Лабораторія цифрової безпеки
Коаліція «За вільний Інтернет»

ПРАВА ЛЮДИНИ ОНЛАЙН
Порядок денний для України

Розроблено в рамках проекту Digital Rights Agenda for Ukraine,
що фінансується Агентством США з міжнародного розвитку (USAID)
через організацію Counterpart International

Вересень 2019

Права людини онлайн: Порядок денний для України / Віта Володовська, Максим Дворовий – Київ: ГО «Лабораторія цифрової безпеки», 2019. – 56 с. Це видання підготовлено та видано в рамках проекту *Digital Rights Agenda for Ukraine*, що фінансується Агентством США з міжнародного розвитку (USAID) через організацію Counterpart International. Погляди, виражені в даній публікації, відображають позицію авторів та не обов'язково відображають позицію USAID та Counterpart International.

м. Київ, 2019

ЗМІСТ

ЦИФРОВІ ПРАВА — ПРАВА ЛЮДИНИ

Головним обов'язком держави є утвердження та забезпечення прав і свобод людини. Цей принцип лежить в основі демократичного ладу та закріплений у статті 3 Конституції України. Ця ж стаття передбачає, що саме права і свободи людини та їх гарантії повинні визначати зміст і спрямованість діяльності держави.

Розвиток та поширення Інтернету створили безпрецедентні інструменти для реалізації громадянами їхніх прав та свобод, у тому числі забезпечили їм можливості вільно висловлювати свої погляди та думки перед широкою аудиторією, отримувати оперативний доступ до будь-якої інформації онлайн. Водночас зросли й загрози, пов'язані зі зловживанням такими правами, поширенням мови ворожнечі та незаконним втручанням у право на повагу до приватного життя людини.

У своїй нещодавній Резолюції 38/2018[1] Рада ООН з прав людини вкотре наголосила: «*права, які людина має офлайн, мають так само захищатися в онлайн-середовищі, зокрема, свобода вираження поглядів, яка діє незалежно від кордонів та обраних людиною засобів комунікації (медіа), відповідно до статті 19 Загальної декларації прав людини та Міжнародного пакту про громадянські та політичні права*».

Рада Європи у своїх документах та в рішеннях Європейського суду з прав людини (Європейський суд) підтримує позицію щодо обов'язків держав-членів забезпечувати кожному, хто перебуває в межах їхньої юрисдикції, права та основоположні свободи, закріплені Конвенцією з прав людини та основоположних свобод (далі — Європейська конвенція), у тому числі й у сфері використання мережі Інтернет. Європейський суд у справі «Їлдирим проти Туреччини»[2] зауважив, що «*наразі Інтернет став одним з основних засобів реалізації громадянами свого права на свободу вираження поглядів та інформації, забезпечуючи їх таким чином необхідними інструментами для участі в діяльності та обговорення політичних та інших питань, що становлять суспільний інтерес*».

Досить часто для позначення прав людини онлайн застосовують термін «цифрові права» (англ. — digital rights), хоча його використання не є науково обґрунтованим. Так, свобода слова чи право на приватність давно включені до каталогу фундаментальних прав людини у низці міжнародних актів — Загальній декларації прав людини, Міжнародному пакті про грома-

---

1 The Human Rights Council A/HRC/38/L.10/Rev.1 «The promotion, protection and enjoyment of human rights on the Internet», 4 July 2018: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1.

2 CASE OF AHMET YILDIRIM AND OTHERS v. TURKEY no. 3111/10, 18 December 2012: http://hudoc.echr.coe.int/eng?i=001-115705.

дянські та політичні права, Конвенції про захист прав людини та основоположних свобод — та підлягають захисту незалежно від способу чи сфери їх реалізації. Свобода вираження поглядів залишається правом незалежно від того, поширюється інформація усно, в газеті чи на веб-сайті. Водночас виникнення такого потенційного «цифрового права» як доступ до Інтернету, а також визначення «права бути забутим» (права вимагати видалення інформації про особу з результатів пошукових сервісів) є досить нещодавніми[3].

З практичного погляду доцільно розглядати поняття «*цифрові права*» не як окрему групу прав людини, а як умовну категорію, що охоплює особливості реалізації та гарантії захисту фундаментальних прав людини в Інтернеті, зокрема свободи вираження поглядів та права на приватність онлайн. Зважаючи на величезну роль, яку відіграє Інтернет у сучасному житті, виокремлення такої категорії допомагає краще систематизувати та вивчати потреби захисту прав людини в онлайн-середовищі, окремі гарантії яких сьогодні розпорошені в рекомендаціях, резолюціях та інших актах міжнародних інституцій.

Хоча на більшість прав та свобод, пов'язаних з Інтернетом, уже поширюються гарантії захисту чинних міжнародних актів, проте такий захист наразі є радше мінімальним, тоді як серйозніші гарантії потребують часу для того, щоб отримати свій розвиток у правозастосовній практиці, зокрема в рішеннях міжнародних судів. Тому втілення та захист прав та свобод онлайн на сьогодні потребують уваги з боку національних органів влади, законодавчого забезпечення гарантій прав людини в онлайн-середовищі та застосування принципів в адміністративній та судовій практиці.

Цей Порядок денний містить рекомендації державним органам щодо впровадження, удосконалення та посилення гарантій захисту прав та свобод людини в онлайн-середовищі. Зокрема, документ містить пропозиції щодо забезпечення права на доступ до Інтернету, свободи вираження поглядів, права на приватність та захист персональних даних, а також окреслює актуальні виклики щодо ролі держави в гарантуванні дотримання прав людини з боку приватних корпорацій.

Водночас важливо також наголосити на окремих загальних рекомендаціях, виконання яких сприятиме підвищенню обізнаності представників органів влади та широкої громадськості з особливостями реалізації прав людини онлайн.

---

[3] Вперше це право було чітко окреслене у справі «Google Spain v AEPD and Mario Costeja González», що була розглянута Європейським судом справедливості у 2014 році: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

Загальні рекомендації щодо посилення захисту прав людини онлайн:

1. В Україні на сьогодні не здійснюється системний моніторинг та аналіз дотримання прав людини онлайн. *Уповноваженому Верховної Ради України з прав людини* як посадовій особі, що забезпечує парламентський контроль за додержанням конституційних прав і свобод людини і громадянина, доцільно розробити та впровадити систему моніторингу й оцінки стану забезпечення цифрових прав людини.
2. *Верховній Раді України (Комітету з питань гуманітарної та інформаційної політики, Комітету з питань цифрової трансформації та іншим комітетам*, предмет відання яких стосується питань державної політики у сфері інформації, інформаційної безпеки та інформаційних технологій) — започаткувати діалог з експертами та правозахисниками щодо законодавчих та інших ініціатив з метою регулювання суспільних відносин в Інтернеті, шляхом створення робочої групи чи проведення робочих зустрічей, задля недопущення порушення прав людини під час розробки та впровадження таких ініціатив, а також задля формування чіткої та збалансованої концепції регулювання відносин, пов'язаних із поширенням інформації в Інтернеті.
3. *Кабінету Міністрів України (Мін'юст, МВС та ін.)* — переглянути/розробити та включити до навчальних програм, програм перепідготовки та підвищення кваліфікації державних службовців та працівників правоохоронних органів окремих предметів з питань розвитку інформаційних технологій та забезпечення прав людини в онлайн-середовищі.
4. *Національній школі суддів України* — включити тренінги з питань розвитку інформаційних технологій та забезпечення прав людини в онлайн-середовищі до обов'язкових програм підготовки суддів.
5. *Міністерству освіти та науки України* — розробити та забезпечити впровадження в шкільні освітні програми обов'язкових компонентів інтернет- та медіа-грамотності. Забезпечити включення відповідних компонентів у програми підготовки та підвищення кваліфікації педагогічних працівників.

ПРАВО НА ДОСТУП ДО ІНТЕРНЕТУ

Доступ до Інтернету — невід'ємна умова для реалізації прав та свобод людини та участі у процесах прийняття рішень з управління державними справами. Доступ до Інтернету поки що офіційно не визнано правом людини на міжнародному рівні, хоча міжнародні інституції систематично наголошують на важливій ролі, яку відіграє Інтернет у демократичному суспільстві. Доступність Інтернету розглядається як засада сприяння реалізації іншим правам та свободам людини, зокрема свободі вираження поглядів онлайн.

У 2003 році Комітет міністрів Ради Європи в Декларації про свободу комунікації в Інтернеті зазначив, що країни-члени Ради Європи мають заохочувати доступ усіх до Інтернет-сервісів без дискримінації та за доступною ціною[4]. У 2014 році у Рекомендації CM/Rec (2014)6 також було наголошено, що люди, які покладаються на Інтернет у своїй діяльності, очікують, що Інтернет-сервіси будуть доступними, безпечними, надійними та надаватимуться без дискримінації[5].

10 липня 2019 року Спеціальний доповідач ООН з питань свободи думки та вираження поглядів, Представник ОБСЄ з питань свободи медіа, Спеціальний доповідач Організації Американських держав з питань свободи вираження поглядів та Спеціальний доповідач з питань свободи вираження поглядів та доступу до інформації Африканської комісії з прав людини та народів оприлюднили щорічну Спільну декларацію «*Виклики для свободи вираження поглядів у наступному десятилітті*»[6]. Це вже двадцята спільна декларація представників міжнародних інституцій і перша, що містить прямий заклик до держав визнати доступ до Інтернету правом людини, оскільки можливість бути онлайн є невід'ємною умовою реалізації свободи вираження поглядів. У документі зазначається, що здійснення свободи вираження поглядів вимагає надійної та універсальної цифрової інфраструктури, регулювання якої забезпечує її функціонування як вільного, доступного як та відкритого простору для всіх зацікавлених сторін.

---

4 Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5.

5 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f3d.

6 Joint Declaration on Challenges to Freedom of Expression in the Next Decade: https://www.osce.org/representative-on-freedom-of-media/425282?fbclid=IwAR2IkGPrxvjhlShXZrJJX_sQa2yoKTiXlprzIi6ZPDCuIeyijAWL9AQERaA.

Варто зазначити, що в окремих країнах «право на доступ до Інтернету» уже знаходить своє юридичне втілення. Так, у Бразилії спеціальний закон, ухвалений у 2014 році («*The Internet Bill of Rights»*[7]), визначає, що забезпечення загального доступу до Інтернету є метою цього регулювання. Конституційна рада Франції у 2009 році також визнала доступ до Інтернету основоположним правом людини, вказавши, що пропоновані у французькому законі про захист прав інтелектуальної власності в Інтернеті норми щодо можливого автоматичного та позасудового відключення доступу порушників до Інтернету мають бути скасовані[8]. У Греції право на Інтернет як право на участь в «інформаційному суспільстві» та доступі до електронного поширення інформації закріплене Конституцією[96].

Право на доступ до Інтернету як право кожного вільно користуватись безпечним та відкритим Інтернетом має охоплювати два аспекти:

Перший аспект — заборона державам необґрунтовано обмежувати доступ до Інтернету, зокрема здійснювати відключення Інтернету в усій країні чи окремих регіонах. Блокування доступу окремих осіб до Інтернету може бути виправданим, але лише за вагомих підстав. До прикладу, Європейський суд з прав людини у справі *Kalda v Estonia,* що стосувалася заборони доступу ув›язненого у пенітенціарному закладі до низки офіційних сайтів, на яких були доступні в електронному варіанті законодавчі акти, рішення судів та рішення Європейського суду з прав людини, вказав, що засудження безперечно тягне за собою обмеження комунікації з зовнішнім світом для ув›язнених. І хоча стаття 10 Європейської конвенції з прав людини не накладає обов›язку надавати доступ до мережі або до конкретних веб-сайтів для ув›язнених, естонське законодавство в цілому дозволяє надавати доступ до окремих сайтів з правовою інформацією на спеціально захищених комп›ютерах, а тому відбулося втручання в права заявника. Таке втручання було визнане таким, що порушує статтю 10 Конвенції, оскільки національні суди не провели належного аналізу ризиків, пов›язаних із використанням відповідних сайтів заявником. Що цікаво, у параграфі 52 рішення Європейський суд наголосив, що «*доступ до Інтернету все частіше сприймається як право, а тому вже лунали заклики до розробки ефективних політик із забезпечення універсального доступу до мережі задля подолання цифрового розриву*»[10].

---

7 Law no. 12.965 of April 23, 2014. Більше про закон: https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf.

8 Decision n° 2009-580 of June 10th 2009 https://edri.org/edri-gramnumber7-123-strikes-censured-council-constitutional/

9 Конституція Греції (англ. мова): https://www.wipo.int/edocs/lexdocs/laws/en/gr/gr220en.pdf.

10 CASE OF KALDA v. ESTONIA, no. 17429/10, 19 January 2016.

Другий аспект цього права зобов'язує держави вживати усіх розумно можливих заходів для забезпечення максимального доступу своїх громадян до Інтернету. Наприклад, розробити та впроваджувати конкретну та ефективну політику задля того, щоб Інтернет був широко доступним, відкритим та надавався за помірну плату для всіх груп населення. Особливі форми сприяння можуть бути поширені на малозабезпечені верстви населення та людей з інвалідністю. Крім цього, умовами для повноцінної реалізації цього права громадянами є також доступ до інформації про технології та цифрова грамотність — можливість отримувати знання та навички з використання Інтернету для задоволення своїх потреб.

