

Віта Володовська,

керівниця напрямку «Цифрові права»
ГО «Лабораторія цифрової безпеки»



Максим Дворовий,

юрист ГО «Лабораторія цифрової безпеки»

ІНТЕРНЕТ-СВОБОДА В УКРАЇНІ 2020

**ДОТРИМАННЯ ПРАВ ЛЮДИНИ
ТА ОСНОВОПОЛОЖНИХ СВОБОД
В ІНТЕРНЕТІ**



За підтримки:

**Американської Асоціації Юристів
Ініціативи з Верховенства Права
(ABA ROLI) в Україні**

ABA
AMERICAN **B**AR ASSOCIATION
Rule of Law Initiative

ЗМІСТ

Вступ	4
Сприятливість середовища для інтернет-свободи	5 - 13
1.1. Законодавча основа	5
1.2. Розроблення регулювання	6
1.3. Регуляторний орган	8
1.4. Ефективні засоби захисту	9
1.5. Захист від кіберзлочинності	10
1.6. Цифрова грамотність	11
РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 12 - 13	
Свобода вираження поглядів	14 - 53
2.1. Доступ до інтернету	14
2.2. Свобода думки, право отримувати та поширювати інформацію	21
2.3. Свобода онлайн-медіа	28
2.4. Законність, легітимність та необхідність обмежень у демократичному суспільстві	34
РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 48 - 53	
Свобода мирних зібрань та об'єднань	54 - 55
3.1. Свобода використовувати інтернет-платформи	54
3.2. Обмеження свободи зібрань та об'єднань в інтернеті	55
РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 55	
Право на повагу до приватного і сімейного життя	56 - 77
4.1. Законодавча основа	56
4.2. Стеження	67
РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 75 - 77	
Дотримання прав людини в діяльності інтернет-посередників 78 - 94	
5.1. Загальні вимоги	78
5.2. Прозорість та підзвітність	81
5.3. Захист свободи вираження поглядів	85
5.4. Захист конфіденційності та захист даних	88
5.5. Доступ до ефективних засобів правового захисту	90
РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 93 - 94	
Національний щорічний звіт	95 - 108
Методологія	96
Перелік міжнародних договорів та рекомендацій у сфері інтернет-свободи	96
Індикатори оцінки	97
Контакти	110

ВСТУП

Світовий, а зараз і український тренд 2010-х років – це суцільна цифровізація. Разом зі здешевленням доступу до Інтернету та зменшенням ціни пристроїв, за допомогою яких можна отримувати блага Всесвітньої мережі, зросла кількість загроз у онлайн-просторі. Там, де з'являються загрози для громадян, дуже часто і дуже швидко виникає і держава, яка прагне ці загрози усунути. Втім, дуже часто такі спроби закінчуються протилежно – і призводять до порушення цифрових прав.

Особливістю Інтернету як середовища реалізації прав людини є також і його неklasичність: окрім взаємовідносин між державою та користувачем, важливою є роль таких гравців, як Інтернет-посередники. Вони у своїй діяльності також можуть порушувати права людини – протиправно передаючи персональні дані третім особам, блокуючи доступ користувачів до сайтів, або ж неналежно видаляючи контент, що містить мову ворожнечі. При цьому, вони часто залишаються недосяжними для держав, адже не знаходяться під їхньою юрисдикцією.

Цей звіт створений задля започаткування традиції щорічного комплексного аналізу стану регулювання трикутника «держава – користувач – Інтернет-посередник» в Україні. Ми спробували окреслити поточне регулювання правовідносин в українській мережі як вихідну точку для подальших досліджень, а також описати основні тренди регулювання протягом 2020 року. Задля цього ми аналізували проекти законодавчих та урядових ініціатив, що публікувалися протягом року, прийняті акти, а також судову практику, та висловили власні рекомендації відповідальним органам – зі сподіванням на імплементацію бодай частини з них у 2021 році.

Висновок за наслідками нашого аналізу дає надію: попри продовження незаконних практик блокувань сайтів, законодавчий спам з новими запропонованими категоріями протиправного контенту, а також низку великих актів, спрямованих на комплексне регулювання певних правовідносин (у сфері медіа, у сфері діяльності спецслужб, у сфері електронних комунікацій тощо), що містять загрози правам людини, у 2020 році вдалося уникнути суттєвого погіршення ситуації. Незважаючи на це, ризики залишаються – а нам залишається сподіватися, що у звіті за 2021 рік не доведеться аналізувати негативний вплив законопроектів, що стали законами.

РОЗДІЛ 1. Сприятливість середовища для інтернет-свободи

1.1. Законодавча основа

Розвиток та поширення інтернету створили безпрецедентні інструменти для реалізації громадянами їхніх прав та свобод, зокрема забезпечили їм можливість 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 Резолюції 38/2018 ¹ Рада ООН з прав людини 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 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), зокрема й у сфері використання мережі «Інтернет». Європейський суд у справі *Ahmet Yildirim v Turkey* 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».**

Відповідно до міжнародних зобов'язань державні органи повинні не лише утримуватися від перешкоджання реалізації прав людини, але й мають створювати належні умови для такої реалізації. Європейський суд з прав людини в рішенні у справі *Editorial Board of Pravoye Delo and Shtekel v Ukraine* ³ 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. Аналогічний обов'язок щодо створення належної нормативно-правової основи для захисту та сприяння реалізації існує і щодо права на повагу до приватного життя та інших основоположних прав.

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 *Ahmet Yildirim and Others v Turkey* App no 3111/10 (ECtHR, 18 December 2012): <http://hudoc.echr.coe.int/eng?i=001-115705>.

³ Справа «Редакція газети "Правое дело та Штекель проти України» (Заява № 33014/05): https://zakon.rada.gov.ua/laws/show/974_807

Чинне національне законодавство практично не містить спеціальних правових норм, спрямованих на захист цифрових прав громадян. На більшість прав та свобод, пов'язаних з інтернетом, поширюються загальні норми конституційного, цивільного, кримінального та адміністративного законодавства. Водночас особливості реалізації прав людини в онлайн-середовищі не завжди належно враховуються у адміністративній та судовій практиці.

1.2. Розроблення регулювання

Міжнародні стандарти вимагають, щоб закони та інші регуляторні акти у сфері інтернету на етапі їх підготовки оцінювалися на предмет можливого впливу на права та основоположні свободи людини.

Закон України «Про Регламент Верховної Ради України»⁴, що регулює законодавчу процедуру, прямо не передбачає обов'язкової оцінки впливу законопроектів, які вносяться на розгляд парламенту, на права людини. Водночас Регламент містить низку процедурних механізмів, які дозволяють її здійснення. Стаття 91 встановлює необхідність обґрунтування у пояснювальній записці до законопроекту правових та інших наслідків застосування закону після його прийняття. Регламент також вимагає здійснення обов'язкової експертизи щодо відповідності законопроектів міжнародно-правовим зобов'язанням України у сфері європейської інтеграції, що на сьогодні охоплює, зокрема, сфери захисту персональних даних, електронних комунікацій та аудіовізуальних медіасервісів. Стаття 103 Регламенту передбачає, що зареєстрований та включений до порядку денного сесії законопроект при підготовці до першого читання в обов'язковому порядку направляється для проведення наукової експертизи, а при підготовці до всіх наступних читань — для проведення юридичної експертизи у відповідні структурні підрозділи Апарату Верховної Ради.

Відсутність окремого фокусу на дотримання прав людини в законопроектній роботі призводить до ухвалення законів, що містять серйозні загрози порушень та звуження обсягу прав людини в онлайн-середовищі. Не сприяє ситуації і відсутність формалізованої ролі Уповноваженого ВРУ з прав людини в законотворчому процесі.

Відповідно до Закону України «Про Уповноваженого Верховної Ради України з прав людини»⁵ Омбудсман здійснює парламентський контроль за дотриманням конституційних прав і свобод людини і громадянина та захист прав кожного на території України і в межах її юрисдикції на постійній основі. Повноваження Омбудсмана охоплюють право вносити в установленому порядку пропозиції щодо вдосконалення законодавства України у сфері захисту прав і свобод людини і громадянина. Регламент Верховної Ради надає Омбудсману гарантоване право на виступ на пленарному засіданні щодо розгляду питань, які стосуються його повноважень. Проте жодних обов'язків стосовно отримання чи надання висновків Омбудсмана до законопроектів щодо дотримання прав людини чинне законодавство не містить.

⁴ Закон України «Про Регламент Верховної Ради України»: <https://zakon.rada.gov.ua/laws/show/1861-17>

⁵ Закон України «Про Уповноваженого Верховної Ради України з прав людини»: <https://zakon.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80#Text>

Ще одним важливим стандартом при розробленні законодавства у сфері інтернету є дотримання принципів інклюзивності (залучення усіх зацікавлених груп) та прозорості.

Чинне законодавство встановлює обов'язковість оприлюднення проєктів нормативно-правових актів — як законопроєктів, так і актів Кабінету Міністрів України, що мають важливе суспільне значення та визначають права й обов'язки громадян України, та проєктів актів інших суб'єктів владних повноважень. Водночас законодавство не містить регламентованих процедур щодо залучення різних зацікавлених сторін до розроблення відповідного регулювання.

Стаття 50 Закону України «Про Кабінет Міністрів України»⁶ встановлює, що до підготовки проєктів актів Кабінету Міністрів України можуть залучатися народні депутати України, науковці та інші фахівці за їх згодою. Закон України «Про комітети Верховної Ради України»⁷ також наділяє парламентські комітети правом створювати робочі групи і призначати їх керівників з-поміж членів комітету для підготовки проєктів актів Верховної Ради України, питань, що обговорюються на засіданнях комітетів, проєктів рішень, рекомендацій, висновків комітетів та включати до складу такої робочої групи, крім членів комітету, інших народних депутатів України, також співробітників науково-дослідних інститутів і навчальних закладів, авторів проєктів законодавчих актів та інших фахівців за їх згодою.

