійно зростаючого переліку часто доволі дивних заборон, які накладаються *Facebook*, необхідно розглянути питання передбачуваності регулювання свободи спілкування[35]. Враховуючи, що приблизно чверть європейських мобільних операторів пропонують необмежений доступ до *Facebook* (у той час, як за доступ до інших сайтів стягується відповідна плата), рівнозначні альтернативи стають все менш доступними у «відкритому» Інтернеті[36].

Політику *Facebook* щодо того, що є дозволеним, не можна спрогнозувати. Наприклад, у 2013 році відповідно до політики компанії дозволялося розміщувати відео обезголовлювання людей[37], але в той же час заборонялися зображення матерів, які годують груддю. Процес розгляду компанією повідомлень про зловживання також було піддано критиці[38].

---

[34] Див. [Електронний ресурс]. – Режим доступу: https://www.facebook.com/communitystandards/.

[35] Див., наприклад, Megan Gibson, *An Effin Shame: Facebook Blocks Irish Town for 'Offensive' Name, Time*, 6 грудня 2011 року, [Електронний ресурс]. – Режим доступу: http://newsfeed.time.com/2011/12/06/an-effin-shame-facebook-blocks-irish-town-for-offensive-name/; або Lauren Berlekamp, March Against Monsanto Event Removed by Facebook, [Електронний ресурс]. – Режим доступу: http://ecowatch.com/2013/08/20/facebook-censors-march-against-monsanto/.

[36] Anne Morris, Report: *45% of operators now offer at least one zero-rated app, FierceWireless: Europe*, 15 липня 2014 року, [Електронний ресурс]. – Режим доступу: http://www.fiercewireless.com/europe/story/report-45-operators-now-offer-least-one-zero-rated-app/2014-07-15.

[37] Bianka Bosker, *Beheadings Belong On Facebook, Huffington Post*, 22 жовтня 2013 року [Електронний ресурс]. – Режим доступу: http://www.huffingtonpost.com/2013/10/22/facebook-beheading-videos_n_4144886.html.

[38] Emma Barnett, *Facebook in new row over sharing users' data with moderators, The Telegraph*, 3 березня 2012 року [Електронний ресурс]. – Режим доступу: http://www.telegraph.co.uk/technology/facebook/9119090/Facebook-in-new-row-over-sharing-users-data-with-moderators.html.

На відміну від позиції *Facebook*, правила та політика соціальної мережі *Twitter* у сфері образливого контенту видаються більш раціональними:

> «Користувачам дозволяється розміщувати контент, у тому числі потенційно провокаційний контент, за умови, що він не порушує правила та Умови обслуговування мережі *Twitter*. *Twitter* не відслідковує контент і не видаляє потенційно образливий матеріал, якщо він не порушує правила та Умови обслуговування. Якщо ви вважаєте, що контент або дії, про які ви повідомляєте, заборонені в межах вашої юрисдикції, зверніться, будь ласка, до місцевих органів влади для проведення ними уважної оцінки відповідного контенту або дій з точки зору можливих порушень місцевого законодавства (...)»[39].

У даному випадку оператор знову є верховним суддею та займає виняткову позицію в комунікаційній сфері.

Крім того, органи державної влади проводять усе більше зустрічей з представниками соціальних мереж (наприклад, Міністри ЄС у 2014 році)[40] для обговорення можливих добровільних заходів, які можуть бути інкорпоровані в умови користування соціальними мережами. Подібним чином втручання Роберта Ханнігана, директора британського центру контролю за комунікаціями *GCHQ*[41], у діяльність газети «*The Financial Times*» у листопаді 2014 року важко розцінити інакше, аніж як примус до здійснення нагляду та цензури, порушуючи при цьому принцип верховенства права[42]. Такий примус було виведено на новий рівень у листопаді 2014 року, коли *Facebook* (але не органи нагляду, які здійснювали над ним моніторинг) став об'єктом публічної критики у зв'язку з тим, що представники мережі не відстежили та не проінформували владу про запис, розміщений особою, яка згодом вбила військового[43].

Скандал «Handygate» у Німеччині

У лютому 2011 року антифашистські групи організували у Дрездені демонстрацію проти маршу представників правого крила, що повинен був проходити в місті. У якості превентивного заходу поліція Німеччини скористалася положеннями статті 129 Кримінального кодексу Німеччини для перехоплення усіх даних телекомунікаційного трафіку провайдерів мобільного зв'язку з метою збирання метаданих про мобільну телефонну активність у певних частинах

[39] Twittter, *Abusive behavior policy* [Електронний ресурс]. – Режим доступу: https://support.twitter.com/articles/20169997.

[40] Європейська комісія, прес-реліз: Спільна заява Мальмстрьом та Альфано на неофіційному міністерському обіді з представниками IT-компаній, 9 жовтня 2014 року [Електронний ресурс]. – Режим доступу: http://europa.eu/rapid/press-release_STATEMENT-14-304_en.htm.

[41] GCHQ означає *Government Communications Headquarters* (Командування урядових комунікацій).

[42] Robert Hannigan, *The web is a terrorist's command-and-control network of choice, Financial Times,* 3 листопада 2014 року [Електронний ресурс]. – Режим доступу: http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html.

[43] Jack Straw, *"Facebook's arrogance and Snowden's hypocrisy put us all at risk: From an ex-Home Secretary, a devastating attack on the internet giants and the traitor beloved by the chattering class",* Daily Mail, 28 листопада 2014 року [Електронний ресурс]. – Режим доступу: http://www.dailymail.co.uk/debate/article-2852535/Facebook-s-arrogance-Snowden-s-hypocrisy-risk-ex-Home-Secretary-devastating-attack-internet-giants-traitor-beloved-chattering-class.html.

міста. Згодом зібрану поліцією інформацію було використано в 45 кримінальних справах для доведення участі підозрюваних. За оцінками, поліція зібрала інформацію про трафік принаймні 40.000 людей та отримала близько одного мільйону записів даних. Метод, який було використано поліцією для збору необхідних даних, залишається невідомим[44].

Після того як про інцидент стало відомо громадськості, поліція та державні посадовці вдалися до дезінформації, що лише посилило загальне обурення. Наприклад, було оголошено, що збір інформації стосувався лише даних про трафік, проте пізніше, з матеріалів кримінальних справ стало очевидно, що поліцією також здійснювався збір особистої інформації та змісту телекомунікацій.

Передбачено законом

Єдиною підставою введення обмежень державною владою права на свободу мирних зібрань та об'єднань є визначення застосування обмежень в законі, а також необхідність таких обмежень у демократичному суспільстві та їхня пропорційність відповідно до статті 11 (2) ЄКПЛ.