Право на доступ до Інтернету має базуватися на кількох важливих принципах:

- *Інклюзивність та недискримінація*. Доступ має надаватися за розумну ціну й бути недискримінаційним. Взаємодія в Інтернеті має бути вільною від дискримінації за будь-якими ознаками, такими як стать, раса, колір шкіри, мова, релігія або віра, політичні чи інші переконання, національність або соціальне походження, належність до національної меншини, майновий стан, походження чи будь-який інший статус, зокрема за етнічною приналежністю, віком або сексуальною орієнтацією. Держава має також сприяти просуванню культурної та мовної різноманітності онлайн, а також створювати технічні умови доступу до Інтернету для вразливих груп, наприклад через підтримку публічних «точок доступу» (бібліотеки, навчальні центри, школи тощо).
- *Мережева нейтральність*. Користувачі повинні мати можливості вільно обирати систему, застосунки, програмне забезпечення. Архітектура Інтернету, комунікаційні системи і формати повинні ґрунтуватись на відкритих стандартах, які забезпечують інтероперабельність, інклюзивність та рівні можливості — вільний обмін інформацією.
- *Безпека Інтернету.* Держава повинна гарантувати безпечність Інтернету. Водночас важливо зазначити, що технічні стандарти, пов'язані з інфраструктурою Інтернету, не повинні застосовуватись для цензури чи незаконного нагляду. Технічні характеристики, які створюють можливості для віддаленого доступу правоохоронцям до обладнання (як це, наприклад, втілено в Росії та пропонувалося в Україні[11]), суперечать демократичним цінностям.

[11] Аналіз проекту Закону «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері» № 6688: https://www.ppl.org.ua/yuridichnij-analiz-vid-koalici%D1%97-za-vilnij-internet-proektu-zakonu-6688.html.

- *Якість сервісу*. Гарантований доступ до Інтернету має відповідати рівню сучасного розвитку та поширення технологій.

Станом на сьогодні право на доступ до Інтернету в українському законодавстві відсутнє. Закон України «Про телекомунікації» визначає перелік загальнодоступних телекомунікаційних послуг, однак він включає в себе лише універсальний доступ до підключення до загальних мереж фіксованого зв›язку, місцевий телефонний зв›язок, виклик служб екстреної допомоги, послуги довідкових служб і зв'язку за допомогою таксофонів. Водночас Україна поступово розвиває технології доступу до зв›язку і планує вивільнення частот під технологію 5G вже у 2020 році[12], хоча значна частина території України досі не покрита технологіями 3G та 4G[13]. Уряд робить окремі дерегуляційні заходи задля збільшення покриття широкосмуговим Інтернетом[14], а також спрямував 1 млрд гривень на інтернетизацію шкіл[15]. Утім якісь цілеспрямовані заходи щодо поширення доступу до мережі не впроваджуються. Попри це, за даними численних досліджень, український Інтернет все ще є одним із найдешевших у світі[16].

---

12 Указ Президента України №242/2019 «про забезпечення умов для впровадження системи рухомого (мобільного) зв'язку п'ятого покоління: https://www.president.gov.ua/documents/2422019-26881.

13 https://www.mobua.net/maps/?pos=48,31,6.

14 Уряд спростив доступ до телекомунікаційних мереж для бізнесу: https://www.kmu.gov.ua/ua/news/u-ramkah-deregulyacijnogo-zasidannya-uryad-sprostiv-dostup-do-telekomunikacijnih-merezh-dlya-biznesu-ta-pravila-pracevlashtuvannya-inozemciv.

15 https://mon.gov.ua/ua/news/uryad-spryamuvav-1-mlrd-grn-na-internetizaciyu-ta-kompyuterizaciyu-ukrayinskih-shkil-liliya-grinevich

16 Ukraine has world's cheapest broadband internet: https://emerging-europe.com/news/ukraine-has-worlds-cheapest-broadband-internet/; https://www.kyivpost.com/technology/ukraines-mobile-internet-one-of-worlds-cheapest.html.

Рекомендації щодо доступу до Інтернету:

1. *Верховній Раді України*, зокрема парламентському *Комітету з питань гуманітарної та інформаційної політики, Комітету з питань цифрової трансформації, а також Кабінету Міністрів України* — розглянути питання щодо можливості та необхідності законодавчого закріплення права та гарантій доступу до Інтернету в Україні
2. *Кабінету Міністрів України (Міністерству цифрової трансформації України)* — забезпечити проведення незалежного аналізу стану доступу користувачів до Інтернету в Україні, зокрема рівня покриття та швидкості Інтернету.
3. *Верховній Раді України (Комітету з питань цифрової трансформації)* та *Кабінету Міністрів України (Міністерству цифрової трансформації України)* — створити сприятливі умови для розвитку інфраструктури доступу до Інтернету, у тому числі шляхом спрощення регулювання ринку телекомунікаційних послуг, та приведення національного законодавства у відповідність із законодавством ЄС у рамках виконання Угоди про Асоціацію між Україною та ЄС.
4. *Міністерству цифрової трансформації України* — сприяти доступу до Інтернету в сільській та географічно віддаленій місцевості, а також розробити спеціальні програми щодо сприяння доступу до Інтернету малозабезпечених верств населення та осіб з інвалідністю.
5. *Верховній Раді України та Кабінету Міністрів України* — утримуватись від ініціювання законопроектів чи заходів, спрямованих на створення перешкод чи блокування доступу до Інтернету, телекомунікаційних мереж.
6. *Міністерству цифрової трансформації України* — гарантувати, що у процесі впровадження нових технологій, розвитку «Інтернету речей» (IOT) тощо, забезпечуватиметься повага до прав людини, зокрема гарантуватиметься принцип «приватності за замовчуванням».

СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ ОНЛАЙН

Свобода вираження поглядів є однією з найважливіших основ демократичного суспільства й однією із ключових умов його розвитку та самореалізації кожної людини. У світлі доступності та можливостей зберігання й передачі великих масивів інформації, Інтернет відіграє важливу роль у розширенні суспільного доступу до новин і сприяє поширенню інформації в цілому. Свобода вираження поглядів включає право вільно шукати, отримувати та поширювати інформацію та ідеї онлайн, обсяг і суть реалізації якого відповідають аналогічному праву вільного вираження поглядів в офлайн середовищі.

Державні органи зобов'язані не лише утримуватись від перешкоджання реалізації права людини на свободу вираження поглядів, але й повинні створювати належні умови для такої реалізації. Європейський суд з прав людини в рішенні у справі «*Редакція газети „Правоє дєло" і Штекель проти України*» визнав, що стаття 10 Європейської конвенції покладає на держави позитивні обов'язки щодо встановлення необхідної нормативно-правової бази для забезпечення належного захисту права на свободу вираження поглядів в Інтернеті.

Коаліція «За вільний Інтернет» проаналізувала всі законодавчі ініціативи у сфері свободи вираження поглядів в Інтернеті, що були зареєстровані у Верховній Раді України попереднього, восьмого, скликання[17]. Аналіз законопроектів та хід їх розгляду парламентом засвідчив відсутність ефективної взаємодії між представниками органів влади, громадянського суспільства, бізнесу (зокрема, провайдерів телекомунікацій) та медіа. Практично всі законодавчі ініціативи, спрямовані на встановлення механізмів регулювання в Інтернеті, розроблялись без належного залучення та обговорення інтересів різних груп. Як наслідок — пропоновані законопроекти часто дублювалися, містили неоднозначні визначення та непропорційні підстави й порядок обмеження свободи слова в Інтернеті.

Низка проаналізованих законодавчих ініціатив, зокрема, була спрямована на повернення кримінальної відповідальності за наклеп та образу. У 2001 році разом з ухваленням нового Кримінального кодексу Україна декриміналізувала наклеп відповідно до найкращих міжнародних стандартів у сфері свободи слова, адже криміналізація висловлювань неминуче веде до придушення дискусії й самоцензури медіа. Навіть якщо в результаті незалежного судового розгляду журналісти зможуть довести правдивість поширеної інформації, сам факт відкриття кримінального провадження тягне

[17] Аналітичний звіт «Свобода слова в Інтернеті: законодавчі ініціативи та практика розгляду кримінальних справ в Україні у 2014—2018 рр.»: https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf

за собою багато негативних наслідків, які можуть серйозно позначитись на роботі медіа[18].

З іншого боку, захист репутації особи або необхідність встановити того, хто поширює протиправний контент, може ускладнюватись через відсутність на відповідному веб-сайті інформації про його власника чи особу, яка відповідає за редакційну політику такого онлайн-медіа, або будь-якої іншої інформації, необхідної для подання відповідної скарги. Українське законодавство на сьогодні не встановлює процедури реєстрації онлайн-ЗМІ та будь-яких спеціальних вимог до їх діяльності. Значна частина онлайн-медіа реєструються як інформаційні агентства, і на їх діяльність поширюються встановлені законодавством гарантії свободи діяльності та норми щодо відповідальності за порушення. Такі інформаційні агентства, серед іншого, зобов'язані оприлюднювати свої вихідні дані: назву, відомості про засновників та власників, прізвище чергового редактора чи відповідального за випуск та їх реквізити, адресу агентства тощо. Проте чинна редакція закону пов'язує оприлюднення таких даних з періодичними «випусками продукції», що не зовсім відповідає діяльності онлайн-медіа, яка має постійний характер. Отже, є сенс переглянути чинне законодавство задля підвищення прозорості діяльності інформаційних агентств та медіа онлайн.

Чинний Цивільний кодекс України у статтях 277 та 278 визначає загальні правила щодо спростування недостовірної інформації чи припинення поширення інформації, що порушує особисті немайнові права особи. Водночас положення кодексу не містять специфічних норм щодо захисту від недостовірної інформації, поширеної онлайн. Застосовуючи вказані норми на практиці, суди доволі часто вдаються до одночасного зобов'язання відповідача спростовувати та видаляти недостовірні відомості, що нерідко є надмірним та невиправданим заходом. Тому є необхідність у здійсненні узагальнення та аналізу судової практики у справах про захист честі, гідності та ділової репутації в Інтернеті та підготовці відповідних рекомендацій для судів.

Крім цього, набуває поширення практика блокування доступу до окремих веб-сайтів на підставі рішення слідчих суддів у рамках застосування заходів забезпечення кримінального провадження. Так, 23 липня 2019 року слідчий суддя Печерського районного суду міста Києва року в рам-

[18] Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression on Freedom of Expression and the Administration of Justice, Commercialisation and Freedom of Expression and Criminal Defamation (2002): https://www.osce.org/fom/99558?download=true.

ках кримінальної справи № 757/38387/19-к виніс ухвалу[19] про накладення арешту на майнові права інтелектуальної власності, які виникають у користувачів мережі Інтернет при використанні 19 веб-сайтів (серед них — blogs.korrespondent.net, enigma.ua та інші), шляхом зобов›язання низки великих українських Інтернет-провайдерів закрити до них доступ. Зазначена ухвала не відповідає[20] вимогам кримінального процесуального законодавства щодо визначення речових доказів, на які може накладатись арешт, та вимогам чинного законодавства щодо обов'язків провайдерів телекомунікаційних послуг, які можуть блокувати повний доступ до певних ресурсів лише у випадку поширення дитячої порнографії. Натомість подібна судова практика відкриває можливості для надзвичайно серйозних зловживань та порушень свободи вираження поглядів онлайн і має бути ретельно переглянута.

Право громадян на інформацію також включає право на доступ до публічної інформації, тобто до відомостей, що перебувають у володінні органів державної та місцевої влади. У 2015 році Закон України «Про доступ до публічної інформації» було доповнено статтею 10-1, яка встановила обов'язок розпорядників оприлюднювати публічну інформацію у формі відкритих даних — у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. Кабінет Міністрів України також затвердив відповідний Перелік наборів даних[21], що їх має оприлюднювати кожен державний орган та органи місцевого самоврядування. У 2018 році Державне агентство з питань електронного урядування запустило оновлений Портал відкритих даних[22]. Водночас аналіз виконання розпорядниками вимог законодавства свідчить, що не всі відкриті дані належно оприлюднюються розпорядниками[23]. Поширеними є порушення, пов'язані з неоприлюдненням даних, які підлягають обов'язковій публікації у форматі відкритих даних, невідповідність оприлюднених даних вимогам повноти, якості, оновлюваності, а також неправомірне обмеження доступу до суспільно важливої інформації.

Інтернет створив безпрецедентні можливості для обміну інформацією. Водночас такий доступ до знань справді неминуче пов'язаний із серйозними ризиками й загрозами, такими, як, наприклад, погрози насильства та

---

19 https://korrespondent.net/ukraine/4124650-pecherskyi-sud-zablokyroval-desiatky-smy-v-ynternete

20 https://hromadske.ua/posts/pecherskij-precedent-za-sho-namagayutsya-zakriti-19-veb-sajtiv-odniyeyu-uhvaloyu-sudu

21 https://zakon.rada.gov.ua/laws/show/835-2015-п - n12

22 https://data.gov.ua/

23 http://texty.org.ua/pg/article/Oximets/read/95708/Derzhorgany_zvolikajut_z_opryludnennam_naboriv_vidkrytyh_danyh.

мова ворожнечі, а також координовані кампанії з поширення дезінформації, що в цілому ускладнює доступ до справді цінної інформації та підриває довіру до ЗМІ.

Зважаючи на це, право на свободу вираження поглядів онлайн не є абсолютним і може підлягати обмеженню. Проте будь-яке регулювання та законодавче обмеження цифрових прав мають розроблятися прозоро, відкрито та інклюзивно, тобто з участю представників не лише державних органів, але й громадянського суспільства та бізнесу. Встановлені обмеження не повинні тлумачитись надто широко й мають відповідати сукупності таких критеріїв, що були визначені Європейським судом з прав людини, рішення якого є обов'язковими для застосування в Україні:

1. Легітимна ціль обмеження

Конституція України до таких легітимних інтересів при обмеженні свободи вираження поглядів відносить, наприклад, інтереси:

- національної безпеки;
- територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам;
- охорони здоров›я населення;
- захисту репутації або прав інших людей;
- запобігання розголошенню інформації, одержаної конфіденційно;
- підтримання авторитету й неупередженості правосуддя.

Аналогічні підстави визначаються Європейською конвенцією (яка також додає захист моралі) та Міжнародним пактом про громадянські та політичні права.

Цей критерій практично завжди виконується, адже категорії сформульовані достатньо широко. Так, журналістське розслідування про корупцію у сфері оборони можна не дати поширити, посилаючись на захист репутації та національну безпеку. Саме тому важливо розглядати всі умови для обмежень у комплексі. Більшість дискусій щодо правомірності обмежень стосуються саме наступних двох критеріїв.