Законодавство не деталізує процедури відбору фахівців до складу таких робочих груп, не гарантує доступу всіх зацікавлених сторін, а також не містить обов'язку щодо розгляду пропозицій до законопроєктів/законів, які вносяться громадянами. Винятком є лише розроблення проєктів регуляторних актів, що стосуються господарської діяльності. Стаття 9 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності»⁸ детально регулює процедуру обговорення проєктів таких актів, зокрема, встановлюючи, що кожен проєкт регуляторного акта оприлюднюється з метою одержання зауважень і пропозицій від фізичних та юридичних осіб, їх об'єднань. При цьому, строк, протягом якого від фізичних та юридичних осіб, їх об'єднань приймаються зауваження та пропозиції, встановлюється розробником проєкту регуляторного акта і не може бути меншим ніж один місяць, а всі зауваження і пропозиції щодо проєкту регуляторного акта та відповідного аналізу регуляторного впливу, одержані протягом встановленого строку, підлягають обов'язковому розгляду розробником цього проєкту. За результатами розгляду розробник проєкту регуляторного акта повністю чи частково враховує одержані зауваження і пропозиції або мотивовано їх відхиляє.

Аналогічний підхід варто було б запровадити і щодо інших актів органів виконавчої влади чи суб'єктів владних повноважень, що мають вплив на реалізацію прав і свобод людини.

⁶ Закон України «Про Кабінет Міністрів України»: <https://zakon.rada.gov.ua/laws/show/794-18#n408>

⁷ Закон України «Про комітети Верховної Ради України»: <https://zakon.rada.gov.ua/laws/show/116/95-%E2%F0#Text>

⁸ Закон України «Про засади державної регуляторної політики у сфері господарської діяльності»: <https://zakon.rada.gov.ua/laws/show/1160-15>

.1.3. Регуляторний орган

Відповідно до міжнародних стандартів, будь-який державний орган, до компетенції якого належать питання, пов'язані з урядуванням інтернету, має здійснювати свою діяльність незалежно від політичного та комерційного впливу, прозора та з дотриманням цілей захисту та просування інтернет-свободи.

В Україні не існує єдиного регуляторного органу у сфері інтернет-урядування. На сьогодні ключовими державними органами в цій сфері є Міністерство цифрової трансформації (Мінцифри) та Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ).

Відповідно до Положення про Міністерство цифрової трансформації⁹ Мінцифри забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до інтернету та телекомунікацій, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку IT-індустрії.

Основними завданнями НКРЗІ є здійснення державного регулювання та нагляду у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом. НКРЗІ здійснює державний нагляд (контроль) за додержанням суб'єктами ринку законодавства про телекомунікації, інформатизацію та поштовий зв'язок, дотриманням операторами, провайдерами телекомунікацій, користувачами радіочастотного ресурсу ліцензійних умов, особливих умов, визначених у відповідних ліцензіях, та Правил здійснення діяльності у сфері телекомунікацій; показників якості надання телекомунікаційних та інформаційно-телекомунікаційних послуг, порядку маршрутизації трафіку на телекомунікаційних та інформаційно-телекомунікаційних мережах та ін.

16 грудня 2020 року Верховна Рада України прийняла проєкт закону України «Про електронні комунікації»¹⁰ з урахуванням частини пропозицій Президента¹¹. Новий закон, що набере чинності 1 січня 2022 року, закріплює низку новел, які поліпшують стан цифрових прав в Україні. Зокрема право на доступ до інтернету як до універсальної послуги, у тексті збережено можливість отримувати комунікаційні послуги анонімно, а також оновлено норми, що сприяють захисту від спаму.

⁹ Положення про Міністерство цифрової трансформації:

<https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919?fbclid=IwAR3ypNvjs8fjr9ZpbqvAfEVlyR4680zuCWUX4m2WgQpjS8K1s3HmK7wEXs>

¹⁰ Закон України «Про електронні комунікації»: <https://zakon.rada.gov.ua/laws/show/1089-IX>

¹¹ Лабораторія цифрової безпеки. Президент ветовав Закон про електронні комунікації:

<https://dslua.org/publications/prezydent-vetuvav-zakon-pro-elektronni-komunikatsii/>

Водночас повноцінна реформа регулювання сфери електронних комунікацій не буде можливою без реформування НКРЗІ, яка на сьогодні не відповідає вимогам незалежності та ефективності. На виконання Україною зобов'язань як сторони Угоди про Асоціацію з ЄС та як учасниці зовнішньополітичної ініціативи «Східне партнерство», народні депутати-члени парламентського комітету з питань цифрової трансформації розробили та зареєстрували у Верховній Раді проєкт закону № 4066 «Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України»¹².

Законопроект покликаний впровадити норми щодо прозорого призначення членів Регулятора комунікаційних послуг на відкритих конкурсних засадах, незалежності Регулятора комунікаційних послуг у прийнятті ним компетентних та справедливих рішень, відкритості та гласності процесу державного регулювання з огляду на Конституцію України та прийняті Конституційним Судом України рішення в частині порядку створення Регулятора комунікаційних послуг, призначення його членів та місця в системі органів влади в Україні.

1.4. Ефективні засоби захисту

Конституція України гарантує кожному право на оскарження в суді рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб, а також право звертатися за захистом своїх прав до Уповноваженого Верховної Ради України з прав людини. Водночас ефективність використання зазначених механізмів не завжди втілюється на практиці.

Згідно зі статтею 15 Закону України «Про Уповноваженого Верховної Ради України з прав людини» у разі виявлення порушення прав і свобод людини, Омбудсман вносить подання Уповноваженого до відповідних органів державної влади, органів місцевого самоврядування, об'єднань громадян, підприємств, установ, організацій незалежно від форми власності, їх посадовим і службовим особам для вжиття відповідних заходів у місячний строк щодо усунення виявлених порушень. За невиконання законних вимог Уповноваженого передбачено адміністративний штраф на суму від 1700 до 3400 грн. Проте процедура притягнення до адміністративної відповідальності досить складна та часто унеможливлює вчасне притягнення винної особи до відповідальності.

З метою посилити інституцію Омбудсмана у квітні 2020 року у Верховній Раді було зареєстровано проєкт закону № 3312 «Про внесення змін до деяких законодавчих актів України щодо Уповноваженого Верховної Ради України з прав людини»¹³. Серед новел законопроекту передбачається чіткий порядок здійснення провадження Уповноваженого за скаргами осіб та у випадках ініціативного реагування Уповноваженого на випадки порушення прав людини і основоположних свобод: вимоги до скарг до Уповноваженого;

¹² Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=69864

¹³ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68542

підстави для відмови у відкритті провадження; визначається, що є зловживанням правом на звернення до Уповноваженого; строки здійснення провадження. Крім того, з метою посилення ефективності діяльності Уповноваженого передбачається, що за результатами провадження, відкритого за індивідуальною скаргою, Уповноважений або представник Уповноваженого можуть внести припис про усунення порушення прав і свобод, який має обов'язковий характер. За невиконання припису Уповноваженого, останній може порушити питання про дисциплінарну відповідальність винної посадової особи.

Законопроект викликав критичні зауваження щодо низки пропонованих положень, проте необхідність посилення інституції Омбудсмана підтримується як авторами законодавчої ініціативи, так і представниками громадянського суспільства та міжнародних інституцій ¹⁴.

Важливість такого позасудового інструменту захисту прав людини є особливо актуальною, зважаючи на тривалість судових проваджень у справах щодо оскарження рішень суб'єктів владних повноважень стосовно порушення цифрових прав громадян. Інструменти судового оскарження порушень цифрових прав часто супроводжуються юридичними та фінансовими бар'єрами, а розгляд судових справ може тривати місяці чи навіть роки. Докладніше ефективність та бар'єри судового захисту свободи вираження поглядів та приватності розглядаються у наступних розділах.

1.5. Захист від кіберзлочинності

Україна ратифікувала Будапештську конвенцію (Конвенцію Ради Європи про кіберзлочинність) ¹⁵ у 2005 році. Цей документ висуває низку вимог до національного права, передбачає криміналізацію низки діянь, а також вимоги до кримінального процесуального права, які мали б забезпечити ефективне розслідування злочинів ¹⁶. Норми матеріального кримінального права були імplementовані до Кримінального кодексу України, де Розділ XVI Особливої частини присвячений злочинам у сфері використання комп'ютерів, систем та комп'ютерних мереж, а також міститься низка статей в інших розділах ¹⁷. У Національній поліції України функціонує департамент кіберполіції, який реалізує державну політику в цій сфері ¹⁸.

Норми кримінального процесуального права, відображені в Будапештській конвенції, не були повністю впроваджені до національного законодавства. Зокрема в рамках кримінального провадження досі не впроваджено можливість використовувати електронні докази.

¹⁴ Законопроект було відкликано у лютому 2021 року. На заміну зареєстровано новий проект закону про внесення змін до деяких законодавчих актів України щодо удосконалення правових засад діяльності Уповноваженого Верховної Ради України з прав людини № 5019: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71010

¹⁵ Закон України про ратифікацію Конвенції про кіберзлочинність: <https://zakon.rada.gov.ua/laws/show/2824-15>

¹⁶ Конвенція про кіберзлочинність: https://zakon.rada.gov.ua/laws/show/994_575

¹⁷ Кримінальний кодекс України: <https://zakon.rada.gov.ua/rada/show/2341-14>

¹⁸ Вебсайт кіберполіції: <https://cyberpolice.gov.ua/>

1 вересня 2020 року до Верховної Ради України було внесено законопроекти № 4003¹⁹ та 4004²⁰. Попри те, що вони пропонують доповнити українське законодавство низкою позитивних новел на кшталт введення такого заходу забезпечення кримінального провадження як термінове збереження інформації, а також запровадження в українське законодавство поняття «електронний доказ», вони містять низку небезпек для прав людини.