Обговорення *ad hoc* з представниками онлайн служб щодо вжиття ними довільних заходів для боротьби з тероризмом навряд чи підпадають під цю категорію. У Рекомендації CM/Rec (2012)4 державам-членам «Про захист прав людини у зв'язку з послугами соціальних мереж» Комітет міністрів[45] не лише розглядає онлайн послуги одночасно, як інструмент для захисту основоположних прав, але також приймає певний рівень довільного втручання. Додаток до Рекомендації закликає держави-члени

> «співпрацювати з приватним сектором та громадянським суспільством з метою захисту права користувачів на свободу вираження поглядів, зокрема беручи на себе зобов'язання, разом із провайдерами соціальних мереж, виконувати такі дії: [з-поміж інших] – надавати користувачам чітку інформацію про редакційну політику провайдера соціальної мережі щодо його поводження з потенційно незаконним контентом, а також контентом та діями в мережі, які, на його думку, є неналежними».

Очевидно, що ці зусилля, спрямовані на заохочення обмежень з боку приватних компаній, можуть розширити межі здійснення добровільної онлайн цензури та призвести до більшого непрямого контролю мереж з боку урядів. Типові принципи верховенства права на зразок передбачуваності, пропорційності та відсутності свавілля не дотримуються в діяльності органів державної влади.

---

[44] Kees Hudig, *Dresden «Handygate» scandal and the persecution of anti-fascist activists //* Statewatch Journal. - Том 21. - № 3. - Липень-вересень 2011 року [Електронний ресурс]. – Режим доступу: http://database.statewatch.org/article.asp?aid=31736.

[45] Рекомендація CM/Rec(2012)4 Комітету міністрів державам-членам «Про захист прав людини у зв'язку з послугами соціальних мереж», 4 квітня 2012 року [Електронний ресурс]. – Режим доступу:https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

Держава заохочує соціальні мережі до добровільної фільтрації та потенційного блокування доступу до онлайн контенту або до забезпечення «активнішої співпраці з боку технологічних компаній», як це прямо вимагається Центром *GCHQ*. Відповідно до умов обслуговування *Facebook* стає зрозумілим, що превентивне видалення контенту є можливим, при цьому чіткі правила для такого видалення відсутні. Ще більше питань викликає те, що законність онлайн контенту визначається приватними організаціями, а не судом, що створює ризик безкарного порушення закону в разі, якщо держава повністю покладатиметься на *ad hoc* правозастосування з боку приватного сектору.

Збір поліцією Німеччини телекомунікаційних даних про учасників демонстрації є порушенням основоположних прав участі, зокрема права на свободу зібрань та об'єднань. Оскільки цей випадок отримав широкий розголос у пресі, існує ризик виникнення «охолоджувального ефекту», пов'язаного з небажанням людей бути зафіксованими в якості учасників демонстрації або їхньою відмовою від використання мобільних пристроїв, що, наприклад, призведе до скорочення використання соціальних мереж учасниками демонстрацій.

Як зазначено в пункті 62 Пояснювального меморандуму, «право на протест однаковою мірою застосовується як в режимі онлайн, так і в режимі офлайн». Відповідно до права на свободу мирних зібрань, державна влада має поважати організацію таких зібрань з використанням Інтернету або телекомунікаційних мереж.

Поліція Німеччини виправдовує контроль за телекомунікаційною інформацією статтею 129 Кримінального кодексу Німеччини, згідно з якою поліції надаються широкі повноваження для боротьби з серйозними злочинами. Як наслідок, поліція попередньо зібрала та використала в кримінальному провадженні непропорційно значний обсяг персональної інформації. ЄСПЛ вже стикався з подібними обставинами у справі «Крюслен проти Франції» (1990), що стосувалася прослуховування телефону поліцією та подальшого використання записів як доказу в кримінальному провадженні. ЄСПЛ визнав порушення статті 8 Конвенції. У пункті 33 свого рішення ЄСПЛ зазначив:

> «Прослуховування та інші форми перехоплення телефонних розмов вважаються серйозним втручанням в приватне життя й кореспонденцію, і тому **підставою для них повинен бути «закон», який в цій частині повинен бути особливо точним. Потрібні чіткі й детально розроблені правила проведення подібних оперативних заходів, особливо з огляду на те, що відповідна технологія постійно розвивається і ускладнюється».**

Свобода мирних зібрань була обмежена державною владою до та під час демонстрації. Контроль телефонних комунікацій був здійснений відповідно до законодавства, проте конкретні норми, які було застосовано, залишаються невідомими. Така діяльність може призвести до значного «охолоджувального ефекту» на учасників демонстрацій, оскільки навіть перебування

поруч з місцем їхнього проведення призведе до збирання та зберігання даних особи.

3.3. Висновок

Інтернет і телекомунікаційні мережі надають можливість відстежувати онлайн діяльність користувачів, які не вжили заходів самозахисту.

Ситуація є набагато заплутанішою з огляду на добровільні заходи, введені в результаті заохочення з боку національних урядів. Майже немає згоди щодо того, наскільки «заохочення» зачіпає негативні зобов'язання держав за ЄКПЛ. Крім того, незрозуміло, яким чином має бути досягнуто балансу між свободою укладання договорів, передбачуваністю та свободою вираження поглядів. У результаті право на відшкодування у зв'язку з «добровільними» обмеженнями, накладеними соціальними мережами у відповідь на примус з боку національних урядів, наразі залишається невизначеним.

Органи влади Німеччини порушили право на свободу мирних зібрань та об'єднань, а також право громадян на приватне життя, здійснивши непропорційний збір інформації та контроль за комунікаціями до виникнення конкретної загрози і за відсутності чіткого обґрунтування таких дій. Єдиним засобом правового захисту, доступним для громадян міста, є подання офіційного запиту до поліції щодо того, збирання яких саме даних було здійснено, і після отримання позитивної відповіді - ініціювання судового розгляду.

Загалом, наведені вище приклади свідчать про те, як основоположні права користувачів на мирні зібрання, об'єднання та участь можуть порушуватися через пряму й опосередковану діяльність органів державної влади.

4 ПРИВАТНЕ ЖИТТЯ І ЗАХИСТ ДАНИХ

4.1. Вступ

Право на приватне життя захищається статтею 8 ЄКПЛ, яка, серед іншого, стосується права на захист персональних даних. Незважаючи на те, що такі права не є абсолютними, необхідні певні гарантії, зокрема законодавче встановлення обмежень, їхня необхідність і надання переваги найменш обмежувальній альтернативі.