2. Законність

Обмеження має бути передбачене законом. Закон має бути оприлюдненим у встановленому порядку та відповідати вимогам якості — бути доступним, чітким, зрозумілим та передбачуваним. Крім цього, застосовувати обмеження мають незалежні органи, чиї повноваження встановлені законом. У низці випадків Європейський суд наголошує на важливості судового нагляду не лише над санкціонуванням обмежень, але й над їх упровадженням. Цей критерій також передбачає існування встановлених законом можливостей захисту від надмірних обмежень, наприклад ефективного оскарження застосованих заходів.

3. Необхідність у демократичному суспільстві

Критерій необхідності включає в себе потребу обґрунтувати «нагальну необхідність» заходів із обмеження права, тобто в чому полягає небезпека легітимним цілям, якщо обмеження не буде застосоване й чому такий захід потрібен для досягнення законної цілі. Далі необхідно забезпечити пропорційність втручання — обмеження має бути мінімально необхідним для ефективного захисту легітимної цілі. Тобто потрібно знайти баланс між ціллю й правом, яке обмежується: блокування всього веб-ресурсу чи видалення лише незаконної інформації. І останнє: держава, яка обмежує якесь право, повинна навести достатні та адекватні підстави для такого втручання, тобто мотивувати своє рішення.

Загальні рекомендації:

1. *Верховній Раді України та іншим суб'єктам законодавчої ініціативи* — забезпечити відповідність будь-яких ініціатив, що можуть призвести до обмеження свободи отримувати та поширювати інформацію онлайн, вимогам міжнародних стандартів у сфері прав людини. Підстави та порядок обмеження свободи поширювати та отримувати інформацію в Інтернеті мають бути чітко визначені законом. Такий закон має бути доступним, передбачуваним та містити захист від неконтрольованих дій державних органів, які забезпечуватимуть виконання обмежень. Обмеження має відповідати нагальній суспільній потребі та бути пропорційним. Зокрема, на підставі рішення суду обмеженню в доступі може підлягати лише чітко й недвозначно визначена законом інформація, а не весь інформаційний ресурс, де вона розміщена. При цьому мають бути забезпечені гарантії від надмірного втручання, зокрема через встановлення строків обмеження, можливості його справедливого оскарження та ін.
2. *Пленуму Верховного Суду* — з метою забезпечення однакового застосування норм права при вирішенні справ, пов'язаних із захистом честі, гідності та ділової репутації онлайн, узагальнити практику застосування матеріального й процесуального законів та підготувати відповідні роз'яснення.
3. *Судам* — при вирішенні питань щодо обмеження свободи вираження поглядів онлайн, у тому числі у справах, пов'язаних із захистом репутації особи, керуватися наведеними вище критеріями щодо легітимності, законності та необхідності, а також здійснювати оцінку таких критеріїв: внесок інформації в обговорення суспільно важливих питань, ступінь публіч-

ності особи, якої стосується інформація, суть інформації, попередня поведінка особи, метод отримання інформації та її достовірність, зміст, форма та наслідки оприлюднення інформації, співрозмірність покарання (санкцій).

4. *Верховній Раді України (Комітету з питань гуманітарної та інформаційної політики)* — ініціювати обговорення з експертами, журналістами, представниками органів державної влади щодо доцільності врегулювання статусу онлайн-медіа та підвищення прозорості їх діяльності (розкриття інформації про власників веб-ресурсів, осіб, відповідальних за редакційну політику, контактні дані для подання скарг на матеріали, оприлюднені у виданні).
5. *Верховній Раді України та іншим суб'єктам законодавчої ініціативи* — утримуватися від будь-яких спроб повернути кримінальну відповідальність за наклеп чи інші висловлювання, що можуть посягати на честь та гідність особи. Громадяни мають право вільно критикувати органи публічної влади та публічних осіб. Законодавчі ініціативи, спрямовані на обмеження права громадян обговорювати питання суспільного інтересу, суперечать демократичним засадам конституційного ладу України.
6. *Уповноваженому Верховної Ради України з прав людини* — посилити контроль щодо своєчасного, повного та якісного оприлюднення публічної інформації у формі відкритих даних, а також належного оновлення такої інформації розпорядниками.
7. *Міністерству цифрової трансформації України* — сприяти повноцінному виконанню вимог законодавства щодо оприлюднення та оновлення наборів відкритих даних належної якості для підвищення підзвітності влади, розвитку інновацій і соціального впливу.

СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ ТА НАЦІОНАЛЬНА БЕЗПЕКА

Інтерес захисту національної безпеки завжди є одним із пріоритетних для держав. Для них безпекова сфера є зоною значної дискреції, оскільки саме в такий спосіб держави мають належним чином захищати права власних громадян від зовнішніх загроз. Ця легітимна мета є наскрізною для міжнародно-правових документів, що гарантують свободу вираження поглядів і трапляється як у статті 10 Європейської конвенції (разом із метою забезпечення територіальної цілісності), так і у статті 19 Міжнародного пакту про громадянські та політичні права. Варто згадати й про положення статті 15 Європейської конвенції та статті 4 Пакту, які допускають відступ (дерогацію) від конвенційних прав під час надзвичайного становища в державі, при якому життя нації перебуває під загрозою, але такий відступ від прав припускається виключно в тих межах, яких вимагає гострота становища. Право на свободу вираження поглядів за обома документами не належить до прав, дерогація яких заборонена, але Україна й не включала ці права до відповідних декларацій, надісланих до Ради Європи та ООН. Насамкінець не можна обійти увагою і статтю 20 Пакту, яка забороняє поширення пропаганди війни.

Чи не найбільшою проблемою з легітимною метою забезпечення національної безпеки є можливість зловживання нею державою для приглушення (а то й вимкнення) опозиційних голосів у суспільстві. Задля усунення зловживань необхідно дотримуватися ретельного балансу між свободою слова та інтересом забезпечення національної безпеки. Зокрема, трактування цього інтересу має бути достатньо вузьким.

Йоганнесбурзькі принципи щодо національної безпеки, свободи вираження поглядів та доступу до інформації, які були підготовлені у 1995 році[24], наголошують, що якщо істинною метою посилання на захист національної безпеки є захист «престижу уряду» або захист від викриття правопорушень, або ж приховування інформації про діяльність державних установ, або щеплення певної ідеології, або придушення мирних акцій протесту, то обмеження будуть неправомірними. При цьому неправомірними також пропонують вважати обмеження, спрямовані за заборону висловлювань, що обстоюють ненасильницькі зміни політики уряду або самого уряду; критики або образливих зауважень щодо нації, держави або її символів, уряду, його установ, або окремих урядовців, або іноземної нації, держави

[24] Johannesburg Principles on National Security, Freedom of Expression and Access to Information, UN Doc E/CN 4/1996/39 (1996): http://hrlibrary.umn.edu/instree/johannesburg.html.

або її символів, уряду, його установ або окремих урядовців (крім випадків, коли це може призвести до насильства та жорстокості); заперечень — на підставі релігії, сумління або переконань — щодо військової мобілізації або служби, певного конфлікту, або застосування чи загрози застосування сили у розв›язанні міжнародних конфліктів; поширення інформації про гадані порушення міжнародних стандартів з прав людини або норм міжнародного гуманітарного права.

У 2011 році у Загальному коментарі № 34 Комітет ООН з прав людини також наголосив[25], що законодавство про державну зраду та інші норми, пов'язані з забезпеченням захисту національної безпеки, мають застосовуватися лише в суворій відповідності з вимогами трискладового тесту обмеження прав людини, як і антитерористичне законодавство з його нормами про заборону підтримки терористичної діяльності та його виправдання.

Окремо слід згадати такий механізм, як санкції — або ж контрзаходи.

У 2014 році Верховна Рада України ухвалила закон «Про санкції», що передбачив можливість Ради національної безпеки і оборони приймати рішення щодо застосування спеціальних економічних та інших обмежувальних заходів до іноземних осіб та компаній з метою захисту національних інтересів, національної безпеки, суверенітету та територіальної цілісності України, протидії терористичній діяльності, а також запобігання порушенню, відновлення порушених прав, свобод та законних інтересів громадян України, суспільства та держави. На підставі цього закону указами Президента України № 133/2017 від 16 травня 2017 року, № 126/2018 від 14 травня 2018 року та № 82/2019 від 19 березня 2019 року, які вводили в дію відповідні рішення РНБО, в Україні було заблоковано понад 200 інформаційних ресурсів, серед яких популярні соціальні мережі «Вконтакте» та «Одноклассники».

Загалом санкції є прийнятними заходами реакції на здійснення порушень міжнародного права, які існують у вигляді агресії Російської Федерації на території України та безпосередньо загрожують інтересам національної безпеки. Певний напрям щодо застосування санкцій у міждержавному контексті дає Проект статей щодо міжнародної відповідальності держав за міжнародні правопорушення (ARSIWA). Відповідно до його норм (а саме статей 50—51) контрзаходи не мають впливати на зобов'язання щодо захисту фундаментальних прав людини, а також мають бути пропорційними та

[25] General comment no 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

співвідносними до завданої шкоди, при цьому враховуючи тяжкість міжнародного правопорушення та вагу прав, що обмежуються.[26]

Водночас практика блокування Інтернет-ресурсів на міжнародному рівні вважається такою, що не відповідає свободі вираження поглядів. Так, *у Загальному коментарі № 34 до Міжнародного пакту про громадянські та політичні права* у пункті 43 згадується, що будь-які обмеження щодо діяльності Інтернет-ресурсів мають бути контентно-специфічними, у той час як загальна заборона на діяльність окремих сайтів та систем не є такою, що відповідає трискладовому тесту обмеження прав людини. У вже згаданій вище *Спільній декларації про свободу вираження поглядів та Інтернет* 2011 року[27] принцип 3 (а) проголошує, що свавільне блокування сайтів, IP-адрес, портів, мережевих протоколів та окремих сервісів (таких як соціальні мережі) є надзвичайним заходом, який може бути виправданий лише відповідно до міжнародних стандартів (по суті — трискладового тесту), зокрема у випадках захисту неповнолітніх від сексуальної наруги.

У Європейському суді з прав людини розглядалося декілька справ, які стосувалися блокування веб-сайтів Туреччиною: «*Ахмет Їлдирим проти Туреччини*» *(Ahmet Yıldırım v Turkey)*[28] (блокування домену Google Sites) та «*Ченгіз та Інші проти Туреччини*» *(Cengiz and Others v Turkey)*[29] (блокування YouTube та Twitter). В обох із них суд дійшов висновку, що блокування сайтів не відповідало стандартам обмеження свободи вираження поглядів за статтею 10 Конвенції, оскільки не було передбачене законом. Отже, міжнародний режим захисту прав людини сприймає блокування сайтів лише як винятковий захід захисту прав інших осіб та національної безпеки, який є припустимим лише за рішенням суду чи іншого незалежного уповноваженого органу та лише в разі, якщо він чітко й однозначно передбачений законом, легітимний і пропорційний меті.

---

[26] Draft Articles on Responsibility of States for Internationally Wrongful Acts, from the International Law Commissions fifty-third session in 2001, in the YBILC (2001), vol. II, part two: http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

[27] U.N. Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression & ACHPR Special Rapporteur on Freedom of Expression and Access to Information, International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet (1 June 2011): http://www.osce.org/fom/78309?download=true.

[28] Ahmet Yıldırım v Turkey App no 3111/10 (ECtHR, 18 March 2013): http://hudoc.echr.coe.int/eng?i=001-115705.

[29] Cengiz and Others v Turkey App nos 48226/10 and 14027/11 (ECtHR, 1 December 2015): http://hudoc.echr.coe.int/eng?i=001-159188.

Коаліція «За вільний Інтернет» у своєму аналізі[30] Указу Президента №126/2018 Про рішення Ради національної безпеки і оборони України від 2 травня 2018 року «Про застосування та скасування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»[31] у частині запровадження «заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів, в т. ч. субдоменів», наголосила на тому, що застосування таких заходів суперечить Конституції України та міжнародним стандартам.

Зобов'язання провайдерів обмежувати доступ до окремих інформаційних ресурсів на підставі рішень РНБО про санкції не відповідає принципу законності. Так, стаття 39 Закону України «Про телекомунікації» визначає обов'язок операторів телекомунікацій блокувати доступ виключно до ресурсів, через які розповсюджується дитяча порнографія, і лише за рішенням суду. Сам Закон «Про санкції» не містить у переліку санкцій такого виду заходів, як «заборона Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів, в т. ч. субдоменів» (хоча перелік не є виключним). Водночас, відповідно до Закону України «Про Раду національної безпеки і оборони», рішення цього органу є обов'язковими виключно для органів виконавчої влади.

Варто також зауважити, що стаття 3 Закону «Про санкції» передбачає, що їх застосування має ґрунтуватися на принципах законності, прозорості, об'єктивності, відповідності меті та ефективності. Однак ні прозорих критеріїв щодо визначення підстав для блокування конкретних інформаційних ресурсів, ні інформації щодо результатів (ефективності) обмеження доступу до вказаних ресурсів оприлюднено не було.

Разом з тим Кримінальний кодекс України встановлює відповідальність за низку злочинів, пов'язаних із поширенням висловлювань, які можуть підлягати законним обмеженням у відповідності з міжнародними стандартами. Так, стаття 109 Кодексу забороняє публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплен-

---

[30] Юридичний аналіз Указу Президента №126/2018 Про рішення Ради національної безпеки і оборони України від 2 травня 2018 року «Про застосування та скасування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» в частині запровадження «заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів, в т.ч. субдоменів»: https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html

[31] Указ Президента України Про рішення Ради національної безпеки і оборони України від 2 травня 2018 року «Про застосування та скасування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: http://www.president.gov.ua/documents/1262018-24150

ня державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, а стаття 110 — публічні заклики чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України. Заборонені також публічні заклики до вчинення терористичного акту, а також розповсюдження, виготовлення чи зберігання з метою розповсюдження матеріалів з такими закликами (стаття 258-2 Кодексу) та публічні заклики до агресивної війни або до розв›язування воєнного конфлікту, (стаття 436). Отже, рішення щодо обмеження доступу до інформації, що загрожує національній безпеці, має ґрунтуватися на результатах відповідних кримінальних розслідувань, що доводять незаконність такого контенту. Ціль захисту національної безпеки повноцінно може бути реалізована лише тоді, коли припиняється сама злочинна діяльність, адже в сучасних умовах блокування будь-якого сайту можна завжди обійти або швидко створити новий сайт, що поширюватиме той же контент.