Норма щодо доступу правоохоронців до інформації, яка зберігається в електронних інформаційних системах (наприклад, до даних у смартфоні чи персональному комп'ютері), на які не поширюється дозвіл на проведення обшуку, якщо слідчий чи прокурор вирішить, що є достатні підстави вважати, що інформація, яка в них міститься, має значення для встановлення обставин у кримінальному провадженні, надає необмежену дискрецію правоохоронним органам та не передбачає жодних механізмів для захисту особи від порушення її права на таємницю кореспонденції. Також пропонується покласти на провайдерів низку обов'язків щодо збереження інформації в телекомунікаційних системах, зокрема про рух трафіку в обсязі, достатньому для ідентифікації абонента та визначення джерела походження трафіку та маршруту його передачі протягом 12 місяців, а також у порядку вимог щодо тимчасового збереження інформації для цілей кримінального провадження. Така інформація надаватиметься, за загальним правилом, за постановою прокурора або слідчого, що створює ризик того, що доступ до будь-якої інформації про комунікації особи може здійснюватися без дотримання належних гарантій судового нагляду²¹. Ці законопроекти включені до порядку денного Верховної Ради, однак наразі не були прийняті нею.

1.6. Цифрова грамотність

Розвиток цифрової освіти визначено одним із пріоритетних напрямків діяльності Мінцифри. Міністерство поставило за ціль залучити до програм розвитку цифрових навичок 6 млн українців до 2024 року.

Для цього у 2020 році Мінцифри створило 1,5 тис. офлайн-хабів цифрової освіти в різних містах України, а також запустило портал Дія. Цифрова освіта²², на якому можна пройти навчання з цифрової грамотності. У 2020 році на порталі було запущено 40 освітніх «серіалів», які переглянули понад 400 тис. українців. Серед них — курси, спрямовані на розвиток базових цифрових навичок, про медіаграмотність, кібербулінг, безпеку дітей онлайн, захист персональних даних та доступ до публічної інформації, а також курси розвитку підприємництва з використанням онлайн-інструментів.

¹⁹ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770

²⁰ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

²¹ Заява Коаліції «За вільний Інтернет»:

<https://dslua.org/publications/paket-zakonoproektiv-shchodo-protydii-kiberzlochynnosti-ta-posylennia-sanktsiynoho-mekhanizmu-vid-1-veresnia-2020-roku-mistyt-zahrozy-dlia-tsyfrovykh-prav-zaiava-koalitsii-za-vilnyy-internet/>

²² Офіційний портал: <https://osvita.dia.gov.ua/>

Мінцифри запустило перший національний тест на цифрову грамотність — Цифрограм. Станом на кінець листопада 2020 року тест складали понад 50 тисяч українців. Відповіли на всі 90 запитань національного тесту й отримали сертифікат більше ніж 34500 українців (69 % від тих, хто почав тест) ²³.

Водночас імплементація програм цифрових навичок та розвитку медіаграмотності у шкільні навчальні програми поки що не має системного характеру.

РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 1:

ВЕРХОВНІЙ РАДІ УКРАЇНИ:

— посилити роль Уповноваженого Верховної Ради України з прав людини щодо здійснення парламентського контролю за дотриманням прав і свобод людини в законодавчих ініціативах, що виносяться на розгляд парламенту або Кабінету Міністрів України, а також посилити повноваження стосовно реагування на порушення у сфері реалізації прав та свобод людини онлайн, з одночасним забезпеченням гарантій незалежності інституції Омбудсмана.

УПОВНОВАЖЕНОМУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ:

— розробити та впровадити систему моніторингу й оцінки стану забезпечення прав людини в онлайн-середовищі.

ВЕРХОВНІЙ РАДІ УКРАЇНИ, КАБІНЕТУ МІНІСТРІВ УКРАЇНИ:

— забезпечувати процес інклюзивного залучення зацікавлених осіб до підготовки та опрацювання нормативно-правових актів, що зачіпають права та свободи людини в онлайн-середовищі, через впровадження кращих практик оприлюднення проєктів нормативних актів, збирання та опрацювання пропозицій громадськості, інформування про результати розгляду таких пропозицій та ін.

ВЕРХОВНІЙ РАДІ УКРАЇНИ, КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ:

— доопрацювати проєкт закону «Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України» № 4066 та запустити процес реформування НКРЗІ, встановивши гарантії незалежності, прозорості, компетентності та ефективності нагляду у сфері електронних комунікацій.

²³ Перші 50 тис. українців складають тест на цифрову грамотність «Цифрограм»:

<https://thedigital.gov.ua/news/pershi-50000-ukrainsiv-pochali-skladati-natsionalniy-test-na-tsifrovu-gramotnist-tsfrogram>

**МІНІСТЕРСТВУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ
ТА МІНІСТЕРСТВУ ОСВІТИ І НАУКИ УКРАЇНИ:**

— розробляти та послідовно впроваджувати програми з розвитку цифрових навичок в загальну систему шкільної освіти.

**КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ
З ПИТАНЬ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ:**

— доопрацювати проєкт закону «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» № 4003 та проєкт закону «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» № 4004 задля усунення ризиків для прав людини перед їх прийняттям за основу та в цілому.

РОЗДІЛ 2. Свобода вираження поглядів

2.1. Доступ до інтернету

Існує широка дискусія щодо того, чи визнавати право на доступ до інтернету правом людини, а також чи слід найменувати його «правом на інтернет». Право на доступ до інтернету закріплене в низці держав на законодавчому рівні, від Естонії до Франції та Коста-Рики, а необхідність його закріплення визначена в численних документах ООН, ОБСЄ та Ради Європи ²⁴. Рекомендація CM/Rec(2014)6 про керівні вказівки щодо прав людини для інтернет-користувачів наголошує на тому, що доступ до інтернету має надаватися без дискримінації та за доступною ціною, а держава має забезпечувати належний доступ до інтернету в географічно віддалених територіях та вразливим групам; також доступ до інтернету може бути обмежений винятково за рішенням суду ²⁵.

2.1.1. Загальний рівень доступу до інтернету

Право на доступ до інтернету поки що не закріплене в законодавстві України. 16 грудня 2020 року Верховна Рада України після врахування пропозицій Президента України ухвалила в цілому проект закону України «Про електронні комунікації», який додає послугу широкосмислового доступу до інтернету у фіксованому місці, що має надаватися за доступною ціною, до переліку універсальних комунікаційних послуг ²⁶. Вимоги до якості такої послуги мають гарантувати доступ споживачів до широкого переліку сервісів: від соцмереж та месенджерів до інтернет-банкінгу й відеозв'язку — та встановлюватимуться центральним органом виконавчої влади у сферах електронних комунікацій та радіочастотного ресурсу. Відповідне право буде закріплене в українському законодавстві з 1 січня 2022 року.

Інфраструктуру з доступу до інтернету в Україні варто аналізувати з декількох аспектів — як цінової доступності, так і фізичної, тобто покриття ним населення та території України.

Якщо говорити про ціновий аспект, то **Україна посідає високі позиції у рейтингах забезпечення доступу до інтернету та вважається однією з країн з найдешевшим інтернетом у світі**. За даними [cable.co.uk](https://www.cable.co.uk), у 2019 році Україна посіла 5 місце у світі за дешевизною мобільного інтернету з середньою ціною 0.46 \$ за 1 ГБ трафіку ²⁷. За даними сервісу [Picodi](https://www.picodi.com), за підсумками 2019 року Україна має найдешевший домашній оптоволоконний інтернет та одну з найдешевших можливостей під'єднання до швидкісного інтернету зі швидкістю 1 Гбіт/сек — середня ціна такого під'єднання становить 6.19 \$ за місяць ²⁸.

²⁴ Максим Дворовий. Чи будемо ми говорити про право на інтернет в Україні:

<https://detector.media/infospace/article/172446/2019-11-15-chy-budemo-my-govoryty-pro-pravo-na-internet-v-ukraini/>

²⁵ Рекомендація CM/Rec(2014)6: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5b31

²⁶ Закон України «Про електронні комунікації»: <https://zakon.rada.gov.ua/laws/show/1089-IX>

²⁷ Worldwide mobile data pricing: <https://www.cable.co.uk/mobiles/worldwide-data-pricing/>

²⁸ Picodi. Сравнение цен на интернет в мире: <https://www.picodi.com/ua/mozhna-deshevshe/sravnienie-tsen-na-internet-v-mire>

При середній заробітній платі населення України в розмірі 10887 гривень 46 копійок станом на жовтень 2020 року ²⁹ (приблизно 388 \$ за курсом НБУ) ³⁰, такі ціни на під'єднання можна вважати доступними для основної маси населення.

Дещо гіршою є ситуація з покриттям інтернетом території та населення України. Цілеспрямовані виміри покриття широкосмуговим інтернетом донедавна не проводилися, на чому наголошував очільник створеного у 2019 році Міністерства цифрової трансформації України Михайло Федоров ³¹. В інтерв'ю в листопаді 2019 року він вказав на дані від НКРЗІ про покриття 62 % території України швидкісним інтернетом та вказав на мету покриття 90-100 % до кінця 2022 року ³². Проведення такого вимірювання було передбачене як одна з цілей діяльності Мінцифри у 2020 році ³³. У проєкті Національної стратегії розвитку широкосмугового доступу до інтернету, підготовленому Мінцифри, фігурує інформація про покриття 85 % населення України якісним фіксованим ШСД станом на травень 2020 року ³⁴. Сам очільник міністерства визнає, що станом на кінець липня 2020 року понад 17000 населених пунктів не охоплені оптичними мережами жодного оператора, а тому понад 4 мільйони українців мешкають у селах, де немає якісного фіксованого інтернету, в той час як 1,55 мільйона українців проживають у віддалених ділянках населених пунктів, у яких вартість під'єднання перевищує 150 % від середньої ринкової вартості під'єднання ³⁵.

Мінцифри опублікувало інтерактивну карту під'єднання населених пунктів до оптоволоконних мереж, з якої можна побачити, що воно є поширеним лише довкола великих міст, а також у західних областях, на Київщині та Черкащині ³⁶.