Право на приватне життя, закріплене у ЄКПЛ, більш детально розглядається в Конвенції №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Як зазначається у Пояснювальному меморандумі, «Конвенція №108 охоплює всі операції, що здійснюються в Інтернеті у зв'язку зі збиранням, зберіганням, зміною, видаленням та відновленням чи поширенням персональних даних»[46].

Цей розділ присвячено праву на видалення та заперечення проти обробки персональних даних в контексті справи «*Google Spain SL, GoogleInc*. проти Іспанського агентства захисту персональних даних (*AEPD*) та Маріо Костехи Гонсалеса», C-131/12, рішення від 13 травня 2014 року (надалі – «справа Костехи» або «судове рішення у справі Костехи»).

4.2. Судова практика– справа Костехи

Справа стосувалася пана Костехи Гонсалеса, громадянина Іспанії, який поскаржився, що на запит за його ім'ям пошукова система Google видавала посилання на дві сторінки в газеті «*La Vanguardia*», датовані 19 січня та 9 березня 1998 року. Статті стосувалися проведення аукціону з продажу нерухомості, пов'язаного зі стягненням боргів за соціальним страхуванням[47].

Пан Костеха вимагав від газети видалити або змінити відповідні сторінки таким чином, що його персональні дані більше не відображалися. Він також допускав можливість використання газетами певних інструментів для запобігання відображенню його даних у результатах пошукових систем. «*La Vanguardia*» відмовила в задоволенні його вимог. Після цього пан Костеха направив компанії *Google* вимогу видалити статті з результатів пошуку. Оскільки компанія *Google* також не задовольнила його вимоги, адвокати Костехи подали скаргу до Іспанського агентства захисту персональних даних (*AEPD*). 30 липня 2012 року Агентство *AEPD* наказало *Google Spain* та *Google Inc* задовольнити вимоги пана Костехи. Компанія *Google* подала апеляцію на адміністративне рішення до іспанського суду - *Audiencia Nacional*, який у свою чергу припинив провадження й направив його до Суду Європейського Союзу для отримання попереднього рішення[48].

[46] Пояснювальний меморандум, пункт 67.

[47] Рішення у справі Костехи, пункт 14.

[48] *Google Spain and Google Inc v AEPD and Costeja, Auto Audiencia Nacional,* 27 лютого 2012 року, [Електронний ресурс]. – Режим доступу: http://www.derechoaleer.org/media/files/olvido/AUTO-GOOGLE-oficial-2.pdf (іспанською).

Правові труднощі

Щодо матеріальної сфери дії чинної Директиви ЄС «Про захист персональних даних»[49] пан Костеха вважав, що обробка даних компанією Google порушувала його основоположні права на приватне життя і захист персональних даних, визнаних статтями 7 та 8 Хартії основних прав ЄС. Таким чином, він повинен був мати можливість скористатися своїм правом на видалення даних (стаття 12, b) Директиви ЄС 95/46) та на заперечення проти обробки даних пошуковою системою (стаття 14.1 a) Директиви 95/46). У свою чергу компанія Google заявляла, що європейське законодавство не могло застосовуватися до неї через те, що, на її думку, вона не здійснювала контроль над даними, і, відповідно, жодні обмеження не могли бути накладені на її право здійснення комерційної діяльності.

Суд Європейського Союзу постановив, що збирання, індексація, зберігання та поширення персональних даних через пошукову систему *Google Search* є «обробкою даних»[50]. Усупереч позиції Генерального адвоката[51] Суд встановив, що, незважаючи на те, що пошукові системи «не здійснюють контроль над персональними даними, опублікованими на веб-сторінках третіх сторін», вони визначають мету й засоби зазначеної вище обробки персональних даних. Відповідно, компанія *Google* повинна розглядатися як така, що здійснює контроль за даними. Фактично, вона відіграє ключову роль у забезпеченні доступу до онлайн інформації. Оскільки *Google* забезпечує доступ до онлайн інформації, її діяльність може «суттєво» впливати на такі основоположні права європейських Інтернет-користувачів як право на приватне життя і захист персональних даних[52].

Засоби правового захисту

Серед засобів правового захисту, доступних особам у випадку виявлення ними «недостовірної, невідповідної чи більше невідповідної» інформації «або надмірної [інформації] в контексті [цілей її обробки] та з огляду на завершення строку», виділяють такі:

- вимагати від осіб, які опублікували інформацію, видалити її або використати файл *robots.txt*, мета-теги чи аналогічні механізми для того, щоб проінформувати *Google* про припинення індексування відповідних *URL*- адрес;
- вимагати від пошукової системи та особи, яка розмістила інформацію, вжити відповідних заходів;
- звернутися до відповідного органу захисту персональних даних;
- отримати відновлення/ компенсацію в судовому порядку.

Щодо пошукових систем на зразок *Google* критерії, встановлені Судом, були частково взяті з Директиви «Про захист персональних даних». Відповідно до судово-

[49] Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року.

[50] Рішення у справі Костехи, пункт 28.

[51] Див. висновки [Електронний ресурс]. – Режим доступу: http://curia.europa.eu/juris/document/document.jsf?doclang=ES&text=&pageIndex=0&part=1&mode=DOC&docid=138782&occ=first&dir=&cid=246284.

[52] Пояснювальний меморандум, пункт 67.

го рішення, суб'єкт даних має право вимагати від пошукової системи як контролера даних не відображати результати під час пошуку за іменем суб'єкта даних:

- коли інформація «видається» «неточною, неспіврозмірною, невідповідною або більше невідповідною чи надмірною для цілей обробки»;
- «з огляду на завершення строку»;
- враховуючи «роль, яку відіграє суб'єкт даних у громадському житті», «вразливість приватного життя суб'єкта даних»;
- для створення «справедливого балансу» між основоположними правами суб'єкта даних та законним інтересом Інтернет-користувачів мати доступ до такої інформації;
- за критеріями, які загалом мають пріоритет над економічною зацікавленістю компанії[53].

Виконання

Виконуючи це рішення, пошукові системи не видаляють інформацію. Вона залишається у базі даних та в мережі Інтернет. Єдина зміна пов'язана з тим, що пошук за іменем особи більше не видаватиме відповідних результатів. Проте, висвітлення цього питання в пресі було досить неточним[54], що могло бути спричинене активною піар-компанією *Google*, пов'язаною з реформуванням європейського законодавства про захист персональних даних[55]. Крім того, плутанина у пресі підтверджує результати дослідження Агенції Європейського Союзу з питань основоположних прав (*FRA*) щодо недостатньої обізнаності населення з правами громадян ЄС у сфері захисту персональних даних[56]. *FRA* також «виявила певні бар'єри, зокрема витрати, надмірну тривалість проваджень і труднощі у виконанні вимог, пов'язаних із тягарем доведення»[57].