Водночас аналіз судової практики у кримінальних справах щодо наведених вище категорій висловлювань свідчить про відсутність обґрунтованого та системного підходу до їх вирішення[32].

По-перше, суди не проводять самостійного аналізу висловлювань, які є предметом розгляду, а обмежуються наведенням тези про висновок спеціаліста чи експерта щодо контенту. Таким чином, факт вчинення злочину встановлюється скоріше не судом, а судовим експертом, який надає оцінку змісту поширеного повідомлення, а роль суду найчастіше зводиться лише до констатації факту наявності кримінального правопорушення та призначення міри покарання. Наведення належної мотивації в рішеннях судів замість перерахування фактів справи, отриманих та розглянутих доказів, процесуальних моментів та цитування норм законодавства є належною гарантією справедливого судового процесу згідно зі статтею 6 Європейської конвенції з прав людини, — і тому недотримання цієї гарантії суттєво впливає на можливість подальшої апеляції рішення.

По-друге, суди не вдаються до самостійного аналізу впливу контенту на користувачів соціальних медіа. Аналіз потенційного впливу на національну безпеку відсутній у рішеннях, а самі суди рідко намагаються розмежувати контент, який загрожує національній безпеці, з мовою ворожнечі. Як наслідок, дуже подібні за змістом пости в соціальних мережах можуть бути по-різному кваліфіковані, що створює неуніфіковану практику.

---

[32] Аналітичний звіт «Свобода слова в Інтернеті: законодавчі ініціативи та практика розгляду кримінальних справ в Україні у 2014—2018 рр.»: https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf

По-третє, у восьми вироках за статтею 109 Кримінального кодексу трапляється кваліфікація судами Інтернету як засобу масової інформації, а це, у свою чергу, тягне застосування більш суворої санкції, оскільки поширення закликів у ЗМІ є обтяжуючою обставиною. Цей підхід є неуніфікованим та загрозливим, адже порушники отримують додаткове покарання за акти, яких вони не вчиняли. Крім того, попри наявність онлайн-версій традиційних медіа, важко кваліфікувати всі веб-сайти як засоби масової інформації за їх природою.

Таким чином, пріоритетом у процесі захисту національної безпеки України має стати вдосконалення правозастосовної та судової практики щодо розслідування злочинів, пов'язаних із поширенням злочинних висловлювань, а не створення нових механізмів блокування інформаційних ресурсів, що може призвести до цензури та порушень прав людини.

Рекомендації щодо свободи вираження поглядів та захисту національної безпеки:

1. *Президенту України, Раді національної безпеки і оборони України* — привести укази Президента України та практику застосування санкцій у відповідність до Конституції та міжнародних зобов'язань України, зокрема в частині обмеження доступу користувачів до визначених указами Президента України інформаційних ресурсів.
2. *Верховній Раді України (Комітету з питань гуманітарної та інформаційної політики)* — переглянути чинне законодавство в інформаційній сфері та розробити прозорі механізми оцінки контенту на предмет їх загрози національній безпеці замість непропорційної заборони широких категорій висловлювань, а також встановити тимчасовість обмежень, накладених на поширення інформації у зв'язку з агресією Російської Федерації, та процедуру періодичної оцінки їх доцільності з оприлюдненням для суспільства результатів такої оцінки.
3. *Верховній Раді України* та *Кабінету Міністрів України*— при розробці та розгляді будь-яких законодавчих (та інших регуляторних) ініціатив, спрямованих на обмеження чи припинення поширення інформації, що загрожує інтересам національної безпеки, забезпечити дотримання міжнародних стандартів прав людини. Зокрема, можливість обмеження доступу до окремих сайтів допускається лише як винятковий захід у випадку поширення такими сайтами дитячої порнографії або іншого злочинного контенту, коли такий контент становить переважну більшість матеріалів, розміщених на

ресурсі. При цьому підстави застосування блокування мають бути чітко визначені законом, застосовуватися з дотриманням належної правової процедури і лише якщо не можуть бути застосовані менш обмежувальні альтернативні заходи. Обмеження мають ґрунтуватися на рішенні суду.

4. *Верховній Раді України (Комітету з питань гуманітарної та інформаційної політики, Комітету з питань правоохоронної діяльності, Комітету з питань свободи слова)* — переглянути норми кримінального законодавства та декриміналізувати окремі види висловлювань, що не містять закликів до насильницьких дій, зокрема використання певної символіки як пропаганди тоталітарних режимів (замінити на адміністративну відповідальність). Будь-які законодавчі пропозиції, що стосуються заборони певних ідей чи символів, потребують відкритості та належного суспільного обговорення. Положення закону повинні бути достатньо конкретними та чіткими для того, щоб особа могла з достатньою впевненістю завчасно передбачити законність або незаконність своїх дій та для того, щоб запобігти свавільному втручанню органів державної влади. Лише дії, що становлять реальну загрозу суспільству, повинні тягти за собою кримінальну відповідальність, яка має бути пропорційною тяжкості вчиненого злочину. Ненасильницькі прояви свободи вираження поглядів не мають каратись позбавленням волі.
5. *Верховній Раді України та Кабінету міністрів України* — сприяти розвитку та забезпечувати проведення наукових досліджень у сфері інформаційних загроз, на основі результатів яких державні органи зможуть розробляти адекватні та ефективні заходи захисту національної безпеки.
6. *Службі безпеки України* — розробити та забезпечити впровадження методичних рекомендацій щодо розслідування злочинів у сфері національної безпеки, пов'язаних з поширенням незаконних закликів та інформації.

СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ ТА МОВА ВОРОЖНЕЧІ

Мова ворожнечі є однією з безумовно заборонених категорій висловлювань, яка не отримує захисту в міжнародному та національному праві. На міжнародному рівні (та на рівні документів обов'язкового характеру) вперше цю заборону було закріплено у статті 4 Міжнародної конвенції про ліквідацію всіх форм расової дискримінації (у вужчому контексті) та у статті 20 Міжнародного пакту про громадянські та політичні права: «*Будь-який виступ на користь національної, расової чи релігійної ненависті, що являє собою підбурювання до дискримінації, ворожнечі або насильства, повинен бути заборонений законом*». Як бачимо, такі формулювання не дають чіткої дефініції мові ворожнечі, однак встановлюють вимогу передбачити в національному законодавстві держав заборону на використання певних категорій висловлювань. Нагадаємо, що Україна ратифікувала обидва документи ще як УРСР у 1969 та 1973 роках відповідно, без будь-яких застережень до відповідних положень.

Попри загальний характер термінології, що вживалася в цих документах, міжнародні організації надалі розробили низку тестів та критеріїв, на підставі яких слід оцінювати наявність чи відсутність мови ворожнечі. Рабатський план дій, затверджений Генеральною Асамблеєю ООН у 2012 році[33], пропонує шестискладовий тест визначення «тяжкості» мови ворожнечі:

1) *контекст виловлювання*, який має помістити його в домінантну соціально-політичну ситуацію щодо таргетованої соціальної групи станом на час висловлювання;

2) *статус особи, що висловлюється*, та її можливість впливати на відповідну аудиторію;

3) *наявність умислу* в особи на підбурювання конкретної групи осіб, оскільки необережність не може призвести до підбурювання як такого в рамках термінології статті 20 Міжнародного пакту;

4) *зміст та форма висловлювання*, які є ключовими елементами для аналізу;

5) *обсяг поширення висловлювання*, який включає аналіз кількості аудиторії, до якої було донесене висловлювання, метод його поширення, чи було висловлювання публічним та чи доступне воно для широкої публіки тощо;

---

[33] UNHRC, «Rabat Plan of Action on the Prohibition of Advocacy of National, Racial or Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence» (2012): http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf.

6) *можливість та неминучість настання наслідків* після висловлювання, які мають бути оцінені державними органами при аналізі певного висловлювання крізь призму стандарту розумності.

Лише кумулятивний аналіз відповідних елементів може дати зрозуміти, чи можна кваліфікувати те чи інше висловлювання як мову ворожнечі. Інший тест розробив Європейський суд з прав людини, який у 2015 році у ключовому рішенні Великої палати щодо застосування статті 10 Європейської конвенції з прав людини — «*Перінчек проти Швейцарії*» (*Perinçek v Switzerland* [GC]) — визначив дещо інші критерії для аналізу, підсумовуючи власну практику в подібних справах. Суд окремо наголосив, що саме взаємозв'язок між різними факторами, а не наголошування на будь-якому з них окремо, має бути визначальним.

Так, у пунктах 204—207 рішення[34] суд вказав, що він зважатиме на:

1) те, чи були вирази висловлені на фоні напруженого політичного чи соціального підґрунтя;

2) те, чи можна сприймати вирази, розумно витлумачені й розглянуті в їхньому безпосередньому чи ширшому контексті, як прямий або непрямий заклик до насильства або як виправдання насильства, ненависті або нетерпимості;

3) спосіб, у який робилися вирази, та їх спроможність — пряму або непряму — призвести до шкідливих наслідків.

Європейський суд з прав людини поділяє справи щодо мови ворожнечі на дві категорії: ті, які підпадають під статтю 17 Конвенції (зловживання правами) і не підлягають захисту за жодних умов, та ті, в яких висловлювання не є явним зловживанням та потребують аналізу на предмет дотримання трискладового тесту обмеження відповідно до частини другої статті 10 Конвенції. До першої категорії зазвичай відносяться справи, вислови в яких заперечують злочини нацизму, сприяють тероризму, антисемітизму або ж закликають до встановлення тоталітарної ідеології.

У контексті Інтернету та застосування статті 17 Конвенції варто звернути увагу на рішення у справі «*Белькасем проти Бельгії*» (*Belkacem v Belgium*).[35] Заявник, керівник організації «*Sharia4Belgium*» («Шаріат для Бельгії»), котрий розмістив на YouTube низку відео, в яких закликав до джихаду та боротьби з невірними, а також висловлював коментарі із закликами до смерті бельгійських політиків, був засуджений до штрафу та півторарічного позбавлення волі за заклики до дискримінації, сегрегації, ворожнечі

[34] Perinçek v Switzerland App no 27510/08 (ECtHR, 15 October 2015): http://hudoc.echr.coe.int/eng?i=001-158235.

[35] Belkacem v Belgium App № 34367/14 (ECtHR, 27 June 2017) (dec): http://hudoc.echr.coe.int/eng?i=001-175941.

та жорстокості щодо немусульман. Його скарга до Суду щодо порушення прав за статтею 10 Конвенції була відхилена: Європейський суд погодився з висновками національних судів і ствердив, що відео, в яких заявник закликає домінувати над немусульманами, навчити їх уроку та подолати їх, становить загальний та жорстокий напад на цінності толерантності, соціальної злагоди та недискримінації, що є підвалинами Конвенції. Зважаючи також і на відповідність бельгійського законодавства у цій сфері європейським стандартам, Суд визнав заяву неприйнятною.

Щодо другої категорії справ у сфері цифрових прав, основним рішенням, вартим уваги, є рішення у справі «*Савва Терентьєв проти Росії*» (*Savva Terentyev v Russia*).[36] У цій справі заявник став жертвою першого в історії Росії застосування положень щодо мови ворожнечі до коментарів в Інтернеті. Власне, сам заявник прокоментував публікацію блогера в LiveJournal щодо обшуків у місцевій газеті в передвиборчий період. Заголовком коментаря був вираз «*ненавижу ментов, сцуконах*»; в самому ж коментарі йшлося про «*было бы хорошо, если в центре каждого города россии, … стояла печь, как в освенциме, где церемониально, ежедневно, а лучше — дважды в сутки … — сжигали бы по неверному менту. … это был бы первый шаг к очищению общества от ментовско-гопотской грязи*». Російські суди мотивували засудження заявника тим, що він однозначно підбурював до жорстокості проти такої соціальної групи, як російські поліцейські, а також свідомо розмістив свій коментар під блогом, який мав більше читачів за його власний. Вони також зазначили, що його висловлювання були особливо небезпечними для національної безпеки, оскільки суперечили засадам конституційного устрою, — і саме цим обґрунтовувалося покарання у вигляді позбавлення волі з випробувальним строком.

Європейський суд, беручи до уваги тест Перінчека, вказав, що в рамках цієї справи сконцентрується на дослідженні природи висловлювань заявника, контексту їх публікації, їх потенціалу призвести до шкідливих наслідків, а також на аналізі мотивації прийняття рішення російськими судами. Суд зазначив, що хоча коментарі та порівняння були достатньо грубими, їх слід розглядати як частину стилю комунікації, який захищається положеннями Конвенції. Такі коментарі заявника, сказані в контексті публічної дискусії щодо ролі поліції у втручанні у виборчий процес, були саркастичною емоційною реакцією заявника на дії, які здалися йому перевищенням повноважень з боку правоохоронних органів; слова ж про церемоніальне спалення невірних копів були провокативною метафорою, спрямованою не на жорстокість щодо поліцейських, а на демонстрацію його бажання очистити си-

[36] Savva Terentyev v Russia App № 10692/09 (ECtHR, 28 August 2018): http://hudoc.echr.coe.int/eng?i=001-185307.

стему поліції від корупції. Крім того, поліція як частина державного апарату має толерувати більшу кількість критики щодо себе, якщо така критика не спричиняє неминучий ризик використання насильства проти поліцейського апарату — і такий ризик не випливає з обставин справи та соціально-політичного контексту тогочасної (2007 рік) Росії.