²⁹ Пенсійний фонд України. Показник середньої заробітної плати за 2020 рік: <https://www.pfu.gov.ua/2121350-pokaznyk-serednoyi-zarobitnoyi-platy-za-2020-rik/>

³⁰ Національний банк України. Офіційний курс гривні щодо іноземних валют на дату 11.12.2020: <https://bank.gov.ua/ua/markets/exchangerates?date=11.12.2020&period=daily>

³¹ Михайло Федоров. Понад 5,5 мільйонів українців не можуть отримати якісний фіксований інтернет. Українська правда. 30 липня 2020 року: <https://www.pravda.com.ua/columns/2020/07/30/7261199/>

³² Міністр розповів про рівень покриття України інтернетом. Радіо Свобода. 24 листопада 2019 року: <https://www.radiosvoboda.org/a/news-pokryttia-internetom/30289573.html>

³³ План роботи Міністерства цифрової трансформації України на 2020 рік: https://thedigital.gov.ua/storage/uploads/files/page/ministry/План_роботи_Мінцифри_на_2020_рік.pdf

³⁴ Міністерство цифрової трансформації України. Проєкт Національної стратегії розвитку широкосмугового доступу до Інтернету: <https://drive.google.com/file/d/1X9xILClpTaXwcOjRdK9l5Mw2cAlZryuQ/view>

³⁵ Михайло Федоров. Понад 5,5 мільйонів українців не можуть отримати якісний фіксований інтернет. Українська правда. 30 липня 2020 року: <https://www.pravda.com.ua/columns/2020/07/30/7261199/>

³⁶ Міністерство цифрової трансформації України та Комітет цифрової трансформації. Наявність ВОЛЗ у населених пунктах: <https://thedigital.gov.ua/fiber>

На Єдиному державному вебпорталі відкритих даних також доступні результати вимірювань Мінцифри щодо наявності покриття населених пунктів України волоконно-оптичними мережами ³⁷. У тестовому режимі Міністерство запустило сайт broadband.gov.ua ³⁸, який розглядається як державна багатофункціональна платформа, на якій публікуватиметься інформація про розвиток широкосмугового доступу до інтернету, зокрема щодо покриття ³⁹.

У вересні 2020 року Уряд зобов'язав НКРЗІ публікувати в режимі відкритих даних таку категорію даних як «Інформація про покриття інтернету, технології, швидкості та кількість абонентів у розрізі кожного населеного пункту, що надається операторами та провайдерами телекомунікацій у рамках відповіді на запити НКРЗІ» ⁴⁰. Наприкінці 2020 року цей набір даних не був оприлюднений на Єдиному державному вебпорталі відкритих даних ⁴¹.

Що ж до покриття мобільним інтернетом, то три основних мобільних оператори (Vodafone, Київстар та Lifecell), які забезпечують надання послуг мобільного інтернету в стандарті 4G, публікують власні дані про покриття мережею ⁴². За оцінкою представників Київстар, їх мережа 4G станом на листопад 2020 року доступна для 85 % населення України ⁴³. Процес покриття активізувався у 2020 році внаслідок одного з указів Президента України в липні 2019 року ⁴⁴. Розгортання мережі 5G передбачене нормативними актами Президента України ⁴⁵, Кабінету Міністрів України ⁴⁶, в той час проведення тендерів на отримання частотного ресурсу для розгортання мережі планується у грудні 2021 року.

³⁷ Єдиний державний вебпортал відкритих даних. Наявність покриття населених пунктів України волоконно-оптичними мережами: <https://data.gov.ua/dataset/788580dd-e3ae-45b4-a93b-f7f3e8a3f80d>

³⁸ <https://broadband.gov.ua/>

³⁹ Міністерство цифрової трансформації України. Проєкт Національної стратегії розвитку широкосмугового доступу до Інтернету: <https://drive.google.com/file/d/1X9xILClpTaXwcOjRdK9l5Mw2cAlZryuQ/view>

⁴⁰ Постанова Кабінету Міністрів України № 870 від 23 вересня 2020 року «Про внесення змін в додаток до Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних»: <https://zakon.rada.gov.ua/laws/show/870-2020-%D0%BF#n8>

⁴¹ Єдиний державний вебпортал відкритих даних. Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації: <https://data.gov.ua/organization/natsionalna-komisiia-shcho-zdiisniue-derzhavne-rehuliuivannia-u-sferi-zviazku-ta-informatyzatsi>

⁴² Vodafone. Наше покриття: <https://www.vodafone.ua/services/network/coverage-map>. Карта покриття Київстар: <https://kyivstar.ua/uk/mm/mobile-internet/karta-pokrytiya-3g>. Lifecell. Покриття: <https://www.lifecell.ua/uk/mobilnij-internet/pokrittya/>

⁴³ Урядовий портал. Михайло Федоров: 5,4 млн українців отримали кращу якість покриття 4G з липня по листопад 2020 року: <https://www.kmu.gov.ua/news/mihajlo-fedorov-54-mln-ukrayinciv-otrimali-krashchu-yakist-pokrittya-4g-z-lipnya-po-listopad-2020-roku>

⁴⁴ Указ Президента України № 497/2019 від 8 липня 2019 року «Про деякі заходи з покращення доступу до мобільного Інтернету»: <https://www.president.gov.ua/documents/4972019-27953>

⁴⁵ Указ Президента України № 242/19 від 17 травня 2019 року «Про забезпечення умов для впровадження системи рухомого (мобільного) зв'язку п'ятого покоління»: <https://www.president.gov.ua/documents/2422019-26881>

⁴⁶ Розпорядження Кабінету Міністрів України № 1409-р від 11 листопада 2020 року: <https://zakon.rada.gov.ua/laws/show/1409-2020-%D1%80>

2.1.2. Спеціальні заходи забезпечення доступу до інтернету

Україна не має надійного доступу до інтернету через спеціальні точки в місцях надання публічних послуг та навчальних закладах. Михайло Федоров публічно заявляє про існування цифрового розриву між містянами та селянами і визнає цю проблему; він також озвучував інформацію про те, що до якісного оптичного інтернету не під'єднано 40 % шкіл, 92 % бібліотек, 37 % лікарень, здебільшого розміщених у селах та невеликих містах. У контексті пандемії це створює проблеми з організацією дистанційного навчання та впровадження телемедицини⁴⁷. У Плані роботи Міністерства цифрової трансформації на 2020 рік одними з заявлених цілей було під'єднання 90 % шкіл до фіксованого широкосмугового доступу до інтернету належної якості, а також отримання актуальних даних та поступове під'єднання до широкосмугового доступу для закладів медицини та соціальної інфраструктури⁴⁸.

Розв'язання проблем з під'єднанням об'єктів соціальної інфраструктури до широкосмугового доступу до інтернету докладніше окреслюється у вже згаданому проєкті Національної стратегії розвитку широкосмугового доступу до інтернету, який пройшов громадське обговорення у 2020 році та очікує на затвердження. Мінцифри планує, що до кінця 2023 року 95 % закладів соціальної інфраструктури повинні бути забезпечені ШСД зі швидкістю не менше 100 Мбіт/с, причому з можливістю оновлення до 1 Гбіт/с без необхідності закупівлі та/або реорганізації мережевого обладнання. Під'єднання закладів соціальної інфраструктури пропонується проводити у три етапи: до кінця 2021 року 55 % закладів має бути під'єднано, а 80 % сільського населення отримати технічну можливість під'єднатися до широкосмугового доступу до інтернету; до кінця 2022 року ці показники мають зрости до 75 % та 95 % відповідно, а до кінця 2023 року – 95 % та 99 %. Проєктом Стратегії заплановано виділити на це понад 5,5 мільярдів гривень⁴⁹. Водночас у Державному бюджеті на 2021 рік на субвенцію з державного бюджету місцевим бюджетам на реалізацію заходів, спрямованих на підвищення доступності широкосмугового доступу до інтернету в сільській місцевості виділено 500 мільйонів гривень замість 3,3 мільярда гривень, вказаних у проєкті Стратегії⁵⁰, що може підважити зусилля Мінцифри. Також можна очікувати зміни дат виконання планів, зазначених у проєкті Стратегії, через те, що вона досі не затверджена.

Уряд планує робити кроки до поліпшення ситуації та виконання своїх позитивних обов'язків із забезпечення доступу до інтернету вразливим категоріям населення. У проєкті Стратегії пропонується впроваджувати заходи з доступності інтернету для осіб з інвалідністю.

⁴⁷ Михайло Федоров. Понад 5,5 мільйонів українців не можуть отримати якісний фіксований інтернет. Українська правда. 30 липня 2020 року: <https://www.pravda.com.ua/columns/2020/07/30/7261199/>

⁴⁸ План роботи Міністерства цифрової трансформації України на 2020 рік: https://thedigital.gov.ua/storage/uploads/files/page/ministry/План_роботи_Мінцифри_на_2020_рік.pdf

⁴⁹ Міністерство цифрової трансформації України. Проєкт Національної стратегії розвитку широкосмугового доступу до Інтернету: <https://drive.google.com/file/d/1X9xILClpTaXwcOjRdK9l5Mw2cAlZryuQ/view>

⁵⁰ Закон України «Про Державний бюджет України на 2021 рік»: <https://zakon.rada.gov.ua/laws/show/1082-IX>

Щодо фінансової доступності, то Мінцифри вважає, що вартість послуг інтернету в розмірі 5-6 % від місячної пенсії є надмірною та постулює плани про введення державної допомоги для забезпечення доступу до мережі таким категоріям населення, що сукупно складатиме приблизно 240 мільйонів гривень на рік ⁵¹. Згідно з проектом Плану заходів на виконання Стратегії, до кінця 2023 року планується забезпечити осіб з інвалідністю термінальним обладнанням для доступу до мережі, до кінця 2021 року – організувати доступ до сайтів органів державної влади, а до кінця 2022 року – розробити програмне забезпечення для спрощеного доступу до інтернету для цієї категорії населення ⁵².