Рішення повторює, але не уточнює більш широкі питання судової практики Суду Європейського Союзу щодо вимоги до посередників вживати дії, які можуть порушувати інші права (такі як свобода інформації), за наявності обмеженої кількості стимулів проти здійснення такого втручання[58].

Суд ставить пошукові системи у складне становище. У той час, як Суд Європейського Союзу встановив обов'язок пошукових систем поважати права суб'єктів персональних даних на видалення та заперечення проти обробки персональних даних

[53] Здебільшого пункти 93, 94, 97, 81.

[54] Деякі приклади [Електронний ресурс]. – Режим доступу: https://edri.org/forgotten/.

[55] Серед іншого було засновано «Консультаційну раду», яка провела зустрічі у кількох столицях держав-членів ЄС нібито для надання допомоги Google у виконанні рішення. Численні втручання свідчили про те, що Google видаляв URL-адреси зі своєї бази даних, хоч рішення і не ставило такої вимоги. Google також додає зловісне попередження під час пошуку за іменами осіб, зазначаючи, що «деякі результати могли бути видалені відповідно до європейського законодавства про захист персональних даних», хоч це і мало можливо. У той час, як компанія заявляє, що такі повідомлення мають на меті «прозорість», вона все ж не розміщує аналогічних повідомлень, ранжуючи результати пошуку, тим самим активно впроваджуючи американське законодавство про авторські права в Європі.

[56] FRA, *Access to data protection remedies in EU Member States,* січень 2014 року, С. 12 [Електронний ресурс]. – Режим доступу: http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf.

[57] FRA, *Access to data protection remedies in EU Member States* - summary, 2014 р. [Електронний ресурс]. – Режим доступу: http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf.

[58] Див., наприклад, аналіз рішення у справі, прийнятого місяць тому, зроблений EDRi [Електронний ресурс]. – Режим доступу: https://edri.org/web-blocking-austria-law-with-the-law-taken-out/.

за певних обставин, самі пошукові системи не мають чіткого, передбачуваного й законодавчо визначеного обов'язку не діяти на власний розсуд. Пошукові системи на зразок Google будуть занадто ретельно виконувати судове рішення з метою уникнення судових розглядів та фінансових санкцій, наприклад, відшкодування шкоди[59].

4.3. Висновок

У справі Костехи, як і в інших справах, від посередників вимагається вжити «обґрунтованих» заходів на основі припущення про існування відповідних гарантій для виконання основоположних прав і свобод громадян ЄС. Пошуковим системам лише «рекомендується» поважати основне право суб'єктів персональних даних на приватне життя та захист їхніх персональних даних.

З одного боку, Керівні принципи ООН щодо бізнесу та прав людини встановлюють, що «зобов'язання поважати права людини є глобальним *стандартом очікуваної поведінки* усіх комерційних підприємств незалежно від місця їхньої діяльності»[60].

З іншого боку, приватні компанії на зразок *Google* не мають чіткого обов'язку поважати принцип якості даних, встановлений статтею 5 Конвенції № 108. Формулювання, яке використовується у Пояснювальному меморандумі до Посібника не дуже прояснює ситуацію:

> «існують принципи та правила, яких *повинні* дотримуватися (...) приватні компанії, що здійснюють обробку персональних даних» (виділення авторське)[61].

Нещодавно, 26 листопада 2014 року, Робоча група, створена відповідно до статті 29 Директиви 95/46/ЄС, затвердила керівні принципи для пошукових систем з метою кращого впровадження рішення. Проте дані принципи не мають зобов'язуючого характеру[62].

У результаті, рішення необхідно розглядати з двох точок зору. З одного боку, Суд надав пану Костесі компенсацію (хоч і через чотири роки після подання першої скарги). Він також підвищив рівень правової визначеності щодо ролі пошукових систем як контролерів даних. З іншого боку, існує більш глобальна проблема, яку необхідно розглянути. Від посередників вимагається вживати обмежувальних заходів (хоч і в меншому масштабі, ніж, наприклад, у справі *UPC Telekabel*) на основі припущення про існування чітких обмежень доступних варіантів виконання цієї вимоги, що відповідно забезпечує повагу до основних прав. Проте, абсолютно не зрозуміло чи такі врівноважуючі обов'язки взагалі існують. У випадку, коли

[59] Судова справа в Іспанії, у якій суд визнав шкоду, нанесену компанією Google (серед інших відповідачів). Див також «Sentencia de la Audiencia Provincial de Barcelona», 364/2014, 17 липня 2014 року.

[60] Див. [Електронний ресурс]. – Режим доступу: http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf.

[61] Пояснювальний меморандум, пункт 68.

[62] Керівні принципи доступні за посиланням: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

виконання обов'язків посередниками є надмірним (наприклад, у випадку вжиття довільних заходів з їхнього боку), хто має надавати компенсацію? Власне посередник, Європейська Комісія, держава, Суд чи інша організація?

Ці проблеми було визнано, але не вирішено в документі, представленому Італією протягом її головування в Раді ЄС у 2014 році:

> «...Деякі делегації звертали увагу на ризик того, що свобода вираження поглядів і загальна зацікавленість громадськості в доступі до інформації можуть поступитися місцем інтересам контролера, зокрема коли останній є пошуковою системою»[63].

5 ОСВІТА ТА ГРАМОТНІСТЬ

5.1. Вступ

Право на освіту закріплене у статті 2 Протоколу 1 до ЄКПЛ, яка встановлює:

> «Нікому не може бути відмовлено у праві на освіту. Держава під час виконання будь-яких функцій, узятих нею на себе в галузі освіти й навчання, поважає право батьків забезпечувати таку освіту й навчання відповідно до їхніх релігійних і світоглядних переконань».

Крім того, Посібник встановлює, що кожна особа повинна мати доступ до навчального та культурного контенту в мережі Інтернет. З огляду на це громадянам гарантується право на доступ до цифрової освіти, включаючи необхідні навички та різноманітні інструменти, які пропонує Інтернет.

Освіта та грамотність прямо пов'язані з наявністю доступу до культурної спадщини. Інтернет виявився унікальним інструментом, який швидко надає доступ до значного обсягу інформації. Проте, для того, щоб користуватися такими перевагами, громадянам необхідні певні знання (загальна й комп'ютерна грамотність).