Суд окремо наголосив на тому, що потенційний вплив висловлювання, зробленого онлайн для незначної кількості читачів, є відмінним від впливу висловлювання, опублікованого на мейнстримних або часто відвідуваних веб-сторінках. Утім російські суди навіть не зробили спроби встановити, скільки ж користувачів ознайомилося з коментарем — натомість саме провадження проти заявника привернуло увагу до цього коментаря. Більше того, Суд також відзначив, що Савва Тєрєнтьєв не був популярним блогером або користувачем соціальних медіа, що могло б принадити увагу публіки до його коментаря. Насамкінець Європейський суд звернув увагу на те, що російські суди не зробили спроби оцінити потенційні негативні наслідки коментаря заявника та встановили міру покарання, яка є непропорційною. Тому, хоча кримінальне покарання за мову ворожнечі є припустимим, відповідні норми кримінального права мають бути сформульовані так, аби не допускати надмірно широкої дискреції держави в обвинуваченні у вчиненні таких злочинів та вибіркового застосування відповідних норм. Як наслідок, було встановлене порушення статті 10 Європейської конвенції з прав людини щодо Савви Тєрєнтьєва — тобто порушення його права на свободу вираження поглядів.

Отже, окрім більш загальних тестів Європейського суду з прав людини, можна зазначити ще декілька ключових моментів із його практики, які потрібно враховувати при аналізі певного висловлювання в мережі щодо наявності мови ворожнечі:

1) використання покарання в рамках кримінального права за мову ворожнечі в Інтернеті може бути прийнятним;

2) водночас в Інтернеті варто толерувати більш грубі висловлювання, оскільки вони є природніми для комунікації в мережевому середовищі;

3) при аналізі тесту Перінчека щодо Інтернет-висловлювань варто встановлювати, наскільки широкою була аудиторія матеріалу та скільки користувачів побачили чи могли його побачити;

4) також значним фактором буде популярність користувача, який оприлюднив висловлювання, та його здатність впливати на публіку.

Українське законодавство теж містить низку положень, пов'язаних з обмеженням поширення мови ворожнечі. Передусім варто згадати статтю 161 Кримінального кодексу України, яка має назву «Порушення рівноправності громадян залежно від їх расової, національної належності, релі-

гійних переконань, інвалідності та за іншими ознаками» та є найближчою змістовно щодо заборони мови ворожнечі. Так, вона забороняє умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті — що загалом відповідає підходам, висловленим у статті 20 Міжнародного пакту про громадянські та політичні права. Покарання за вчинення таких дій — штраф у розмірі від 3400 до 8500 гривень або обмеження волі строком до 5 років з позбавленням права обіймати певні посади протягом 3 років, а за наявності обтяжуючих обставин — до 8 років позбавлення волі. Також існує стаття 300 Кримінального кодексу України, що передбачає відповідальність за ввезення в Україну творів, що пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, з метою збуту чи розповсюдження або їх виготовлення, що може каратися обмеженням волі на строк до 3 років, а за наявності обтяжуючих обставин — позбавленням волі на строк до 5 років.

Заборона на подібні висловлювання передбачена також статтею 28 Закону України «Про інформацію» («інформація не може бути використана для закликів до насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі») та статтею 6 Закону України «Про телебачення і радіомовлення» («не допускається використання телерадіоорганізацій для розпалювання національної, расової чи релігійної ворожнечі та ненависті»).

Закон України «Про засади запобігання та протидії дискримінації в Україні» також забороняє обмежувати права людини за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, віку, інвалідності, етнічного та соціального походження, громадянства, сімейного та майнового стану, місця проживання, мовними та іншими ознаками. Водночас закон є досить абстрактним та не пропонує жодних ефективних механізмів протидії мові ворожнечі.

На розгляді Верховної Ради України перебуває проект Закону про внесення змін до деяких законодавчих актів України (щодо гармонізації законодавства у сфері запобігання та протидії дискримінації із правом Європейського Союзу) № 0931[37], який попередній парламент ухвалив у першому читанні ще у 2016 році. Серед пропозицій законопроекту — зміни до статті 161 Кримінального кодексу України, що пропонують залишити кримінальну відповідальність виключно за умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образу почуттів громадян у зв›язку з їхніми релігійними переконаннями. Тоді як пряме чи непряме обмеження прав або встановлення прямих чи непрямих привілеїв громадян за ознака-

[37] Картка проекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66561

ми раси, кольору шкіри, політичних, релігійних та інших переконань, статі, інвалідності, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками — пропонується виключити з диспозиції статті Кримінального кодексу та замінити адміністративною відповідальністю шляхом доповнення Кодексу України про адміністративні правопорушення статтею 188[48] «Порушення законодавства у сфері запобігання та протидії дискримінації». Зазначені зміни, на думку авторів, забезпечать пропорційність та співмірність відповідальності за порушення законодавства в цій сфері та значно спростять процедурний механізм розгляду судами справ за фактами дискримінації.

Такий підхід у цілому відповідає міжнародним стандартам щодо розмежування жорсткої та слабкої мови ворожнечі. Водночас звуження ознак кримінально караної мови ворожнечі виключно до національних, расових та релігійних підстав не охоплює можливі небезпечні заклики до ненависті на підставі етнічного чи соціального походження, мовних або гендерних ознак.

Крім цього, потребують вирішення й суттєві проблеми у правозастосуванні норм законодавства щодо протидії мові ворожнечі. За період 2007—2018 років національні суди ухвалили 14 рішень за статтею 161, в яких суди давали оцінку тим чи іншим проявам мови ворожнечі. З-поміж цих справ лише три стосувалися поширення протиправного контенту в Інтернеті[38]. Невелика кількість справ частково спричинена кваліфікацією дій, що мають ознаки розпалювання ворожнечі, за іншими положеннями Кримінального кодексу, які містять більші міри покарання за злочини проти національної безпеки.

Характерним для цих рішень є відсутність спроби судів аналізувати зміст поширених висловлювань самостійно, не кажучи про застосування практики Європейського суду з прав людини та тесту Перінчека. Переважно суди сліпо спираються на висновки експертизи і не дають їм власної оцінки: це як коментарі у групах «Вконтакте», так і розміщення графічних файлів. Також не аналізується обсяг поширення матеріалів, кількість підписників того чи іншого користувача або користувачів певної групи; зазвичай суд зупиняється на тому, що контент був доступний усім користувачам соціальних мереж, а також надійшов як сповіщення друзям. Крім того, більшість справ закінчується укладенням угоди про визнання вини, а тому засуджені не отримують покарання за вчинене.

---

[38] Analytical report “Freedom of Expression on the Internet: Legislative Initiatives and Practice of Examination of Criminal Cases in Ukraine in 2014-2018.”: https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf

Рекомендації щодо свободи вираження поглядів та протидії мові ворожнечі:

1. *Верховній Раді України (Комітету з питань забезпечення правоохоронної діяльності, Комітету з питань прав людини)* — вдосконалити вимоги національного законодавства щодо протидії мові ворожнечі, зокрема розмежувати кримінальну та адміністративну відповідальність за дискримінаційні висловлювання, залежно від ступеня їх загрози.
2. Судам — при розгляді справ щодо поширення мови ворожнечі враховувати такі критерії при визначенні наявності, ступеня та міри покарання за мову ворожнечі:
   - *зміст та форма висловлювання*, які є ключовими елементами для аналізу. При цьому варто брати до уваги особливості комунікації в мережевому середовищі, зокрема його вищу толерантність до грубих висловлювань;
   - *контекст висловлювання* (наприклад, чи були вирази висловлені на фоні напруженого політичного чи соціального підґрунтя)*;*
   - *статус і популярність особи, що висловлюється*, та її можливість впливати на відповідну аудиторію;
   - *наявність умислу* в особи на підбурювання конкретної групи осіб;
   - *обсяг поширення висловлювання*, який включає аналіз кількості аудиторії, до якої було донесене висловлювання, метод його поширення, чи було висловлювання публічним та чи доступне воно для широкої публіки тощо;
   - *можливість та неминучість настання наслідків* після висловлювання, які мають бути оцінені державними органами при аналізі певного висловлювання крізь призму стандарту розумності. Сама по собі відсутність реальних наслідків не обов'язково виключає кримінальну відповідальність, але може впливати на міру покарання.
3. *Міністерству внутрішніх справ* — забезпечити розробку та впровадження методичних рекомендацій щодо розслідування злочинів, пов'язаних із мовою ворожнечі та погрозами онлайн. До підготовки рекомендацій залучити експертів-правозахисників.

ПРАВО НА ПОВАГУ ДО ПРИВАТНОГО ТА СІМЕЙНОГО ЖИТТЯ

Право на повагу до приватного та сімейного життя є фундаментальним правом кожної людини. Стаття 32 Конституції України встановлює, що ніхто не може зазнавати втручання в його особисте й сімейне життя, та забороняє збирати, зберігати, використовувати конфіденційну інформацію про особу без її згоди (крім випадків, визначених законом). Водночас, як і свобода вираження поглядів, це право не є абсолютним і може обмежуватись із підстав, визначених Конституцією та законами, в інтересах національної безпеки, економічного добробуту та прав людини. Важливими елементами цього права є також гарантії захисту репутації особи та право громадян знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Європейська конвенція у статті 8 також визначає, що кожен має право на повагу до свого приватного й сімейного життя, до свого житла та кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб. Європейський суд з прав людини у своїй практиці досить широко тлумачить зміст цього права, включаючи до нього найрізноманітніші аспекти розвитку та самореалізації особистості в стосунках з іншими та зовнішнім світом. Водночас, з погляду реалізації прав людини в онлайн-середовищі, доцільно детальніше зупинитися на аспектах інформаційної та комунікаційної приватності.

Право на інформаційну приватність виникло як механізм захисту від безконтрольного поширення фактів про приватне життя особи й передбачає захист персональних даних особи та іншої конфіденційної інформації про неї від їх неправомірного збирання, зберігання чи поширення. В умовах стрімкого розвитку сучасних інформаційних технологій, що дозволяють збирати, обробляти та поширювати інформацію практично про будь-яку особу в необмежених обсягах, захист інформаційної приватності особи набуває особливого значення. З цією метою на держави покладаються позитивні обов'язки щодо впровадження законодавства про захист персональних даних.

Комунікаційна приватність особи знаходить свій вияв у праві на повагу до кореспонденції особи, тобто в забезпеченні таємниці листування (у тому числі електронної), телефонних розмов особи та іншої комунікації за до-

помогою будь-яких засобів. Європейський суд досить широко, еволюційно тлумачить поняття «кореспонденція»[39], оскільки технології зв'язку постійно розвиваються й обмеження сфери захисту лише щодо класичних способів неодмінно призведе до небажаного звуження самого права на приватність. Комунікаційна приватність є гарантією конфіденційності обміну інформації між особами. Вона тісно пов›язана, але не є тотожною «інформаційній приватності», оскільки тут захист надається не тільки змісту інформації, що передається засобами зв'язку, а власне праву особи бути впевненим у тому, що його розмови не будуть доступними іншим, незалежно від засобів, якими користується ця особа для комунікації.

Будь-яке втручання в зміст комунікації операторами мережі або постачальниками послуг заборонене, за винятком, якщо це здійснюється з технічних умов запису або передавання послання, з інших законних причин, чи на виконання контракту, укладеного з абонентом. При цьому дані про особу, які були зібрані в такому порядку, можуть передаватись тільки державним органам і лише якщо це відповідає положенням п. 2 ст. 8 Європейської конвенції, зокрема, передача даних передбачена законом, необхідна в демократичному суспільстві, наприклад для захисту державної або громадської безпеки, боротьби зі злочинністю, захисту особи[40]. Це, зокрема, означає, що держава не повинна надавати правоохоронним органам неконтрольовані можливості безпосереднього доступу до приватних комунікацій.

Інтернет-користувачі мають право на анонімність та використання псевдонімів. Однак таке право не є абсолютним — особа користувача може бути розкрита за рішенням суду. Водночас законодавство має чітко встановити підстави, коли допускається розкриття такої інформації (наприклад, кримінальне розслідування). Зокрема, стаття 18 Конвенції про кіберзлочинність (Будапештська конвенція)[41] передбачає, що постачальники Інтернету на підставі ордера можуть бути зобов'язані розкривати інформацію про користувачів, яка «означає будь-яку інформацію, у формі комп›ютерних даних чи в іншій формі, яка знаходиться у постачальника послуг, відноситься до користувачів його послуг, не є даними про рух даних або власне даними змісту інформації, та за допомогою якої можна встановити:

---

39 Copland v. the United Kingdom (no. 62617/00), 3 April 2007

40 Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e

41 Конвенція про кіберзлочинність (CETS No.185): https://zakon.rada.gov.ua/laws/show/994_575

a. тип комунікаційної послуги, яка використовувалася, її технічні положення й період користування послугою;

b. особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки та платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг;

c. будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди або домовленості про постачання послуг».

Водночас, відповідно до статті 15 Будапештської конвенції, застосування таких заходів має супроводжуватись адекватним захистом прав і свобод людини та бути пропорційним, а також включати судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування й терміну таких повноважень або процедур.

У 2015 році забезпечення права на приватність було визначено одним зі стратегічних напрямків Національної стратегії у сфері прав людини[42]. Серед очікуваних результатів було визначено створення дієвого інституційного механізму контролю за додержанням права на приватність, зокрема за діяльністю правоохоронних органів, та запровадження системи, яка унеможливлює створення надмірних державних баз персональних даних та виключає можливість протиправного втручання у приватність. План дій[43], що був розроблений Кабінетом Міністрів України на виконання Стратегії, включає, серед іншого, такі заходи, як перегляд підстав проведення оперативно-розшукових заходів та негласних слідчих дій, визначення вичерпного переліку підстав, що унеможливлюють зловживання таким правом, підготовка рекомендацій щодо дотримання законодавства у сфері захисту персональних даних під час застосування систем відеоспостереження, проведення оцінки на предмет відповідності вимогам законодавства, наповнення, адміністрування та захисту таких баз персональних даних, як Єдиний державний демографічний реєстр, Реєстр пацієнтів, освітянські реєстри, і внесення пропозицій щодо правового врегулювання виявлених невідповідностей та ін. Проте жоден із перелічених пунктів досі не був виконаний.

2 вересня 2019 року у Верховній Раді України був зареєстрований проект Закону про оперативно-розшукову діяльність (№ 1229[44], ініціатор — Ко-

---

[42] Указ Президента України «Про затвердження Національної стратегії у сфері прав людини»: https://zakon.rada.gov.ua/laws/show/501/2015

[43] Розпорядження Кабінету Міністрів України «Про затвердження плану дій з реалізації Національної стратегії у сфері прав людини на період до 2020 року»: https://zakon.rada.gov.ua/laws/show/1393-2015-р - п13.