Нормативні підвалини для здійснення спеціальних заходів забезпечення доступу до інтернету закладає Закон України «Про електронні комунікації» ⁵³. З 1 січня 2022 року в законодавстві з'являться механізми, які дозволять реалізувати положення Стратегії, згадані вище. Ним впроваджується моніторинг вартості доступу до універсальних послуг. Як наслідок, вразливі групи споживачів зможуть отримати адресну цільову допомогу в доступі до якісного інтернету, якщо вартість під'єднання буде для них занадто високою.

Також держава бере на себе обов'язок забезпечити універсальні послуги на певній території, якщо вони відсутні або їх неможливо надати на комерційних умовах. У такому разі Мінцифри проводить конкурс (публічні закупівлі) між постачальниками, щоб забезпечити визначену територію послугами широко-смугового доступу до мережі «Інтернет». Якщо переможця конкурсу не встановлено або жоден постачальник не взяв у ньому участі, регуляторний орган має визначити одного чи кількох постачальників, що мають забезпечити доступ до інтернету. Відмова зі сторони постачальника можлива лише, якщо держава має заборгованість за розгортання комунікаційних мереж такому постачальнику. Розгортання таких мереж також підлягає компенсації з державного бюджету. Порядок її отримання встановить Кабінет Міністрів України.

2.1.3. Правомірність обмеження доступу до інтернету

Україна не має чинного нормативного регулювання, яке б чітко передбачало можливість від'єднання доступу до інтернету, але містить норми, тлумачення яких дозволяє припустити застосування такого заходу.

Закон України «Про правовий режим надзвичайного стану» передбачає можливість застосування особливих правил користування зв'язком та передачі інформації через комп'ютерні мережі під час надзвичайного стану, оголошеного внаслідок терактів, міжнаціональних та міжконфесійних конфліктів, масових безпорядків, або ж задля відновлення конституційного ладу. Ці заходи можуть вводитися указом Президента України на строк до 30 діб, який підлягатиме подальшому затвердженню Верховною Радою України.

⁵¹ Міністерство цифрової трансформації України. Проект Національної стратегії розвитку широко-смугового доступу до Інтернету: <https://drive.google.com/file/d/1X9xILClpTaXwcOjRdK9l5Mw2cAlZryuQ/view>

⁵² Міністерство цифрової трансформації України. Проект Плану заходів з реалізації Національної стратегії розвитку широко-смугового доступу до Інтернету: <https://drive.google.com/file/d/1S9JEEHBnTtY7aSwcS0y1b9OQdDrQPSQy/view>

⁵³ Закон України «Про електронні комунікації»: <https://zakon.rada.gov.ua/laws/show/1089-IX>

Цей строк може бути продовжено не більше ніж на 30 діб за аналогічною процедурою затвердження, а також про них має бути поінформовано світову спільноту через Генерального секретаря ООН відповідно до Міжнародного пакту про громадянські та політичні права ⁵⁴.

Так само Закон України «Про правовий режим воєнного стану» передбачає, що у разі його введення на відповідних територіях військово-командування разом з військовими адміністраціями може забороняти передачу інформації через комп'ютерні мережі. Інформування міжнародної спільноти про ці заходи відбувається у порядку, аналогічному до інформування про обмеження, введені за надзвичайного стану ⁵⁵. Варто пам'ятати, що попри ширшу межу дискреції держави щодо обмеження прав людини за надзвичайного та воєнного стану, а також те, що цифрові права не належать до тих, від яких заборонено відступати, як за міжнародними документами, так і за Конституцією України ⁵⁶, такі обмеження дозволені виключно в тих межах, яких вимагає гострота становища, і за умови, що такі заходи не суперечать іншим її зобов'язанням згідно з міжнародним правом ⁵⁷.

Також чинний Закон України «Про телекомунікації», окрім ситуацій воєнного та надзвичайного стану, передбачає, що обмеження можуть встановлюватися безпосередньо провайдерами за режиму надзвичайної ситуації та надзвичайного стану з метою оповіщення та забезпечення телекомунікаційними послугами учасників ліквідації наслідків надзвичайних ситуацій, відбудовних робіт та здійснення відповідних заходів органами влади — за погодженням з НКРЗІ ⁵⁸.

Прийнятий 16 грудня 2020 року проєкт закону України «Про електронні комунікації» передбачає внесення змін до тексту Закону України «Про боротьбу з тероризмом». Згідно з ним з 1 січня 2022 року в районі проведення антитерористичної операції може здійснюватися тимчасове обмеження надання електронних комунікаційних послуг у порядку, встановленому Кабміном. Закон повторно закріплює можливість встановлення тимчасових обмежень провайдерами в наданні послуг з доступу до інтернету за умов надзвичайного стану та за режиму надзвичайної ситуації, а також за воєнного стану ⁵⁹.

Механізмів судового контролю чи оскарження рішень щодо обмеження доступу до інтернету за воєнного та надзвичайного стану не передбачено. Практики використання наявних норм задля обмеження доступу до інтернету на території України у 2020 році зафіксовано не було. Також слід нагадати, що будь-яке їхнє застосування має суворо відповідати трискладовому тесту обмеження прав людини та передусім бути пропорційним.

⁵⁴ Закон України «Про правовий режим надзвичайного стану»: <https://zakon.rada.gov.ua/laws/show/1550-14>

⁵⁵ Закон України «Про правовий режим воєнного стану»: <https://zakon.rada.gov.ua/laws/show/389-19>

⁵⁶ Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

⁵⁷ Конвенція про захист прав людини і основоположних свобод: https://zakon.rada.gov.ua/laws/show/995_004

⁵⁸ Закон України «Про телекомунікації»: <https://zakon.rada.gov.ua/laws/show/1280-15>

⁵⁹ Закон України «Про електронні комунікації»: <https://zakon.rada.gov.ua/laws/show/1089-IX>

Стосовно обмежень використання інтернету в пенітенціарних закладах, то Кримінально-виконавчий кодекс передбачає право засуджених до позбавлення волі на користування інтернетом під контролем адміністрації у вільний від роботи час їхнім власним коштом або коштом інших осіб шляхом внесення таких коштів на електронний гаманець. Засудженим дозволяється створювати електронну скриньку та користуватися нею під контролем адміністрації; зважаючи на індивідуальні ризики засуджених, адміністрація має право ознайомлюватися зі змістом вхідних та вихідних повідомлень ⁶⁰.

Порядок організації надання засудженим доступу до глобальної мережі «Інтернет» деталізує ці положення та передбачає створення інтернет-класів або ізольованих робочих місць, в окремих випадках дозволяється надавати такі послуги в камерах. Доступ надається за заявою до адміністрації установи та відповідно до графіка роботи інтернет-класу. Відомості про надання засудженим права користуватися інтернетом обліковуються та заносяться до спеціального журналу, як і використання ними ІР-телефонії та відеозв'язку ⁶¹. Передбачається, що під час доступу до мережі засудженим дозволяється відвідувати певний перелік сайтів, визначений адміністрацією установи, який формується відповідно до категорій, затверджених згаданим порядком. Засуджені можуть отримати доступ до сайтів органів державної влади та місцевого самоврядування, міжнародних організацій, творчих, освітніх, спортивних, культурних, юридичних та довідкових сайтів, а також до сайтів зареєстрованих медіа; на запит засудженого адміністрація закладу може надати доступ і до інших сайтів ⁶². На рівні Кодексу заборонено відвідувати вебсайти соціальних мереж, ресурси, що пропагують жорстокість, насильство, еротичного або порнографічного змісту, переглядати матеріали, що можуть негативно вплинути на психічний стан засудженого, реєструватися на будь-яких інших сайтах, окрім дозволених та з метою створення електронної скриньки, а також формувати будь-які бази даних ⁶³.

Важливо згадати, що Порядок передбачає захист таємниці листування засудженого у тому разі, якщо кореспонденція проводиться з Уповноваженим Верховної Ради України з прав людини, Європейським судом з прав людини, судами, а також іншими відповідними органами міжнародних організацій, членом або учасником яких є Україна, уповноваженими особами таких міжнародних організацій, прокурором, захисником у кримінальному провадженні, який здійснює свої повноваження. Це контрастує з необхідністю реєстрації логінів та паролів поштових скриньок засуджених, передбаченою Порядком ⁶⁴.

⁶⁰ Кримінально-виконавчий кодекс України: <https://zakon.rada.gov.ua/laws/show/1129-15>

⁶¹ Порядок організації надання засудженим доступу до глобальної мережі Інтернет, затверджений наказом Міністерства юстиції України № 1280/31148 від 20 жовтня 2017 року: <https://zakon.rada.gov.ua/laws/show/z1280-17>

⁶² Порядок організації надання засудженим доступу до глобальної мережі Інтернет, затверджений наказом Міністерства юстиції України № 1280/31148 від 20 жовтня 2017 року: <https://zakon.rada.gov.ua/laws/show/z1280-17>

⁶³ Кримінально-виконавчий кодекс України: <https://zakon.rada.gov.ua/laws/show/1129-15>

⁶⁴ Порядок організації надання засудженим доступу до глобальної мережі Інтернет, затверджений наказом Міністерства юстиції України № 1280/31148 від 20 жовтня 2017 року: <https://zakon.rada.gov.ua/laws/show/z1280-17>

Обмеження права на доступ до інтернету в місцях позбавлення волі не передбачене. Це означає, що у тому разі, якщо засуджений має належні грошові кошти для отримання доступу до мережі та дотримується усіх зазначених вище умов, адміністрація пенітенціарного закладу не може обмежити його в цьому праві. З огляду на це, законодавство не передбачає спеціального механізму оскарження додаткових обмежень, тож будь-яке рішення, дія чи бездіяльність щодо права на доступ до інтернету засуджених оскаржуватиметься в загальному порядку адміністративного судочинства ⁶⁵.