Цей розділ присвячено аналізу окремих випадків, у яких право на освіту може перебувати під загрозою в онлайн середовищі, а також шляхам його захисту й зміцнення.

Що відбувається?

Стрімкий розвиток Інтернету та комп'ютерних технологій залишив багато людей похилого віку та родин з обмеженими економічними ресурсами в несприятливому становищі. Доступ до таких технологій і можливість викори-

[63] Рада Європейського Союзу «Право бути забутим та рішення у справі Google - Координаційні дебати», 29 вересня 2014 року [Електронний ресурс]. – Режим доступу: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013619%202014%20INIT.

стовувати їх є надзвичайно важливими для повноцінної реалізації права на освіту. Як зазначено в Пояснювальному меморандумі, «Інтернет користувачі повинні мати можливість отримувати в Інтернеті базову інформацію, освіту, знання та навички з метою реалізації своїх прав людини і основоположних свобод»[64].

Незважаючи на стрімке поширення смартфонів, планшетів і ноутбуків, певні прошарки населення все ще не мають доступу до таких гаджетів або позбавлені змоги використовувати їх. Навіть тим, хто виріс у середовищі інформаційних технологій, завжди є чому вчитися. Освітні бар'єри можна зменшити шляхом надання апаратного та програмного забезпечення, відкритого для користування, на якому студенти зможуть вільно аналізувати, досліджувати, покращувати та поширювати свої навички, тим самим спільно покращуючи якість технічних можливостей. Використання закритого апаратного забезпечення та форматів, зокрема в навчальних закладах, є перешкодою їхньої доступності. Вони також створюють бар'єр для такого доступу в майбутньому, оскільки закриті формати нерідко стають несумісними із різними операційними системами або навіть із різними версіями того ж програмного забезпечення через декілька років.

Зрештою, право на доступ до культурного, наукового, дослідницького й іншого контенту суттєво різниться в межах держав-членів Ради Європи, і за умов стрімкого впровадження та розвитку комп'ютерних технологій, доступ до онлайн контенту розвивається швидше, ніж відповідне законодавство. Це стосується багатьох законів про авторські права, які були прийняті до виникнення найбільш популярних платформ, що використовуються для створення, доступу й поширення культурного контенту, зокрема *YouTube, WordPress, Facebook ma Twitter.*

5.2. Судова практика – відмінності у використанні контенту в освітньому середовищі та блокуванні сайтів у Франції та Естонії

Як було зазначено вище, неузгодженість законів про авторське право (та відповідних винятків) може призводити до відмінностей у доступі до освіти. Способи, за допомогою яких громадяни отримують доступ до книг і мультимедійного контенту та повторно використовують їх для освітніх або творчих цілей, суттєво відрізняються в кожній державі-члені Ради Європи. Таким чином, деякі онлайн послуги, які доступні, наприклад, в Іспанії, можуть бути недоступними в Сербії; деякі веб-сайти недоступні в Туреччині, але доступні в Росії; до того ж, як буде описано в цьому розділі, деякі способи використання об'єк-

[64] Пояснювальний меморандум, пункт 87.

тів авторського права можуть бути дозволені в освітніх цілях в Естонії, але заборонені у Франції. Щодо останнього прикладу, відмінності у відповідних підходах у Франції й Естонії створюють різні умови для навчання студентів у цих країнах: у той час як в Естонії вчитель має право в освітніх цілях цитувати, компілювати, перекладати або адаптувати авторські роботи, вчителі у Франції позбавлені такого права[65].

Системи винятків та обмежень, складні механізми ліцензування і труднощі під час нагляду за діяльністю організацій з питань охорони авторських прав є лише окремими складовими, які створюють перешкоди для освітян під час доступу до культурного контенту відповідно до діючого режиму охорони авторських прав. Як і у випадку з будь-якими іншими обмеженнями, у судовій практиці ЄСПЛ чітко встановлено, що з метою виконання Конвенції обмеження не може впливати на сутність права та, зокрема, мати законну мету. Крім того, застосовані заходи мають бути пропорційні меті[66].

Правові труднощі

Відмінності в режимах авторського права в Естонії та Франції викликають питання щодо того, чи є такі обмеження пропорційними, як це вимагається судовою практикою ЄСПЛ. Крім того, не зрозуміло, чи відбувається втручання в даному .випадку відповідно до «закону», який є достатньо доступним та передбачуваним. Якщо так, то чи міститься у ньому «законна мета»? Чи є втручання «необхідним у демократичному суспільстві» для досягнення такої мети? Іншими словами, чи є обмеження пропорційним своїй меті?

Законною метою обмеження є захист закріплених у статті 1 Протоколу № 1 до ЄКПЛ майнових прав осіб, які створили контент. Проте, в контексті досліджуваних відмінностей між Францією та Естонією, здається, немає належних причин, щоб вважати таке втручання необхідним у демократичному суспільстві. Відсутні будь-які докази, які б доводили, що Естонія порушила права авторів контенту, надавши можливості для широкого використання об'єктів авторського права в навчальній діяльності. З іншого боку, Естонія має значно більший потенціал для надання комплексної освіти, ніж Франція, у зв'язку з наданням ширшого доступу до різноманітного аудіовізуального та письмового контенту. Таким чином, обмеження щодо використання певного контенту можуть призвести до суттєвих обмежень права на освіту, що порушуватиме положення Конвенції та суперечитиме судовій практиці ЄСПЛ.

[65] Teresa Nobre, *Educational Resources Development: Media Copyright Exceptions and Limitations in Europe, Creative Commons Project Open Educational Resources Policy in Europe, Working Paper,* липень 2014 року [Електронний ресурс]. – Режим доступу: http://oerpolicy.eu/wp-content/uploads/2014/07/working_paper_140714.pdf.

[66] Див., наприклад, справу ЄСПЛ Ashingdane v. the United Kingdom, 28 травня 1985 року.

Насправді, більш гнучка система, що використовується в Естонії, не суперечить законній меті законодавства про захист авторських прав. Відповідно до «трьохскладового тесту», встановленого різними міжнародно-правовими документами, насамперед Бернською конвенцією 1967 року, такі відхилення дозволені лише у випадках, коли вони «не порушують будь-яким необґрунтованим способом законні інтереси автора». Отже, логічно зауважити, що відповідно до принципу використання «найменш обмежувальної альтернативи», запропонованого Судом Європейського Союзу, обмеження, накладені Францією, не відповідають праву на «доступ до освітнього, культурного та наукового контенту в цифровій формі», встановленому Посібником.