[44] Картка проекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66597.

жем'якін А.А.). Пропонована редакція закону містить чіткіші положення та гарантії, що стосуються обмеження прав людини у зв'язку з проведенням оперативно-розшукової діяльності. Водночас законопроект все ще не повною мірою відповідає міжнародним зобов'язанням у сфері прав людини. Так, документ все ще занадто широко визначає підстави для застосування оперативно-розшукових заходів (наприклад, «*потреба в отриманні розвідувальної інформації в інтересах безпеки суспільства і держави*»), а також передбачає можливість застосування таких заходів в окремих невідкладних випадках не лише без санкції суду, а навіть без погодження з прокурором. Йдеться, у тому числі, про зняття інформації з електронних інформаційних систем та каналів зв'язку.

У Верховній Раді України восьмого скликання було зареєстровано декілька законопроектів, спрямованих на розширення повноважень правоохоронних органів щодо доступу до приватних комунікацій. Так, наприклад, проект Закону «Про внесення змін до деяких законодавчих актів України (щодо вдосконалення порядку здійснення досудового розслідування» №1220 від 03.12.2014[45] передбачав обов'язок операторів телекомунікацій за власні кошти встановити на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими підрозділами органів внутрішніх справ та органів безпеки оперативно-розшукових заходів, проведення негласних слідчих (розшукових) дій та забезпечення (віддаленого) тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо, і забезпечувати функціонування цих технічних засобів. При цьому законопроект пропонував встановити можливість для слідчих в окремих «невідкладних» випадках отримувати тимчасовий доступ до такої інформації навіть без попередньої ухвали слідчого судді або суду. Схожі положення містилися й у проекті Закону «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю» №2133а[46] та проекті Закону «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері» № 6688[47], жоден з яких не був ухвалений навіть у першому читанні.

Разом з тим, 21 січня 2019 року Адміністрація Державної служби спеціального зв'язку (ДССЗЗІ) та захисту інформації України та Служба безпеки

[45] Картка проекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=1220&skl=9

[46] Картка проекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55668

[47] Картка проекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236

України затвердили спільний Наказ №25/82 «*Про затвердження Загальних технічних вимог до технічних засобів для блокування доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) в телекомунікаційних мережах*». При цьому Закон України «Про телекомунікації», що встановлює правову основу діяльності у сфері телекомунікацій, визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами, не передбачає обов'язку операторів телекомунікацій встановлювати будь-які технічні засоби для блокування доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) в телекомунікаційних мережах.

Небезпека зазначеного наказу полягає в тому, що передбачені ним технічні характеристики вказаного обладнання фактично дозволятимуть у режимі реального часу моніторити, блокувати та видозмінювати Інтернет-трафік користувачів. У наказі сказано, що обладнання має забезпечувати, зокрема, підтримку та обробку «технологій передачі голосу VoIP (Skype, Viber, WhatsApp, BBM, SIP)»; технологій для обміну миттєвих повідомлень та відео Messenger (Telegram, MS Messenger, ICQ, Jabber тощо); соціальних мереж (Twitter, Facebook, Vkontakte, «Одноклассники» тощо); технологій адаптивного транслювання потокового відео VideoStreaming (Youtube, Youtube HD, Adobe RTMP тощо)». СБУ, ДССЗЗІ чи хтось інший, хто контролюватиме відповідне обладнання, зможуть за низкою ознак визначати, на які сайти ходить користувач, а також якими месенджерами й засобами для обходу блокувань він користується, і за бажання блокувати їх або суттєво сповільнювати. При цьому реальні можливості контролювати дотримання законодавства при використанні такого обладнання, зважаючи на можливості віддаленого доступу до нього правоохоронців, відсутні[48].

У справі «*Роман Захаров проти Росії*»[49] Європейський суд розглядав російське законодавство, яке дозволяло здійснювати таємне перехоплення мобільних телефонних комунікацій за допомогою подібних технічних засобів. Зокрема, суд звернув увагу на технічні можливості щодо безпосереднього доступу до обладнання, що дозволяє забезпечувати відповідні заходи. Суд визнав, що спосіб здійснення таємного спостереження в Росії надає службам безпеки та поліції технічні засоби для обходу процедури санкціонування та перехоплення будь-яких повідомлень без попереднього судового дозволу. Хоча можливість зловживання з боку недобросовісних чиновників, ніколи не може бути повністю виключена незалежно від систе-

[48] https://zaborona.com/interactive/nash-onlajn-leviafan/

[49] Roman Zakharov v. Russia (no. 47143/06) 4 December 2015

ми (див. «*Клас та інші проти Німеччини*»), Суд вважає, що така система, як російська, яка дає змогу спецслужбам і поліції безпосередньо перехоплювати комунікації кожного громадянина, не вимагаючи від них навіть ставити до відома провайдерів телекомунікаційних послуг, унеможливлює ефективний контроль за законністю таких заходів. У подібній системі ризик зловживань, притаманний будь-якій системі таємного спостереження, стає особливо загрозливим.

Зважаючи на це, законодавство має передбачати адекватні та ефективні гарантії проти свавілля. Це охоплює, зокрема, чітке визначення підстав та обставин для втручання, зрозумілі правила щодо припинення перехоплення, зберігання та знищення отриманої інформації. Процедури санкціонування мають гарантувати, що заходи таємного спостереження застосовують лише тоді, коли вони справді «необхідні в демократичному суспільстві» (відповідають меті, пропорційні, обґрунтовані). Нагляд за перехопленням має відповідати вимогам незалежності, орган контролю також повинен мати достатньо повноважень і компетенції для здійснення ефективного та постійного нагляду за дотриманням законодавства при застосуванні заходів спостереження. Законодавство має також передбачати можливості захисту у випадку неналежного застосування таких заходів до особи.

Українське законодавство на сьогодні не регулює використання таких технічних засобів для здійснення оперативно-розшукових заходів (утім, як і для блокування інформаційних ресурсів). Тобто гарантії, необхідні для захисту таємниці комунікацій від свавільного втручання, на сьогодні відсутні. Саме тому встановлення обладнання з технічними характеристиками, що дозволяють безпосередній доступ представникам правоохоронних органів, створить можливості для безконтрольного втручання в наші електронні комунікації і є неприпустимим.

Рекомендації щодо захисту комунікаційної приватності особи:

1. *Верховній Раді України та іншим суб'єктам законодавчої ініціативи* — гарантувати, що всі законодавчі ініціативи, що передбачають втручання в приватне життя з боку державних органів, зокрема щодо таємниці електронних комунікацій, будуть підлягати відкритому й широкому обговоренню (у тому числі з участю правозахисників), з метою забезпечити відповідність пропонованих обмежень міжнародним стандартам законності, легітимності, пропорційності, виправданості та обґрунтованості обмежень.
2. *Верховній Раді України* — переглянути законодавство у сфері оперативно-розшукової, контррозвідувальної діяльності та

кримінального процесу, щоб забезпечити відповідність правових норм вимогам передбачуваності та прозорості:

- чітко й точно сформульоване, доступне для ознайомлення законодавство, що дає можливість зрозуміти, за яких обставин можуть застосовуватись відповідні заходи спостереження та зняття інформації;
- мінімальні гарантії щодо обмеження дискреційних повноважень органів влади: визначений характер порушень, за які може застосовуватись захід, категорій осіб, які можуть підлягати моніторингу, процедура проведення дій, гранична тривалість, порядок аналізу, використання та зберігання отриманих даних, умови передачі даних іншим суб'єктам або їх знищення
- зобов'язати провайдерів телекомунікацій розкривати інформацію про виконання запитів правоохоронних органів щодо надання доступу до даних особи, за винятком випадків, коли розкриття такої інформації прямо заборонене процесуальним законодавством та є необхідним в демократичному суспільстві.

3. *Верховній Раді України (Комітету Верховної Ради України з питань правоохоронної діяльності)* — забезпечити відкрите й широке обговорення проекту Закону про оперативно-розшукову діяльність № 1229 з метою усунення загроз праву громадян на приватність та забезпечення відповідності положень законопроекту міжнародним стандартам.
4. *Верховній Раді України (Комітету з питань цифрової трансформації)* — забезпечити приведення законодавства у сфері електронних комунікацій у відповідність зі стандартами ЄС та Ради Європи, у тому числі Конвенцією про кіберзлочинність.
5. *Кабінету Міністрів України, Уповноваженому Верховної Ради України з прав людини* — забезпечити виконання Плану дій Національної стратегії у сфері прав людини в частині захисту права особи на приватність, зокрема запровадити регулярне щорічне звітування правоохоронних органів щодо застосування заходів, пов'язаних із втручанням у таємницю електронних комунікацій та зобов'язати відповідні правоохоронні органи оприлюднювати зазначену інформацію на своїх веб-сайтах.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Окремим важливим аспектом захисту приватності особи є виконання державою позитивних обов'язків щодо створення належної законодавчої та інституційної системи захисту персональних даних.

Закон України «Про захист персональних даних» був ухвалений у 2010 році й відтоді не зазнавав істотних змін. Водночас Конвенція Ради Європи про захист осіб у зв›язку з автоматизованою обробкою персональних даних, на виконання якої його було прийнято, була істотно модернізована у травні 2018 року відповідним Протоколом CM(2018)2[50]. Україна поки що не приєдналася до Протоколу, але взяла на себе зобов'язання привести законодавство про захист персональних даних у відповідність із вимогами ЄС. Так, відповідно до пункту 11 Плану заходів щодо виконання Угоди про асоціацію з ЄС, затвердженого Постановою Кабінету Міністрів України №1106 від 25.10.2017[51], передбачено вдосконалення законодавства про захист персональних даних для приведення його у відповідність із Загальним регламентом захисту даних, що набув сили 25 травня 2018 року[52]. Підготовку відповідного законопроекту здійснює Уповноважений Верховної Ради України з прав людини. Водночас, зважаючи на комплекс суспільних відносин, яких стосуватимуться зміни до законодавства, варто забезпечити відкритий процес підготовки нової редакції закону, у тому числі з участю експертів-правозахисників.

Первинним обов'язком будь-якої держави-учасниці Європейської конвенції є впровадження законодавчих гарантій забезпечення прав особи, тобто має існувати належне правове регулювання відносин приватності. Незважаючи на значну свободу розсуду, надану державам щодо забезпечення поваги до приватного та сімейного життя особи, стандарти Європейської конвенції мають бути дотримані. Зокрема, для захисту інформаційної приватності особи держави повинні забезпечити принципи справедливості, законності та пропорційності при збиранні та обробці персональних даних, передбачити права та обов'язки суб'єктів відповідних правовідносин, а також створити органи, які здійснюватимуть контроль за дотриманням зазначених принципів і захищатимуть порушені права[53].

---

[50] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[51] Постанова Кабінету Міністрів України «Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони»: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF

[52] Загальний регламент захисту даних: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf

Як зауважив Європейський суд, будь-яке зберігання персональних даних органами влади вважається втручанням у право на повагу до приватного життя[54], тому обов'язково має бути виправдане легітимною метою. Зважаючи на це, створення та функціонування будь-яких державних реєстрів має бути виправдане легітимною метою, а перелік, обсяг інформації, її використання та порядок доступу до неї третіх осіб мають бути чітко врегульовані законом.

Так, Конституційний Суд України у своєму рішенні від 11 жовтня 2018 року[55] у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) окремих положень абзацу першого пункту 40 розділу VI «Прикінцеві та перехідні положення» Бюджетного кодексу України визнав неконституційними норми, відповідно до яких: «під час здійснення повноважень з контролю за дотриманням бюджетного законодавства в частині моніторингу пенсій, допомог, пільг, субсидій, інших соціальних виплат Міністерство фінансів України має право на безоплатне отримання інформації, що містить банківську таємницю, персональні дані, та на доступ до автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателем (адміністратором) яких є державні органи або органи місцевого самоврядування».

Конституційний Суд зауважив, що Міністерство може бути наділене повноваженнями щодо отримання та обробки інформації, що містить персональні дані, лише для досягнення легітимної мети. Проте через відсутність будь-яких меж дискреції, встановленої законом, щодо подальших дій з інформацією, яка містить персональні дані, унеможливлювався навіть мінімальний захист суб'єкта персональних даних. Оспорюваними положеннями Кодексу не передбачено критеріїв визначення змісту та обсягу інформації, що містить персональні дані, категорій осіб як суб'єктів персональних даних, проміжків часу, яких мають стосуватися персональні дані, строків, порядку та умов їх зберігання, тобто чітко не встановлено меж повноважень державного органу, що унеможливлює настання відповідальності

---

53 Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling: https://www.garanteprivacy.it/documents/10160/10704/Recommendation+2010+13+Profiling.pdf/42ed93be-031c-4298-bed7-ae79231c7ad5?version=1.2

54 Leander v. Sweden (no. 9248/81), 26 March 1987.

55 Рішення Конституційного Суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) окремих положень абзацу першого пункту 40 розділу VI „Прикінцеві та перехідні положення" Бюджетного кодексу України: http://ccu.gov.ua/docs/2406

держави за можливі зловживання. Отже, суд констатував, що наведені норми не відповідали критерію якості закону — суперечили таким елементам принципу верховенства права, як юридична визначеність і заборона свавілля, що могло призвести до порушення конституційного права кожного на приватне життя. Проаналізовані судом критерії доцільно застосувати до аналізу відповідності повноважень державних органів та посадових осіб до державних реєстрів та інших баз даних, що містять персональні дані громадян. Крім цього, варто також наголосити, що державні органи зобов'язані вживати ефективних технічних та організаційних заходів задля захисту конфіденційної інформації від несанкціонованого доступу.

Водночас, якщо щодо захисту персональної інформації, що міститься в державних базах даних, існує певна нормативна база, то питання збирання, зберігання та обробки інформації системами відеоспостереження залишаються поза увагою законодавця, позбавляючи громадян можливостей ефективно захистити свої права. Так, лише в Києві на сьогодні встановлено понад 7 тисяч камер відеоспостереження, і, за даними Київської міської державної адміністрації[56], ця кількість буде зростати.