2.2. Свобода думки, право отримувати та поширювати інформацію

Практика Європейського суду з прав людини говорить, що стаття 10 Конвенції захищає не лише зміст інформації, а й засоби її поширення, оскільки будь-яке обмеження, накладене на такі засоби, призводить до втручання у право отримувати та поширювати інформацію ⁶⁶. З огляду на це, важливо пам'ятати, що блокування сайтів, IP-адрес, портів, мережевих протоколів та окремих сервісів (таких, як соціальні мережі) є надзвичайним заходом, який може бути виправданий лише у разі, якщо він передбачений законом, є необхідним для захисту прав людини або інших законних інтересів, є пропорційним, альтернативні засоби, які б менше втручалися у права, відсутні, а мінімальних гарантій належного процесу дотримано ⁶⁷.

2.2.1. Блокування інтернет-ресурсів

Українське законодавство містить три механізми блокування інтернет-ресурсів. Закон України «Про телекомунікації» передбачає обов'язок провайдерів телекомунікацій на підставі рішення суду обмежувати доступ своїх абонентів до ресурсів, через які здійснюється розповсюдження дитячої порнографії ⁶⁸. Цей механізм можна вважати таким, що відповідає критерію законності, є необхідним і пропорційним, зважаючи на загрозу, яку несе поширення відповідного контенту, позитивом є і те, що механізм судовий. Втім, ця норма втратить чинність з 1 січня 2022 року в разі набрання чинності Законом України «Про електронні комунікації».

Другий механізм закріплено в законодавстві із серпня 2020 року з прийняттям Закону України «Про державне регулювання діяльності щодо організації та проведення азартних ігор» ⁶⁹.

Відповідно до його положень особа, яка організовує, проводить чи надає доступ через вебсайт до азартних ігор без відповідної ліцензії, має протягом трьох днів обмежити до нього доступ на вимогу Комісії з регулювання азартних ігор та лотерей.

⁶⁵ Кодекс адміністративного судочинства України: <https://zakon.rada.gov.ua/laws/show/2747-15>

⁶⁶ Ahmet Yildirim and Others v Turkey App no 3111/10 (ECtHR, 18 December 2012): <http://hudoc.echr.coe.int/eng?i=001-115705>

⁶⁷ OSCE Representative on Freedom of the Media. Joint declaration on freedom of expression and “fake news”, disinformation and propaganda. 3 March 2017: <https://www.osce.org/files/f/documents/6/8/302796.pdf>

⁶⁸ Закон України «Про телекомунікації»: <https://zakon.rada.gov.ua/laws/show/1280-15>

⁶⁹ Закон України «Про державне регулювання діяльності щодо організації та проведення азартних ігор»: <https://zakon.rada.gov.ua/laws/show/768-IX>

Аналогічний обов'язок щодо обмеження доступу до сайту чи вебсторінки передбачено і для провайдера послуг хостингу, на технічних засобах якого розміщений вебсайт або його частина, за допомогою якої надається доступ до азартних ігор без відповідної ліцензії. Порядок обмеження доступу до сайту, передбачений Законом, в частині звернення вимог про блокування до особи, яка здійснює діяльність без ліцензії, може бути припустимим попри позасудовий характер, оскільки не потребує оцінки контенту сайту та ставить вимогу блокування у залежність від дотримання формальних ознак. Проте проблемою є дискреція, надана Комісії для встановлення порядку направлення та виконання вимог, згаданих вище, оскільки не містить достатніх запобіжників від зловживань⁷⁰. Відповідний порядок блокування ще не розроблено Комісією.

Третій механізм передбачено Законом України «Про авторське право і суміжні права»⁷¹. Він може застосовуватися лише у випадку неможливості обмежити доступ до протиправного контенту та полягає у тому, що постачальник послуг хостингу має обмежити доступ до вебсторінки, яка містить матеріал, що порушує авторське право. Механізм, як і вся процедура обмеження доступу до контенту в цьому законі, є позасудовим.

Спроби закріпити більшу кількість механізмів блокування інтернет-ресурсів в українському законодавстві у 2020 році також були. Низка з них пропонується проєктом закону «Про медіа» № 2693-д, який перебуває на розгляді у Верховній Раді України і є доопрацьованим текстом законопроєкту, внесеного у 2019 році⁷². Текст Закону містить таку санкцію щодо онлайн-медіа як заборона поширення на території України. Вона може застосовуватися винятково за рішенням суду, прийнятим відповідно до звернення Нацради та лише у випадку, якщо онлайн-медіа припустилося трьох значних або двох грубих порушень протягом року. Також заборону поширення онлайн-медіа на території України можна застосувати в разі вчинення грубого порушення суб'єктом у сфері онлайн-медіа, особу якого не вдалося встановити, і який не виконав відповідний припис Національної ради.

Законопроєкт також уточнює способи, у які має реалізуватися судове рішення про заборону поширення онлайн-медіа. Наприклад, якщо доменне ім'я вебсайту онлайн-медіа зареєстроване в домені UA. або UKR та ресурси для його розміщення надаються хостером в Україні – забезпечити обмеження доступу до такого ресурсу суд зобов'язуватиме саме реєстратора та постачальника послуг хостингу, а не провайдерів телекомунікацій, які забезпечують доступ користувачів до інтернету.

Проєкт закону «Про медіа» також передбачає можливість Нацради звернутися до суду з вимогою про заборону поширення іноземного аудіовізуального медіа-сервісу на замовлення (наприклад, «Нетфлікс») на території України, якщо таке поширення створює загрозу інтересам забезпечення інформаційної безпеки України.

⁷⁰ Лабораторія цифрової безпеки. В Україні з'явився новий механізм обмеження доступу до сайтів: <https://dslua.org/publications/v-ukraini-z-iavyvsia-novyy-mekhanizm-obmezhenia-dostupu-do-saytiv/>

⁷¹ Закон України «Про авторське право і суміжні права»: <https://zakon.rada.gov.ua/laws/show/3792-12>

⁷² Картка законопроєкту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

Таке обмеження діятиме лише в період збройної агресії і стосуватиметься лише тих суб'єктів, що зареєстровані в державі-агресорі, мають у своїй структурі власності фізичних осіб-громадян або резидентів держави-агресора, юридичних осіб, зареєстрованих там, або медіасервіси яких повністю чи переважно спрямовані на державу-агресора. Заборона поширення іноземного аудіовізуального медіасервісу на замовлення на території України здійснюється, зокрема, шляхом зобов'язання провайдерів (операторів) телекомунікацій обмежити доступ користувачів до відповідних сервісів.

Ще один законопроект, який варто згадати у цьому контексті, — це проект закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України № 3196-д, який фактично викладає Закон «Про Службу безпеки України» в новій редакції⁷³. Згідно з нормами цього проекту СБУ наділяють повноваженнями **здійснювати обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або вчинення розвідувально-підривної діяльності на шкоду Україні, протидії проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації, тих, які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в діяльність об'єктів критичної інформаційної інфраструктури, з використанням технічних засобів, що встановлюються операторами, провайдерами телекомунікацій та іншими суб'єктами господарювання**. Попри те, що пропонується, аби таке блокування відбувалося у судовому порядку, впровадження цієї процедури містить низку ризиків щодо нечіткості закріплених категорій протиправного контенту та гарантій належного судового процесу⁷⁴. Станом на сьогодні, законопроекти 2693-д та 3196-д перебувають на розгляді у Верховній Раді України та не були відхилені, що створює ризик їх подальшого прийняття та імплементації.

Блокування сайтів застосовувалося і на підставі норм законодавства, які не дозволяють говорити про можливість блокування. Так, позасудова процедура блокування відповідно до Закону України «Про санкції», який не містить положень, які б зобов'язували провайдерів обмежувати доступ до контенту, неодноразово критикувалася за її невідповідність критеріям передбачуваності та пропорційності⁷⁵.

⁷³ Картка законопроекту: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243

⁷⁴ Лабораторія цифрової безпеки. Блокування сайтів, масове стеження, фільтрування кандидатів на виборах, або Нові повноваження СБУ: <https://dslua.org/publications/blokuvannia-saytiv-masove-stezhennia-filtruvannia-kandydativ-na-vyborakh-abo-novi-povnovazhennia-sbu/>

⁷⁵ Лабораторія цифрової безпеки. Громадські організації закликають Президента України та РНБО забезпечити законність та прозорість при застосуванні санкцій до Інтернет-ресурсів: <https://dslua.org/publications/hromads-ki-orhanizatsii-zaklykaiut-prezydenta-ukrainy-ta-rnbo-zabezpechyty-zakonnist-ta-prozorst-pry-zastosuvanni-sanktsiy-do-internet-resursiv/>

Ще один спосіб блокування інтернет-ресурсів був винайдений судами та полягає у «накладенні арешту на майнові права інтелектуальної власності, які виникають у користувачів мережі “Інтернет” при використанні вебсайтів». Він також не відповідає критеріям передбачуваності закону та не базується на жодній нормі чинного законодавства ⁷⁶.

Попри широку критику використання описаних вище механізмів для блокування інтернет-ресурсів, ця практика продовжила втілюватися у життя у 2020 році. Зокрема 15 травня 2020 року на 3 роки було продовжено санкції проти російських сервісів «Mail.ru», «Вконтакте» та «Одноклассники», а на 1 рік — проти «Яндексу» ⁷⁷. Залишаються заблокованими й інші сайти, блокування яких було передбачене аналогічними Указами Президента у 2018 ⁷⁸ та 2019 ⁷⁹ роках.