5.3. Висновок

З метою надання загального доступу до культурного, наукового, дослідницького й аналогічного контенту, перелік обмежень і винятків із законодавства про захист авторського права держав-членів Ради Європи повинен бути якомога чіткішим та гнучкішим. Це стосується, зокрема, винятків, що встановлюються задля задоволення освітньої мети.

Крім того, необхідно чітко встановити, як саме вчителі можуть використовувати об'єкти авторського права.

Зрештою, можна запровадити нові підходи у сфері академічного контенту, що фінансується за рахунок державних коштів та зазвичай є доступним для кожного в бібліотеці певного університету, але при цьому онлайновий доступ надається лише студентами певного факультету. Пояснювальний меморандум підкреслює цю проблему, встановлюючи, що:

«Інтернет користувачі повинні мати можливість вільного доступу до наукових і культурних здобутків в Інтернеті, що фінансуються державою. 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 з метою виплати винагороди правовласникам за їхню роботу в межах допустимих винятків у сфері захисту прав інтелектуальної власності»[67].

[67] Пояснювальний меморандум, пункт 86.

6 ДІТИ І МОЛОДЬ

6.1. Вступ

Діти мають ті ж права, що й усі інші особи – починаючи з права на свободу вираження поглядів і завершуючи правом на приватне життя. Через свій низький статус у більшості спільнот та залежність від дорослих діти також мають особливі права для захисту їх від загроз, зловживань та дискримінації. Проте, наразі майже відсутнє розуміння того, як саме необхідно захищати увесь комплекс прав дитини в цифровому середовищі та є лише кілька прикладів ефективної боротьби з порушеннями таких прав.

Відсутність чіткості й діяльності у цій сфері пояснюється багатьма причинами, зокрема труднощами регулювання технологій, які постійно розвиваються, новими перешкодами, які вони створюють для врівноваження захисту дітей та гарантування їхньої автономії, відсутністю знань про нові технології серед дорослих, які беруть участь у житті дітей, а також викликами, пов'язаними зі зміною рамок приватного життя, на які суспільство реагує досить повільно. Це також пов'язано з тим, що здійснення нагляду за онлайн діяльністю та введення надто широких обмежень на онлайн контент зазвичай відбувається під гаслами боротьби з тероризмом та захисту прав дітей. У деяких випадках такі аргументи справді базуються на бажанні захистити дітей, у інших – слугують для прикриття цензури, обмежуючи при цьому права як дітей, так і дорослих[68]. Посібник Ради Європи покликаний сприяти вирішенню питання, як саме права дитини можуть бути реалізовані в цифровому середовищі.

Усі права, зазначені в Посібнику Ради Європи з прав людини для Інтернет-користувачів, застосовуються до дорослих і дітей, проте Посібник виокремлює п'ять особливих прав для дітей. Цей розділ присвячено розгляду того, як саме деякі з цих прав – яким приділяється менше уваги – застосовуються на практиці, з метою продемонструвати необхідність більш чіткого тлумачення й забезпечення прав дитини в цифровому середовищі. Зокрема, серед таких прав дитини розрізняють:

- бути почутою і брати участь у прийнятті рішень, які торкаються її інтересів;
- отримувати інформацію мовою, яка відповідає її віку й освіченості, від вчителів, вихователів та батьків або опікунів, а також
- отримувати чітку інформацію про онлайн контент і поведінку, які є незаконними (наприклад, домагання онлайн), а також мати можливість заявляти про потенційно незаконний контент.

[68] Наприклад, парламент Росії запропонував створити «фільтрований Інтернет», починаючи з запуску домену .ДЕТИ (діти), який розміщуватиме лише контент, наданий державою й громадськими організаціями, виробниками та продавцями товарів і послуг для дітей, а також особами, чия робота прямо пов'язана з дітьми. Див. також RT, Russians should only have access to a 'filtered internet - lawmaker, 3 липня 2014 року [Електронний ресурс]. – Режим доступу: http://rt.com/politics/170216-russia-internet-filter-mizulina/. Див. також перелік веб-сайтів, заблокованих у Туреччині здебільшого з міркувань захисту дітей [Електронний ресурс]. – Режим доступу: http://engelliweb.com/. Більше інформації з цього приводу можна знайти у доповіді Спеціального доповідача ООН з питань свободи переконань та вільного вираження поглядів, A/69/335, ст. 12, жовтень 2014 року [Електронний ресурс]. – Режим доступу: https://www.crin.org/en/library/publications/freedom-expression-child-rights-focused-report-un-special-rapporteur-freedom.

6.2. Судова практика – Інтернет-фільтри у Сполученому Королівстві

Що відбувається?

Нібито у цілях захисту дітей було розроблено систему для використання технологій фільтрування. Такі системи фільтрування встановлюються Інтернет-провайдерами у мережі та активуються за умовчанням.

Згідно з доповіддю неурядової громадської організації «Група відкритих прав» (*Open Rights Group*), система блокує майже 10 відсотків із 100 000 веб-сайтів, які використовуються найчастіше (визначено аналітичною службою *Alexa*)[69].

Яким чином це порушує права дитини?

Загальні обмеження контенту, що виходять за рамки розуміння нелегального контенту, є непропорційними меті захисту дітей[70] та порушують їхні права, зазначені в Посібнику, кількома шляхами. До них, серед іншого, належать такі права:

> ***«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;»***

Інтернет-фільтри зазвичай використовують один централізований список, який означає, що єдиною опцією для родини є або використання такого фільтру, або відмова від його використання. Це позбавляє дітей – і навіть їхніх батьків і вчителів – можливості в будь-який значущий спосіб впливати на рішення щодо того, що є доступним.

Визначення дітей як «осіб, що не є дорослими» є занадто спрощеним. Дитинство охоплює значний діапазон віку та вмінь. Загальні фільтри позбавляють можливості налаштувати систему відповідно до віку або вмінь дитини чи дітей, яких вони мають захищати. Це означає, що п'ятирічна та п'ятнадцятирічна дитина підпадають під однакові обмеження, незалежно від їхньої зростаючої самостійності.

Крім того, діти набагато швидше та легше, ніж дорослі, орієнтується в інформації та комунікаційних технологіях, і їхні батьки це знають. Дослідження, проведене у Сполученому Королівстві, виявило, що 43% батьків вважають, що їхні діти знають про Інтернет більше, ніж вони самі. Цей показник досягає 63% серед батьків дітей віком від 12 до 15 років[71]. Діти завжди шукатимуть нові шляхи для подолання обмежень їхньої свободи. Фактично, постійно зростаюча кількість

[69] Див. https://blocked.org.uk/ для отримання більш детальної інформації.