Рекомендації щодо вдосконалення захисту персональних даних:

1. *Президенту України, Кабінету Міністрів України (Мін'юст, МЗС) та Верховній Раді України (Комітет з питань зовнішньої політики та міжпарламентського співробітництва)* — підписати та ратифікувати Протокол змін до Конвенції про захист осіб у зв›язку з автоматизованою обробкою персональних даних (CETS No.223), що посилює вимоги до захисту персональних даних країнами Ради Європи та був відкритий до підписання 10 жовтня 2018 року.
2. *Верховній Раді України (Комітет з питань інтеграції України з Європейським Союзом, Комітет з прав людини), Уповноваженому Верховної Ради України з прав людини* — привести національне законодавство у відповідність із вимогами оновленої Конвенції та Загального регламенту ЄС з захисту даних, з дотриманням таких рекомендацій:

   а) Прозорість та інклюзивність мають бути забезпечені на всіх етапах розробки та розгляду відповідного законопроекту. Доцільно також провести міжнародну експертизу підготовленого документа на предмет його відповідності стандартам РЄ та ЄС.

[56] https://kyivcity.gov.ua/news/bezpechna_stolitsya_kiv_uviyshov_u_top-50_mist_svitu_z_naybilshim_pokrittyam_kamerami_videosposterezhennya

б) Впровадити щонайменше такі мінімальні стандарти захисту персональних даних:

- *Законність* — поєднання чіткої законодавчої підстави, легітимної цілі, відкритості та поінформованості користувачів про обробку персональних даних;
- *Обґрунтованість мети обробки* — конкретна, законна й обмежена в часі;
- *Мінімізація даних* — обсяг зібраних даних має бути відповідним, не надмірним та адекватним меті;
- *Достовірність інформації* — інформація має бути актуальною й достовірною, користувачі можуть вимагати оновлення, виправлення чи видалення інформації;
- Впровадження заходів технічного захисту та конфіденційності інформації;

в) Гарантувати щонайменше такі права осіб, пов'язані з обробкою їх даних:

- Право на *доступ до інформації* про власні дані та їх обробку та право на роз'яснення інформації щодо обробки персональних даних особи;
- Право *заперечувати проти обробки* персональних даних, зокрема коли йдеться про використання алгоритмів для профайлінгу;
- Право *вимагати видалення* персональної інформації, яка не відповідає принципам обробки персональних даних;
- Право на *виправлення неточної інформації*;

г) Винятки із зазначених принципів та обмеження прав осіб мають бути визначені в законі, що включає: чіткі й однозначні підстави, процедуру судового нагляду та механізми відшкодування у разі незаконних дій.

3. *Верховній Раді України (Комітет з прав людини), Уповноваженому Верховної Ради України з прав людини, Кабінету Міністрів України* — забезпечити створення незалежного наглядового органу у сфері захисту персональних даних та забезпечити достатні ресурси для ефективного здійснення його повноважень. Зокрема, до повноважень наглядового органу потрібно включити здійснення можливості проводити розслідування щодо випадків порушення вимог законодавства та накладення санкцій, ініціювати судовий розгляд у разі виявлення порушень вимог щодо обробки персональних даних. Наглядовий орган також має сприяти організаціям та

установам, у тому числі приватним компаніям, у дотриманні законодавства через підготовку рекомендацій, надання консультацій тощо.

4. *Кабінету Міністрів України, Уповноваженому Верховної Ради України з прав людини* — забезпечити виконання Плану дій Національної стратегії у сфері прав людини, зокрема цілей щодо захисту персональних даних:
    - Підготувати рекомендації щодо дотримання законодавства у сфері захисту персональних даних під час застосування систем відеоспостереження;
    - Провести оцінку на предмет відповідності вимогам законодавства, наповнення, адміністрування та захисту таких баз персональних даних, як Єдиний державний демографічний реєстр, Реєстр пацієнтів, освітянські реєстри, і внесення пропозицій щодо правового врегулювання виявлених невідповідностей;
    - Провести ревізію баз даних, які ведуться правоохоронними органами, з метою приведення їх у відповідність із вимогами закону або скасування та ін.

ПРАВА ЛЮДИНИ ОНЛАЙН ТА ПРИВАТНІ КОМПАНІЇ

Загальна декларація прав людини, міжнародні пакти та конвенції на сьогодні покладають обов'язки щодо дотримання та захисту прав людини виключно на держави. Хоча варто заеначити, що Декларація все ж закликає закликає всіх поважати та просувати права людини.

Водночас кількість активних користувачів Facebook у 2019 року щомісяця становить вже понад 2,4 млрд осіб[57], а в найпопулярнішого сервісу Google — YouTube — близько 2 млрд користувачів[58]. Це більше, ніж населення будь-якої країни світу (принаймні, за офіційними даними). При цьому можливості платформ впливати на інформацію, яку отримують та поширюють користувачі, та можливості збирати персональні дані часто перевищують повноваження будь-яких державних органів, за винятком, можливо, Китаю та кількох інших недемократичних країн.

Зважаючи на це, закономірним є питання, чи не час великим онлайн-платформам брати на себе зобов'язання дотримуватись високих міжнародних вимог у сфері прав людини, і, відповідно, чи зможуть громадяни отримати ефективний і дієвий механізм оскаржувати порушення своїх прав з боку таких платформ.

Власне, Європейський Союз вже передбачив серйозні зобов'язання щодо захисту персональних даних для великих Інтернет-корпорацій і навіть показово застосував свої високі штрафи до Google (50 млн євро за порушення вимог щодо інформованої згоди[59]). Дещо раніше суди ЄС визнали існування «права бути забутим», яке зобов'язує видаляти з результатів пошуку посилання на окремі публікації.

Разом з тим, ці заходи поки ніяк не зачіпають інші загрози правам людини з боку великих корпорацій, зокрема видалення контенту та блокування користувачів на основі правил платформ, що часто суперечать міжнародним стандартам свободи слова. Про це свідчить аналіз міжнародної організації «Артикль 19», яка оцінювала Стандарти спільноти Facebook[60], Youtube[61] та Правила Twitter[62]. Зокрема, суперечності є не лише у використ-

---

57 https://newsroom.fb.com/company-info/

58 https://variety.com/2019/digital/news/youtube-2-billion-users-tv-screen-watch-time-hours-1203204267/

59 http://yur-gazeta.com/golovna/google-oshtrafovano-na-50-mln-za-porushennya-norm-gdpr.html

60 https://www.article19.org/resources/facebook-community-standards-analysis-against-international-standards-on-freedom-of-expression/

61 https://www.article19.org/resources/youtube-community-guidelines-analysis-against-international-standards-on-freedom-of-expression/

62 https://www.article19.org/resources/twitter-rules-analysis-against-international-standards-on-freedom-of-expression/

танні низки оціночних категорій при обмеженні «незаконного контенту», але й відсутні ефективні можливості для оскарження обмежень чи навіть отримання пояснень підстав для його застосування. Водночас варто зауважити, що Google, до прикладу, оприлюднює інформацію про видалення контенту у відповідь на вимоги суду чи державних органів у публічній базі «Lumen»[63].

Окремої уваги заслуговує використання алгоритмів для фільтрації та пріоритизації контенту, який ми переглядаємо. Так, результати пошуку, які ми отримуємо, часто залежать не лише від мови, але й від багатьох інших (часто прихованих) факторів, які базуються на інформації про нас, яка зберігається корпорацією. І хоча це нібито має сприяти швидкому пошуку саме того, що нам потрібно, це також створює для нас «інформаційну бульбашку», тобто навпаки — обмежує наші можливості доступу до знань.

Сфера взаємин у трикутнику «держава — приватні компанії — особи» досить довго залишалася без будь-яких спроб регулювання з боку міжнародної спільноти. Саме тому питання дотримання прав людини у цьому трикутнику також залишається достатньо дискусійним щодо розподілу ролей між основними гравцями. У 2011 році ООН підготувало та оприлюднило «Керівні принципи щодо бізнесу та прав людини», також за іменем автора названі «Принципами Раггі».[64] Вони містять певні нариси щодо того, якою має бути корпоративна соціальна відповідальність бізнесу щодо дотримання прав людини. Так, вони передбачають, що держава має в законодавстві передбачити обов'язок підприємств поважати у своїй діяльності права людини й надати керівні роз'яснення з цього приводу. У районах, вражених конфліктами, держава має допомагати підприємствам ідентифікувати та запобігати ризикам їхньої діяльності для дотримання прав людини, а також відмовляти в будь-якій допомозі бізнесу, що пов'язаний із серйозними порушеннями прав людини. При цьому підприємства мають уникати будь-якого шкідливого впливу на права людини, гарантовані Міжнародним біллем про права людини, та усувати шкідливий вплив там, де він виникає з їхньої діяльності. Цей документ також закликає кожен бізнес мати політику з дотримання прав людини та проводити due diligence прав людини. Як держави, так і бізнес, мають також забезпечити належний та ефективний механізм відшкодування збитків, завданих порушенням прав людини з їхнього боку.

У 2019 році на важливість ролі приватних корпорацій у сфері регулювання свободи вираження поглядів звернули увагу і Спеціальні доповідачі

---

63 https://lumendatabase.org/

64 https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

з питань свободи вираження проглядів міжнародних та регіональних організацій з захисту прав людини. У своїй Спільній декларації «Виклики для свободи вираження поглядів у наступному десятиріччі»[65] вони наголосили на необхідності імплементації компаніями «Принципів Раггі», з подальшим наглядом держави за такою імплементацією. Вони також закликали до розвитку незалежних механізмів нагляду, прозорості та відповідальності з участю всіх зацікавлених сторін задля перегляду правил розміщення контенту, які суперечать міжнародним стандартам у сфері захисту прав людини, — тобто до співрегуляції у сфері регулювання контенту.

[65] https://www.article19.org/wp-content/uploads/2019/07/Joint-Declaration-2019-Final-text.pdf.

Рекомендації щодо ролі держави стосовно захисту прав людини в діяльності приватних компаній:

1. *Кабінету міністрів України, Уповноваженому Верховної Ради України з прав людини* — ініціювати та сприяти повноцінному діалогу органів державної влади з представниками громадянського суспільства та приватними корпораціями щодо забезпечення прав людини в діяльності приватних компаній.
2. *Верховній Раді України (Комітету з питань гуманітарної та інформаційної політики, Комітету з питань цифрової трансформації)* — ініціювати обговорення з експертами, представниками Інтернет-платформ та органів державної влади щодо доцільності законодавчого закріплення вимог з прозорості та підзвітності діяльності Інтернет-компаній, зокрема у сферах реклами (у т. ч. політичної), захисту персональних даних, протидії дезінформації.
3. *Верховній Раді України (Комітету з питань гуманітарної та інформаційної політики, Комітету з питань цифрової трансформації, Комітету з питань правової політики та ін.), Міністерству цифрової трансформації* — розробити ефективні засоби правового захисту людини від порушення її фундаментальних прав з боку приватних компаній (шляхом удосконалення антимонопольного законодавства, законодавства у сфері персональних даних, зобов'язання платформ визначити механізми ефективного оскарження тощо).
4. *Верховній Раді України (Комітету з питань гуманітарної та інформаційної політики, Комітету з питань цифрової трансформації)* — створити умови та активно сприяти започаткуванню механізмів співрегулювання для забезпечення прав людини в діяльності Інтернет-платформ.
5. *Кабінету Міністрів України, Уповноваженому Верховної Ради України з прав людини* — забезпечувати ефективну комунікацію уряду з представниками найбільших міжнародних Інтернет-платформ щодо викликів дезінформації та порушення прав людини у зв'язку з військовою агресією Російської Федерації.
6. *Кабінету Міністрів України* — впроваджувати спільні програми щодо підвищення Інтернет-грамотності громадян, роз'яснення прав користувачів соціальних мереж щодо їх прав, захисту від шкідливого контенту тощо.

ВІДПОВІДАЛЬНІСТЬ ІНТЕРНЕТ-ПОСЕРЕДНИКІВ ЗА НЕЗАКОННИЙ КОНТЕНТ

Реалізація прав у мережі була б неможливою без ролі посередників — Інтернет-платформ, Інтернет-провайдерів, розробників фізичної інфраструктури Інтернету, завдяки яким здійснюється доступ до мережі. З одного боку, більшість таких посередників виконує пасивну роль і не має жодного впливу на онлайн-контент. Отже, вони є нічим іншим, як аналогом поштаря, який сприяє доставці інформації з одного місця на інше. З іншого боку, з розвитком технологій та алгоритмів низка веб-сайтів (значною мірою — соціальних мереж та пошуково-рекламних сервісів) почала впливати на ранжування контенту, надала можливість його автоматично фільтрувати та створила екосистему, що дозволяла видаляти шкідливий контент. Цим самим деякі веб-сайти створили власну регуляторну систему, яка є повністю незалежною від державної за винятком надзвичайних випадків бездіяльності посередника. Все це ставить питання про те, якою є система відповідальності посередників в Україні та світі на зараз та якої модифікації вона потребує.

Стаття 14 Директиви Європейського союзу 2000/31/ЄС про електронну комерцію встановлює так званий принцип «*safe harbour*», за яким постачальники послуг хостингу (до яких належать, зокрема, соціальні мережі — відповідно до рішення Суду справедливості ЄС у справі «*SABAM v Netlog*»[66]) звільняються від відповідальності за розміщений ними контент у разі, якщо:

1) не мають відомостей про незаконну діяльність та контент або про обставини, з яких випливає очевидний незаконний характер такої діяльності (*«actual knowledge»*);

2) отримавши відомості про таку діяльність та контент, діють достатньо оперативно для видалення або обмеження доступу до такого контенту (*«expeditious removal»).*

Ці положення також перегукуються з пунктами американського DMCA (Digital Millenium Copyright Act). Обидва акти заклали основу для режиму «*notice-and-takedown*» як основної процедури, що використовується для обмеження доступу до шкідливого контенту в мережі. У Директиві про електронну комерцію у статті 15 також наголошується, що держави не можуть зобов›язати посередників загального обов›язку моніторити інформацію, що передається через них, або ж проактивно шукати факти чи обставини, які свідчать про незаконний контент чи активність. При цьому моніторинг в окремих випадках не забороняється.