Також у 2020 році продовжилася практика використання арешту майнових прав інтелектуальної власності як заходу, яким фактично встановлюється блокування ⁸⁰. За даними, оприлюдненими НКРЗІ для операторів та провайдерів, у 2020 році прийнято 4 таких рішення ⁸¹. Варто відзначити, що на рівні апеляційних судів у 2020 році прийняті рішення, що визнавали неправомірність таких заходів ⁸². Зокрема, Київський апеляційний суд в ухвалі від 18 листопада 2020 року у справі № 757/45636/20-к, у якій один з провайдерів оскаржував відповідний захід, зазначив, що **«арешт майнових прав інтелектуальної власності, які виникають у користувачів мережі “Інтернет” при використанні вебресурсів, зазначеною нормою КПК України не передбачений»** ⁸³. Одне з медіа, доступ до сайту якого заблоковано ще з 2019 році, — «Enigma» — подало заяву до Європейського суду з прав людини, яка у липні 2020 року була зареєстрована судом у Страсбурзі ⁸⁴.

⁷⁶ Ухвала суду про блокування 17 сайтів суперечить українському законодавству і міжнародному праву — Лабораторія цифрової безпеки: <https://medium.com/@cyberlabukraine/ухвала-суду-про-блокування-19-сайтів-суперечить-українському-законодавству-і-міжнародному-праву-с19b111745ae>

⁷⁷ Указ Президента України № 184/2020 від 14 травня 2020 року «Про рішення Ради національної безпеки і оборони України від 14 травня 2020 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: <https://www.president.gov.ua/documents/1842020-33629>

⁷⁸ Указ Президента України № 126/2018 від 14 травня 2018 року «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)»: <https://www.president.gov.ua/documents/1262018-24150>

⁷⁹ Указ Президента України № 92/2019 від 19 березня 2019 року «Про рішення Ради національної безпеки і оборони України від 19 березня 2019 року «Про застосування, скасування та внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: <https://www.president.gov.ua/documents/822019-26290>

⁸⁰ Ухвала Дніпровського районного суду міста Києва від 30 січня 2020 року у справі № 755/1439/16-к: <https://reyestr.court.gov.ua/Review/87263489>

⁸¹ Новини. Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&language=uk>

⁸² Ухвала Київського апеляційного суду від 5 березня 2020 року у справі № 11-сс/824/1427/2020: <https://reyestr.court.gov.ua/Review/88231731>; Ухвала Київського апеляційного суду від 10 вересня 2020 року у справі № 757/3623/20-к: <https://reyestr.court.gov.ua/Review/91552942>

⁸³ Ухвала Київського апеляційного суду від 18 листопада 2020 року у справі № 757/45636/20-к: <https://reyestr.court.gov.ua/Review/93299672>

⁸⁴ Платформа прав людини. 16 липня 2020 року: <https://www.facebook.com/ppl.org.ua/posts/865518630605983/>

В українській практиці попередніх років також можна згадати спроби Служби безпеки України звернутися до Інтернет асоціації України з проханням обмежити доступ до певних сайтів на території України ⁸⁵, а також діяльність робочої групи при Міністерстві інформаційної політики, яка формувала перелік сайтів, які містять інформацію з ознаками такої, що заборонена до розповсюдження нормами українського законодавства ⁸⁶. Остання велася за незрозумілими критеріями ⁸⁷; повноважень для ведення такої діяльності як для СБУ, так і для Міністерства інформаційної політики в законодавстві закріплено не було. З інформації з відкритих джерел, подібна практика у 2020 році не застосовувалася.

2.2.2. Блокування, фільтрування та видалення онлайн-контенту

Водночас із практикою блокувань інтернет-ресурсів, яка суперечить визнаним стандартам у сфері захисту прав людини, в Україні майже відсутні механізми блокування, фільтрування та видалення онлайн-контенту. Також, на відміну від блокувань інтернет-ресурсів загалом, невідомо про випадки блокування, фільтрування та видалення безпосередньо контенту, а вже згаданий проєкт закону «Про медіа» пропонував закріпити принцип технологічної нейтральності, згідно з яким надання будь-якої переваги одним користувачам у порівнянні з іншими, залежно від змісту послуги, що надається, змісту та обсягу даних, які передаються, кінцевого обладнання користувача чи за іншою ознакою, було б забороненим ⁸⁸.

Єдина норма в законодавстві, яка говорить про це, викладена у статті 52-1 Закону України «Про авторське право та суміжні права» ⁸⁹. Відповідно до її положень, унеможлиблюється доступ лише до протиправного контенту та в рамках позасудової процедури, за якою особа, яка вважає, що її авторські права порушені, спочатку звертається до власника вебсайту щодо видалення контенту, а лише у разі відсутності його реакції — до постачальника хостингу. На видалення контенту надається 48 годин, окрім випадків, коли власник вебсайту може довести, що має права на поширення того чи іншого контенту. Процедура також передбачає можливість відновлення доступу до заблокованого контенту. Загалом ця процедура є належною та відповідає міжнародним стандартам у сфері захисту прав людини.

⁸⁵ СБУ просить заблокувати сайти, які пропагують війну (документ). Лівий берег. 4 серпня 2014 року: https://lb.ua/society/2014/08/04/275122_sbu_prosit_zablokirovat_sayti.html

⁸⁶ Міністерство інформаційної політики України. Перелік сайтів, які містять інформацію з ознаками такої, що заборонена до розповсюдження нормами українського законодавства: <http://mip.gov.ua/documents/116.html>

⁸⁷ Суд відмовив Коаліції «За вільний інтернет» у розкритті критеріїв «незаконності» сайтів. Доступ до правди. 17 жовтня 2019 р.: <https://dostup.pravda.com.ua/news/publications/sud-vidmovyv-koalitsii-za-vilnyi-internet-u-rozkrytti-kryteriiv-sud-vidmovyv-koalitsii-za-vilnyi-internet-u-rozkrytti-kryteriiv-nezakonnosti-saitiv-vid-mininformpolityky>

⁸⁸ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

⁸⁹ Закон України «Про авторське право і суміжні права»: <https://zakon.rada.gov.ua/laws/show/3792-12>

На урядовому рівні у 2020 році обговорювався проєкт Національної стратегії з захисту дітей у цифровому середовищі на період до 2025 року⁹⁰. Його нормами передбачається запровадження фільтрування контенту та сервісів у мережі «Інтернет» у місцях навчання та повсякденного перебування дитини протягом 2021-2024 років. Пропозиція врахувати необхідність пропорційності таких заходів вже у тексті Стратегії для зменшення ризиків⁹¹ була відхилена на стадії громадського обговорення, але все ще може бути втілена на практиці. Проєкт стратегії також передбачає запровадження режиму видалення та блокування матеріалів, що містять сексуальну експлуатацію та насильство над дітьми, відповідно до якого при виявленні контенту, провайдери інтернет-послуг негайно видаляють такий матеріал (якщо хостинг сервера відбувається в межах території України) або за рішенням суду блокують доступ до інтернет-ресурсу на території України, а правоохоронні органи України залучають представників правоохоронних органів країни, на серверах якого відбувається хостинг матеріалу, для його видалення в джерелі. Такий механізм може відповідати стандартам у сфері свободи вираження поглядів у разі його прийняття. Втім, станом на кінець 2020 року, проєкт Стратегії не був прийнятий, тому ці положення також не були реалізовані та не почали втілюватися у життя Міністерством цифрової трансформації України.

2.2.3. Право на оскарження

За вимогами Конституції України, кожному гарантується право на оскарження в суді рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб⁹². Порядок такого оскарження регламентується Кодексом адміністративного судочинства України — тому оскарження блокувань ресурсів, яке відбувається за рішенням або за участі органу державної влади, можливе через адміністративні суди⁹³.

Важкою є ситуація з оскарженням блокувань, які не мають належного підґрунтя в національному законодавстві. Якщо говорити про блокування, що відбуваються в рамках кримінального провадження та застосування заходів забезпечення провадження, то право на його оскарження в апеляційному порядку мають підозрюваний, обвинувачений та треті особи; касація не передбачена⁹⁴. Такими третіми особами, зокрема, є провайдери послуг, за апеляцією яких були скасовані деякі блокування у 2020 році⁹⁵.

⁹⁰ Міністерство цифрової трансформації України. Повідомлення про проведення публічного громадського обговорення проєкту розпорядження Кабінету Міністрів України «Про схвалення Національної стратегії з захисту дітей у цифровому середовищі на період до 2025 року.»:

<https://thedigital.gov.ua/regulations/povidomlennya-pro-provedennya-publichnogo-gromadskogo-obgovorennya-proyektu-rozporядzhennya-kabinetu-ministriv-ukrayini-pro-shvalennya-nacionalnoyi-strategiyi-z-zahistu-ditej-u-cifrovomu-seredovishi-na-period-do-2025-roku>

⁹¹ Лабораторія цифрової безпеки. Захист дітей у цифровому середовищі: що настратегувало Мінцифри: <https://dslua.org/publications/zakhyst-ditej-u-tsyfrovomu-seredovyshchi-shcho-nastratehuvalo-mintsyfy/>

⁹² Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

⁹³ Кодекс адміністративного судочинства України: <https://zakon.rada.gov.ua/laws/show/2747-15>

⁹⁴ Кримінальний процесуальний кодекс України: <https://zakon.rada.gov.ua/laws/show/4651-17>

⁹⁵ Ухвала Київського апеляційного суду від 18 листопада 2020 року у справі № 757/45636/20-к: <https://reyestr.court.gov.ua/Review/93299672>

Щодо оскарження обмежень, накладених відповідно до Закону України «Про санкції», то його норми не передбачають можливості оскарження рішення у суді⁹⁶. Оскільки санкції вводяться Указом Президента України, то оскарженню може підлягати безпосередньо указ. Судова практика є неоднорідною щодо можливості користувачів оскаржити блокування: Верховний Суд у справі щодо правомірності блокувань «Вконтакте» та «Однокласники» вказав, що «права та законні інтереси користувача Указом Президента України від 15.05.2017 № 133/2017 не порушено»⁹⁷. У пізнішому рішенні щодо правомірності блокувань сервісів «Яндекс» Велика Палата Верховного Суду не була такою категоричною та визнала, що «уведені в дію Указом санкції обмежують право на доступ, зокрема, до певних інтернет-ресурсів, що може розглядатися як втручання у гарантовану статтею 10 Конвенції свободу одержувати й передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів», що може імпліцитно свідчити про визнання можливості користувачів оспорювати блокування відповідно до практики Європейського суду з прав людини у справі *Ahmet Yildirim v Turkey*⁹⁸.