[70] *Child Exploitation and Online Protection Centre, Understanding Online Social Network Services and Risks to Youth:* Stakeholder Perspectives, 2006 рік, пункт 44.

[71] OFCOM, *Children and Parents: Media Use and Attitudes Report* 2014, жовтень 2014 [Електронний ресурс]. – Режим доступу: http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parents-oct-14/.

обмежень щодо використання дітьми публічного простору, що накладаються дорослими з міркувань безпеки, є однією з причин того, чому діти з головою поринули в онлайн середовище[72]. Це означає, що будь-які системи фільтрування для захисту дітей мають бути створені за їхньої участі, що в свою чергу сприятиме їхньому захисту та розвитку.

> ***«2. Ви можете очікувати на отримання інформації мовою, яка 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;»***

Загальні фільтри надають штучне відчуття безпеки. Насправді ж вони позбавляють дітей критичного мислення по відношенню до інформації, яку ті отримують, та дають дорослим змогу уникнути складних розмов замість того, щоб сприяти дискусіям і спілкуванню про те, як робити поінформований вибір.

Попередньо встановленні налаштування виключають самостійні дії дітей щодо власного захисту, які передбачають, зокрема, звернення за порадою до друзів, братів та сестер, батьків, а також зміну налаштувань приватності[73]. Фактично, ЮНІСЕФ у своїй доповіді, присвяченій поглядам дітей на їхні права в цифрову епоху, зазначає, що діти з усіх куточків світу зазвичай демонструють свою обізнаність з питаннями приватності й способами власного захисту онлайн[74].

Проте, діти не лише виступають в ролі пасивних одержувачів онлайн інформації, але й створюють контент. Блокуючи веб-сайти за певними ключовими словами, загальні фільтри можуть не лише накласти обмеження на дитячу творчість без прямого на те умислу, але й перешкодити підтримці між дітьми. Наприклад, веб-сайти або форуми, які надають інформацію та підтримку актуальних для молоді тем, зокрема про статеве виховання, веб-сайти про лесбіянок, гомосексуалістів, бісексуалів та транссексуалів (ЛГБТ)[75]. Ще одна навіть більш загрозлива тенденція у інших державах-членах Ради Європи – і насамперед в Росії – пов'язана з використанням гасел захисту дітей у якості прикриття реальних причин блокування доступу до інформації та виправдання дискримінації сексуальних меншин, включаючи дітей-членів ЛГБТ спільноти. Однак, у випадку, коли зазначені вище питання регулюються законом, а не самовільними угодами з Інтернет-провайдерами (друга модель характерна для Великобританії), суди можуть і надають важливі заходи безпеки.

---

[72] Danah Boyd, *It's Complicated: the social lives of networked teens* [Електронний ресурс]. – Режим доступу: http://www.danah.org/itscomplicated/.

[73] Pew Research, *Where teens seek online privacy advice,* 15 квітня 2013 року [Електронний ресурс]. – Режим доступу: http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/.

[74] UNICEF and Young and Well Cooperative Research Centre, *Children's Rights in the Digital age: A download from children around the world,* жовтень 2014 року [Електронний ресурс]. – Режим доступу:http://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf.

[75] *Open Rights Group, 'Censorship'* [Електронний ресурс]. – Режим доступу: https://www.openrightsgroup.org/issues/censorship.

«3. Ви можете очікувати на отримання чіткої інформації про те, який онлайн-контент і 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;»

Відсутня чіткість критеріїв, призводить що призводять до блокування веб-сайту, а також незрозуміло, хто повинен визначати, який саме контент та поведінка є допустимими, а які - ні. У той час, як багато заблокованих веб-сайтів є незаконними й потенційно шкідливими, інші переслідують навчальну мету, наприклад ті з них, що містять правдиву й об'єктивну інформацію на тему статевого виховання, політики та захисту[76]. У випадках, коли інформація про фільтр є доступною, останній виявляється непристосованим до віку дитини або індивідуальних обставин.

«4. 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.»

Загальні Інтернет-фільтри загрожують безпеці дітей, оскільки вони перешкоджають відкритому обговоренню між дітьми та їхніми батьками або вчителями. Альтернативні джерела якісної інформації, які розміщують достовірну інформацію, що дає дітям змогу приймати поінформовані рішення щодо їхнього життя, також є недоступними. Зрештою, дослідницький проект в рамках Шкільної інспекції Великобританії (OFSTED) дійшов висновку, що діти знаходяться в найменшій небезпеці, коли їм надають можливість самостійно управляти ризиками[77]. Це підтверджується у доповіді Королівського коледжу психіатрів, у якому зазначається, що батьки, які слідкують за онлайн активністю своїх дітей через побоювання, що їхні діти стануть об'єктом залякувань або своїми діями завдадуть собі шкоди, можуть підірвати дитячу довіру до них і тим самим лише викличуть ескалацію проблеми[78]. Дані також свідчать, що поінформовані й активні батьки і вчителі, які можуть надавати підтримку дітям онлайн та офлайн (дві сфери, які все важче розрізняти), є найефективнішим засобом захисту[79].

---

[76] Серед іншого, контент, який підпав під визначення небажаного, містив зображення насилля, «контент, пов'язаний з екстремізмом», «веб-сайти про анорексію та розлади харчової поведінки», «веб-сайти, пов'язані з суїцидом», «алкоголь» та «паління», а також «веб-форуми», «езотеричний контент» та «засоби для обходження веб-блокування». Див. також Open Rights Group, 'Censorship' [Електронний ресурс]. – Режим доступу: https://www.openrightsgroup.org/issues/censorship.

[77] OFSTED, *The safe use of new technologies,* лютий 2005 року [Електронний ресурс]. – Режим доступу: http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies.

[78] Laura Donnelly, *Self-harm fears over parental surveillance of children's 'digital life', Telegraph,* 6 листопада 2014 року [Електронний ресурс]. – Режим доступу: http://www.telegraph.co.uk/health/children_shealth/11145958/Self-harm-fears-over-parental-surveillance-of-childrens-digital-life.html.

[79] UNICEF, *Global Safety Online: Global Challenges and Strategies,* травень 2012 року, С. 45 [Електронний ресурс]. – Режим доступу: http://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

6.3. Висновок

Майже усі національні Інтернет-провайдери у Великобританії використовують блокування за умовчанням, зокрема для нових користувачів. Базову концепцію було описано як «натиснути та забути»: батьки лише одного разу повинні відповісти на питання про необхідність увімкнення фільтру. Фільтрування, в основу якого закладена згода за умовчанням, також обмежує вибір і відповідальність батьків, оскільки відключення (наприклад, за допомогою сконфігурованої під кінцевих користувачів програми) несе певні фактичні й уявні ризики для приватності. Наприклад, фіксується відключення кимось із батьків фільтра, який серед іншого блокує порнографію.