---

66 SABAM v. Netlog NV, Case C 360/10: http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=150383

У 2011 році Спеціальні доповідачі міжнародних організацій зі свободи вираження поглядів видали Спільну декларацію про свободу вираження поглядів та Інтернет[67], де у принципі 1 (c) було наголошено на необхідності розробки собливого регулювання для мережі. Щодо посередників у принципах 2 (a) та 2 (b) Декларації зазначається таке:

1) жоден, хто надає технічні сервіси з доступу до Інтернету (зокрема, надання доступу, пошукового функціоналу, передачі або кешування до інформації), не може бути притягнутий до відповідальності за контент, створений іншими й розповсюджений на цих платформах, до того часу, доки вони не втручаються у контент або відмовляються підкоритися судовому рішенню щодо видалення такого контенту; при цьому варто розглянути можливість поширення цього режиму на будь-яких посередників;

2) посередники не можуть бути змушені моніторити користувацький контент та не можуть бути зобов›язані до позасудового обмеження доступу до контенту у разі, якщо такий механізм не відповідає стандартам свободи вираження поглядів.

Отже, Декларація підсумовує положення різноманітних національних режимів регулювання щодо того, чим є «actual knowledge», додавши чіткішу вимогу щодо ролі судів у прийнятті рішень про обмеження доступу до чи видалення шкідливого контенту. Ця вимога є гарантією дотримання процесуальних прав як посередників, так і користувачів. У 2017 році у своїй Спільній декларації щодо свободи вираження поглядів, «фейкових новин», дезінформації та пропаганди у принципі 1 (d) гарантія судового розгляду була деталізована та розширена, а імунітет посередників було рекомендовано поширити на всі випадки, окрім втручання таких посередників у контент або ж їх відмови підкоритися рішенню щодо видалення контенту, прийнятому відповідно до гарантій належного процесу незалежним, безстороннім та авторитетним наглядовим органом (таким, як суд).

Основним та до певної міри кодифікаційним документом у сфері відповідальності посередників є Манільські принципи щодо відповідальності посередників, розроблені світовими неурядовими організаціями у 2015 році та покликані підсумувати найкращі практики з обмеження відповідальності посередників за контент у мережі[68]. Серед основних положень щодо відповідальності посередників варто відзначити такі:

принцип I (b) — посередники мають імунітет від користувацького контенту у випадках, коли вони не втручалися в модифікацію такого контенту;

---

[67] Joint declaration on freedom of expression and the Internet: https://www.osce.org/ru/fom/78310

[68] Manila Principles on Intermediary Liability: https://www.manilaprinciples.org/principles

принцип I (d) — режим відповідальності посередників ніколи не може включати вимоги активного моніторингу контенту;

принцип II (a-b) — посередники не мають обмежувати контент, окрім як за рішенням незалежної та безсторонньої судової установи, яка встановила протиправність контенту, причому таке рішення має включати визначення протиправності контенту в певній юрисдикції, описувати та давати Інтернет-ідентифікатор такого контенту, аналізувати докази на підтримку обґрунтування рішення та, де це застосовно, вказувати на періодичність обмеження;

принцип III (d) — у разі, якщо посередники застосовують позасудовий механізм обмеження доступу до контенту, вони не мають змістовно оцінювати контент, а повинні направляти обґрунтовані скарги до особи, що створила відповідний контент («notice-and-notice»);

принцип IV — будь-яке обмеження контенту має бути лімітоване до конкретної одиниці контенту, а для обмеження мають застосовуватися найменш обмежувальні технічні заходи — включно з можливістю обмежувати доступ до контенту в певному географічному регіоні та/або на певний період часу з можливістю періодичного перегляду;

принцип V — закони та політики з обмеження контенту мають поважати належний процес включно з правом бути заслуханим, правом на апеляцію тощо, а також мають брати до уваги права людини;

принцип VI (b) — уряд не може використовувати позасудові заходи для обмеження контенту, в тому числі через тиск до змін умов користування посередниками;

принцип VI (d-e) — уряди та посередники мають публікувати звіти з прозорості з інформацією про всі запити на обмеження контенту та їх виконання.

Станом на зараз цей документ є одним з найбільш комплексних щодо відповідальності посередників та компілює найкращі практики, які підлягають імплементації при створенні та оновленні законодавства у сфері регулювання Інтернету.

Однією ж з найсвіжіших є Рекомендація Комітету Міністрів Ради Європи CM/Rec(2018)2[69] щодо ролей та відповідальності Інтернет-посередників. Вже у преамбулі наголошується, що з розвитком технологій класична класифікація посередників на активних та пасивних втратила свою роль, оскільки один посередник може виконувати різні ролі — як просто надавати доступ до інформації, так і здійснювати контроль над нею через модерацію та

[69] Рекомендація Комітету Міністрів Ради Європи CM/Rec(2018)2 щодо ролей та відповідальності Інтернет-посередників: https://rm.coe.int/1680790e14

ранжування. Рекомендація обертається довкола деталізації трискладового тесту обмежень у контексті посередників. Зокрема, вона підтверджує необхідність будь-якого законодавства у цій сфері гарантувати права людини, а також вказівку державам щодо публікації інформації про запити щодо обмеження доступу до шкідливого контенту, а посередникам — щодо прозорості їх діяльності з обмеження контенту як за державними, так і за приватними запитами. Пункт 1.3.2 містить вказівку на необхідність отримання рішення суду або іншої незалежної адміністративної установи, рішення якої підлягають судовому перегляду, задля обмеження доступу до контенту (окрім випадків очевидної незаконності контенту або наявності вимог щодо оперативного видалення).

Укотре підкреслюється заборона прямо чи непрямо накладати на посередників обов›язки щодо загального моніторингу контенту. Одним із ключових у документі є пункт 1.3.7, який знову наголошує на режимі «*safe harbour*», однак припускає співвідповідальність посередників у випадку, якщо вони недостатньо оперативно обмежують доступ до контенту після отримання інформації про його незаконність. Водночас отримання сповіщень про таку потенційну незаконність має базуватися на юридичному аналізі з боку державних органів, а не самого посередника; відповідний режим відповідальності не має заохочувати обмеження доступу до легального контенту. Рекомендація також закликає до встановлення диференційованого підходу до відповідальності посередників.

Також Рекомендація згадує й про модерацію контенту самими посередниками. Пункт 2.3 документа наголошує на використанні найменш обмежувальних технічних засобів у цьому процесі, суворому обмеженні обсягів блокування чи видалення контенту, а також комунікації причин ужиття таких заходів. Щодо застосування автоматичних систем ідентифікації контенту, то вони визнаються корисними для обмеження появи контенту, що вже був обмеженим у доступі, однак вказується, що ці системи недостатньо розуміють контекст висловлювань і потребують людського нагляду. При їх застосуванні слід зважати на ризик надто обмежувального або навпаки, надто м›якого регулювання.

Можна підсумувати, що в останні роки концепція «*safe harbour*» не втратила своїх позицій та загалом залишається домінантною щодо визначення режиму відповідальності посередників за поширення шкідливого контенту. Водночас чіткіше викристалізувався стандарт необхідності отримати «*actual knowledge*» щодо незаконності контенту через судове рішення чи рішення іншого незалежного органу. Обмеження доступу до контенту посередниками має забезпечуватися через найменш обмежувальні заходи задля забезпечення прав користувачів таких посередників в Інтернеті. При

цьому самі посередники мають бути максимально усунуті від необхідності самостійно оцінювати контент на відповідність законодавству чи міжнародним стандартам у сфері свободи вираження поглядів, а також на них не може бути покладено обов›язок з моніторингу інформації, що проходить через платформу.

Друге проблемне поняття у сфері відповідальності посередників — те, наскільки оперативним має бути обмеження доступу до контенту у разі отримання відомостей про його протиправність. Ця сфера належить до дискреції держав, які є суверенними у створенні національних режимів регулювання, а міжнародні стандарти зазвичай обмежуються загальними фразами щодо достатньої швидкості та належної кількості часу для прийняття посередником рішення. Існує невелика кількість документів, в яких розроблялося поняття «expeditious removal» на транснаціональному рівні. Зокрема, у 2016 році в рамках Європейського Союзу було підписано Кодекс поведінки щодо протидії незаконній мові ворожнечі онлайн. Підписанти, до яких належать Facebook, Microsoft, Twitter, Google та інші, погодилися взяти на себе зобов›язання переглядати більшість сповіщень щодо видалення незаконної мови ворожнечі протягом 24 годин та, у разі потреби, видаляти такий контент або обмежувати до нього доступ. У Рекомендації Європейської Комісії C(2018) 1177 щодо заходів ефективної протидії протиправному контенту онлайн[70] згадується строк в 1 годину після отримання сповіщення для видалення терористичного контенту.

Утім на міжнародному рівні домінантною є позиція, що аналіз того, чи достатньо оперативно було обмежено доступ до контенту, має залежати від природи контенту в кожній конкретній справі, що підводить нас до третьої важливої категорії у сфері відповідальності посередників — який контент є протиправним. Саме від шкідливості потенційного впливу контенту прямо залежною є вимога щодо швидкості видалення контенту.

У справі «Delfi AS v Estonia»[71] Європейський суд з прав людини розглянув питання відповідальності новинного порталу за образливі коментарі, що були розміщені під однією із публікацій. Суд окреслив низку критеріїв, які вплинули на його аналіз та рішення про відсутність порушення свободи вираження поглядів у цій справі. Суд узяв до уваги контекст коментарів, заходи, вжиті посередником для обмеження доступу до протиправного контенту, відповідальність безпосередніх авторів контенту як альтернатива відповідальності посередника, а також наслідки провадження в національних

[70] European Commission Recommendation C(2018)1177 on measures to effectively tackle illegal content online: https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[71] Delfi AS v. Estonia (no. 64569/09) 16 June 2015

судах для компанії-посередника (виплата моральної компенсації на суму 320 євро). У своєму аналізі суд дійшов висновку, що коментарі, які є предметом розгляду справи, слід класифікувати як мову ворожнечі й заклики до насильства та визнав, що коментарі були видалені достатньо оперативно (у день отримання скарги). Утім, оскільки новинний портал мав економічний інтерес у публікації коментарів, лише сам портал мав технічну спроможність видаляти коментарі, а також зважаючи на ускладненість ідентифікації анонімних коментаторів та очевидно протиправний характер коментарів, видалення яких іноді необхідне навіть без сповіщень, накладення відповідальності на Інтернет-портал було визнане таким, що відповідає статті 10 Європейської конвенції з прав людини.

Водночас у 2019 році Європейський суд з прав людини опублікував рішення у справі «*Høiness v Norway*»[72]. Вона стосувалася розміщення на форумі одного з Інтернет-порталів коментарів користувачів, які заявниця, професійна юристка, сприйняла як сексуальні домагання. Два коментарі були видалені одразу після отримання сповіщення редактором Інтернет-порталу, а третій — за власною ініціативою одного з модераторів. Однак заявниця почала провадження в норвезьких судах щодо стягнення моральної шкоди за дифамацію — та програла в усіх інстанціях. Європейський суд з прав людини також проаналізував цю справу відповідно до критеріїв, сформульованих у своїй попередній практиці у «*Delfi AS v Estonia*». Він відзначив, що сайт, на якому публікувалися коментарі, хоча й був великим новинним сайтом, створеним з метою отримання економічної вигоди, його форум не можна вважати продовженням статей на самому сайті, оскільки обговорення на ньому ініціювалися користувачами мережі. Крім того, самі коментарі, що є предметом розгляду у справі, не становили мови ворожнечі або підбурювання до насильства, а також були видалені або до отримання сповіщення (один з коментарів), або за 13 хвилин після отримання належного сповіщення. З огляду на це, Суд не встановив порушень статті 8 щодо права на повагу до приватного життя заявниці.

Отже, одним із ключових критеріїв є зміст користувацького контенту. Якщо йдеться про мову ворожнечі чи підбурювання до насильства, є підстави застосовувати більш жорсткі стандарти, у тому числі щодо необхідності оперативного видалення контенту з платформи, яку надає посередник.

[72] Høiness v Norway (no. 43624/14) 19 March 2019

Рекомендації щодо відповідальності Інтернет-посередників:

1. *Верховній Раді України та іншим суб'єктам законодавчої ініціативи* — утримуватися від внесення законодавчих ініціатив, що суперечать міжнародним стандартам прав людини та покладають на Інтернет-посередників надмірні обов'язки щодо моніторингу та перевірки користувацького контенту, а також безумовну відповідальність за будь-які коментарі, що розміщуються третіми особами.
2. *Судам та правоохоронним органам* — при визначенні, чи несуть окремі Інтернет-посередники відповідальність за незаконний контент, що був розміщений на їх майданчику користувачами, обов'язково брати до уваги такі критерії та принципи:
    - посередники мають імунітет від користувацького контенту у випадках, коли вони не втручалися в модифікацію такого контенту;
    - режим відповідальності посередників ніколи не може включати вимоги активного моніторингу контенту;
    - посередники не мають обмежувати контент, окрім як за рішенням незалежної та безсторонньої судової установи, яка встановила протиправність контенту, причому таке рішення має включати визначення протиправності контенту в певній юрисдикції, описувати та давати Інтернет-ідентифікатор такого контенту, аналізувати докази на підтримку обґрунтування рішення та, де це застосовно, вказувати на періодичність обмеження;
    - у разі, якщо посередники застосовують позасудовий механізм обмеження доступу до контенту, то вони мають не змістовно оцінювати контент, а повинні направляти обґрунтовані скарги до особи, що створила відповідний контент («*notice-and-notice*»);
    - будь-яке обмеження контенту має бути лімітоване до конкретної одиниці контенту, а для обмеження мають застосовуватися найменш обмежувальні технічні заходи — включно з можливістю обмежувати доступ до контенту в певному географічному регіоні та/або на певний період часу з можливістю періодичного перегляду.