Системи фільтрування загалом стосуються контенту, який є незаконним або, на думку провайдера, вважається шкідливим, що викликає питання щодо того, чи є такі обмеження (на отримання та передання) інформації «визначеними законом».

Теоретично такі заходи є «добровільними», проте їх було введено як прямий результат тиску з боку уряду. Таким чином, не зрозуміло, чи можна покладати відповідальність за такі обмеження на державу, оскільки фактично саме вона обумовила їхнє введення, хоч і незаконно.

Масштаб порушення прав, з огляду на наявність альтернативних Інтернет-провайдерів, залежить від доступності підключення, вільного від будь-якого фільтрування. Вибір між кількома провайдерами, щодо яких неможливо спрогнозувати, які обмеження вони можуть ввести, – навіть враховуючи різницю між ними (різні ціни, обладнання тощо) та фактори небезпеки (проблеми з виставленням рахунків, відсутність обслуговування) – навряд чи є справжнім вибором.

Необхідність захисту дітей під час користування будь-якими електронними пристроями є очевидною. Справедливим є зауваження про дуже тонку межу між незаконним і шкідливим контентом. Однак, для того, щоб сформувати відкрите та справедливе суспільство, у якому інформаційно-комунікаційні технології допомагають суспільству й кожному індивіду розвиватися замість того, щоб деградувати, будь-які обмеження законного контенту мають бути прозорими, відповідати віку, постійно переглядатися, а також визначатися колективно з організаціями громадянського суспільства та самими дітьми. Органи, які забезпечують виконання таких норм, повинні бути незалежними й захищеними від втручання осіб, що переслідують політичні та економічні інтереси[80].

Отже, відповідна політика повинна базуватися на фактах, довірі та спілкуванні, замість того, щоб керуватися страхом та підозрами.

[80] Спеціальний доповідач ООН з питань свободи переконань та вільного вираження поглядів, A/69/335, жовтень 2014 року, С. 12 [Електронний ресурс]. – Режим доступу: https://www.crin.org/en/library/publications/freedom-expression-child-rights-focused-report-un-special-rapporteur-freedom

7 ЗАГАЛЬНИЙ ВИСНОВОК: ЕФЕКТИВНІ ЗАСОБИ ПРАВОВОГО ЗАХИСТУ?

Право на ефективний засіб правового захисту закріплене в статті 13 ЄКПЛ.

Як зазначається у Посібнику та Пояснювальному меморандумі, існують різні види засобів правового захисту. Вони можуть мати форму запитів, пояснень, відповідей, виправлень, вибачень, відновлення порушених прав чи підключення, компенсації тощо. Інтернет-користувачі повинні мати право на «легкодоступну» інформацію про свої права та засоби правового захисту. Як зазначено в Пояснювальному меморандумі, «жоден засіб правового захисту не може сам по собі повністю задовольнити вимоги статті 13». Лише «передбачена законодавством сукупність засобів такого захисту може виконати це завдання»[81].

Стаття 13 ЄКПЛ стосується лише засобів правового захисту з боку національних органів у випадку порушення прав і свобод. Тим не менше, як зазначається у Посібнику та Пояснювальному меморандумі, кожен Інтернет-користувач повинен мати право на отримання ефективної компенсації від Інтернет-провайдерів, національних та/або європейських органів і судів.

Насамперед дуже важливо, щоб Інтернет-провайдери мали чіткі, передбачувані зобов'язання, встановлені законодавством, щодо надання засобів правового захисту від порушень прав людини та основоположних свобод. Як зазначено в Керівних принципах ООН щодо бізнесу та прав людини, приватні компанії мають забезпечувати законні, доступні, передбачувані, справедливі, прозорі та сумісні з правами людини механізми подання скарг, які можуть бути «джерелом безперервного навчання», «заснованого на участі та діалозі».

По-друге, державні органи влади та/або організації з захисту прав людини мають надавати додаткову підтримку Інтернет-користувачам під час порушення їхніх прав і свобод в онлайн середовищі. З точки зору примусового виконання, такі зобов'язання стають ще важливішими, коли обмеження або порушення прав та/або свобод мають кримінальний характер.

По-третє, Інтернет-користувачі можуть ініціювати судовий розгляд. Стаття 6 ЄКПЛ надає Інтернет-користувачам право на справедливий судовий розгляд, хоч це і має бути крайнім заходом. Після вичерпання національних засобів правового захисту Інтернет-користувач має шість місяців з моменту винесення остаточного рішення на національному рівні для звернення до Європейського суду з прав людини (див. також статтю 35.1 ЄКПЛ). Після набрання чинності

[81] Див. ЄСПЛ, Silver and others v. UK, №5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 пункт 113; Kudla v. Poland, №30210/96, пункт 157.

Протоколом №15 такий період буде скорочено до 4 місяців (див. також статтю 4 Протоколу)[82].

Зрештою, ключовим питанням, яке необхідно розглянути, є визначення того, чи є такі засоби правового захисту «наявними, відомими, доступними, а також чи надаються за помірну плату та забезпечують належне відшкодування» на практиці та відповідно до закону.

[82] Див. пояснювальну записку: Рада Європи, Пояснювальний звіт до Протоколу № 15, який вносить зміни до Конвенції про захист прав людини і основоположних свобод [Електронний ресурс]. – Режим доступу: http://www.echr.coe.int/Documents/Protocol_15_explanatory_report_ENG.pdf.

Наведені приклади свідчать про те, що, як правило, надання правового захисту є можливим. Однак, існує проблема, пов'язана з відстоюванням прав у випадках, коли обмеження накладаються юридичними особами «добровільно» за відсутності законодавчо визначеного зобов'язання. Залишається невирішеним питання щодо меж негативних зобов'язань держав під час заохочення ними приватних компаній до накладення обмежень. Аналогічним чином, чітко не встановлені позитивні зобов'язання держави реагувати у випадках накладення таких обмежень за участі держави або без залучення останньої.

Зрештою, така невизначеність щодо окреслених вище питань може бути пояснена новим для правової сфери феноменом, що розглядає Інтернет як публічний простір, який перебуває в приватній власності. Було б доволі корисним, якби Рада Європи розробила рекомендації щодо імплементації ЄКПЛ у даному контексті.