Попри наявність формальних механізмів для оскарження блокувань, залишається сумнівною їхня ефективність та те, наскільки їх можна вважати дієвими засобами правового захисту в розумінні статті 13 Європейської конвенції про права людини⁹⁹. Однією з причин може бути підстава для блокувань, адже питання, пов'язані з національною безпекою, часто розглядаються судами без належного аналізу правових позицій сторін та мають недосконалу мотивувальну частину. Варто згадати і про загальний контекст недовіри до судів¹⁰⁰, спричинений корупційними ризиками, зокрема до Окружного адміністративного суду міста Києва, який уповноважений розглядати більшість справ щодо оскарження актів центральних органів державної влади, розташованих у місті Києві¹⁰¹.

2.2.4. Прозорість обмежень

Питання прозорості обмежень контенту в інтернеті в Україні є неоднозначним. З одного боку, наявні механізми блокування інтернет-ресурсів та видалення контенту, які можна було б назвати правомірними, не містять чітких вимог щодо інформування громадськості про блокування тих чи інших ресурсів. Рішення суду доводиться до відома сторін у справах та підлягає публікації у Єдиному державному реєстрі судових рішень¹⁰². Проте єдиний каталог заблокованих сайтів відсутній.

⁹⁶ Закон України «Про санкції»: <https://zakon.rada.gov.ua/laws/show/1644-18>

⁹⁷ Постанова Верховного Суду від 13 квітня 2018 року у справі № 800/198/17: <https://reyestr.court.gov.ua/Review/73397535>

⁹⁸ *Ahmet Yildirim and Others v Turkey* App no 3111/10 (ECtHR, 18 December 2012): <http://hudoc.echr.coe.int/eng?i=001-115705>

⁹⁹ Конвенція про захист прав людини та основоположних свобод: https://zakon.rada.gov.ua/laws/show/995_004

¹⁰⁰ 76 % українців не довіряють судовій системі. ZMINA. 21 лютого 2020 року: <https://zmina.info/news/76-ukrayincziv-ne-doviryut-sudovij-systemi/>

¹⁰¹ Центр політико-правових реформ. Реорганізація адміністративного суду Києва – питання національної безпеки України: <https://pravo.org.ua/ua/news/judiciary/20874581-reorganizatsiya-administrativnogo-sudu-kieva-pitannya-natsionalnoyi-bezpeki-ukrayini>

¹⁰² Закон України «Про доступ до судових рішень»: <https://zakon.rada.gov.ua/laws/show/3262-15>

Якщо розглядати неправомірні заходи з блокування інтернет-ресурсів, такі, як впровадження санкцій та використання механізмів кримінального провадження, то прозорість цих обмежень не викликає сумнівів. Укази Президента про введення санкцій були належно опубліковані на сайті голови держави¹⁰³. НКРЗІ також висвітлювало на своєму сайті резолютивні частини рішення судів щодо арешту майнових прав інтелектуальної власності, які виникають у користувачів мережі «Інтернет» при використанні вебресурсів, в яких зазначалося про можливість їх оскарження¹⁰⁴.

Різноманітні практики стосовно прозорості запроваджують провайдери, що надають послуги інтернету. На прикладі блокування сайту «Enigma» можна побачити, що різні провайдери при переході на сторінку видання надавали різну інформацію — від таблички «немає з'єднання з сайтом» до того, що сайт заблоковано за рішенням суду та посилань на згадані вище президентські укази¹⁰⁵. Уніфікованих вимог щодо повідомлення про блокування сайту чинне законодавство не містить.

2.3. Свобода онлайн-медіа

2.3.1. Свобода діяльності

Онлайн-медіа в Україні не зобов'язані отримувати спеціальний дозвіл чи ліцензію для здійснення своєї діяльності онлайн чи ведення блогів (крім реєстрації підприємницької діяльності, якщо необхідно).

Проект закону «Про медіа» № 2693-д пропонує запровадити добровільну реєстрацію онлайн-медіа як суб'єктів у сфері медіа та врегулювати їхній статус¹⁰⁶.

Відповідно до законопроекту ознаками онлайн-медіа є регулярне поширення масової інформації, використання для цього окремого сайту чи сторінки на платформах спільного доступу до інформації (наприклад, ютуб-канал) з індивідуальною назвою та наявністю редакційного контролю.

¹⁰³ Указ Президента України № 184/2020 від 14 травня 2020 року «Про рішення Ради національної безпеки і оборони України від 14 травня 2020 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: <https://www.president.gov.ua/documents/1842020-33629>; Указ Президента України № 126/2018 від 14 травня 2018 року «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)»: <https://www.president.gov.ua/documents/1262018-24150>; Указ Президента України № 92/2019 від 19 березня 2019 року «Про рішення Ради національної безпеки і оборони України від 19 березня 2019 року «Про застосування, скасування та внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: <https://www.president.gov.ua/documents/822019-26290>.

¹⁰⁴ Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації. До уваги операторів, провайдерів телекомунікацій!: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2000&language=uk>; Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації. До уваги операторів, провайдерів телекомунікацій!: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1935&language=uk>; Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації. До уваги операторів, провайдерів телекомунікацій: інформація щодо ухвали слідчого судді Печерського районного суду м. Києва: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1903&language=uk>.

¹⁰⁵ Безпрецедентний наступ на свободу слова в Україні. Заблоковано десятки сайтів. Enigma. 30 липня 2019 року: <https://enigma.ua/articles/bezpretsedentniy-nastup-na-svobodu-slova-v-ukraini-zablokovano-desyatki-nezaleznykh-saytiv>

¹⁰⁶ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

Таке визначення частково відображає підхід Ради Європи, сформульований у Рекомендації CM/Rec(2011)7 про нове визначення медіа ¹⁰⁷, однак потребує подальшого уточнення. Відповідно до законопроекту детальніші критерії та процедури віднесення того чи іншого ресурсу до онлайн-медіа мають бути розроблені органом спільного регулювання, тобто безпосередньо представниками медіа та Національної ради.

Реєстрація онлайн-медіа може давати певні переваги суб'єктам у сфері медіа та їхнім журналістам. Зокрема, законопроект № 2693-д передбачає, що винятково зареєстровані медіа можуть отримувати державну підтримку, а також укладати договори про висвітлення діяльності державних органів та органів місцевого самоврядування. Журналістам зареєстрованих медіа гарантується акредитація в органах влади (заборонено відмовляти в акредитації). Крім цього, зареєстровані онлайн-медіа отримують право брати участь у механізмах співрегулювання, що передбачає не лише участь у розробленні правил та кодексів, але і додаткові гарантії захисту при розгляді справ щодо можливого порушення законодавства — звернення за експертизою до органу спільного регулювання.

Водночас відсутність реєстрації онлайн-медіа не може бути перешкодою для їхньої діяльності.

2.3.2. Гарантії журналістської діяльності

Європейський суд з прав людини у своєму рішенні у справі Editorial Board of Pravoye Delo and Shtekel v Ukraine ¹⁰⁸ ще у 2011 році звернув увагу на недостатність у національному законодавстві належних гарантій для журналістів, які використовують інформацію, отриману з інтернету (п. 66). Зокрема, ЄСПЛ зауважив, що українське законодавство, зокрема Закон України «Про друковані засоби масової інформації (пресу) в Україні», надає журналістам імунітет від цивільної відповідальності за дослівне відтворення матеріалу, опублікованого у пресі. Проте відповідно до позиції національних судів такий імунітет журналістів не поширюється на відтворення матеріалу з інтернет-джерел, які не зареєстровані згідно із Законом України «Про друковані засоби масової інформації (пресу) в Україні». У зв'язку з цим ЄСПЛ зауважив, що на той час не існувало національних нормативних актів стосовно державної реєстрації інтернет-видань і що, як стверджував Уряд, Закон України «Про друковані засоби масової інформації (пресу) в Україні» та інші нормативні акти, які регулюють сферу засобів масової інформації в Україні, не містили будь-яких положень про статус інтернет-видань або використання інформації, отриманої з інтернету.

¹⁰⁷ YRecommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media: <https://www.osce.org/files/f/documents/1/f/101403.pdf>

¹⁰⁸ Справа «Редакція газети "Правое дело" та Штекель проти України» (Заява № 33014/05): https://zakon.rada.gov.ua/laws/show/974_807

ЄСПЛ відзначив, що інтернет як інформаційний і комунікаційний інструмент дуже відрізняється від друкованих засобів масової інформації, особливо у тому, що стосується здатності зберігати та передавати інформацію. Електронна мережа, яка обслуговує мільярди користувачів у всьому світі, не є і потенційно не буде об'єктом такого ж регулювання та засобів контролю. Ризик завдання шкоди здійсненню та використанню прав людини і свобод, зокрема права на повагу до приватного життя, який становлять інформація з інтернету та комунікація в ньому, є безумовно вищим, ніж ризик, який походить від преси. Отже, підходи, що регулюють відтворення матеріалу з друкованих засобів масової інформації та інтернету, можуть відрізнятися. Останній, безперечно, має коригуватися з урахуванням притаманних цій технології рис для того, щоб забезпечити захист зазначених прав і свобод та сприяння їм. Однак, беручи до уваги роль, яку відіграє інтернет у контексті професійної діяльності засобів масової інформації, та його важливість для загального здійснення права на свободу вираження поглядів, ЄСПЛ відзначив, що відсутність на національному рівні достатньої законодавчої бази, яка б дозволяла журналістам використовувати отриману з інтернету інформацію без страху наразитися на санкції, серйозно перешкоджає пресі бути «сторожовим псом суспільства».

На думку ЄСПЛ, повне виключення такої інформації зі сфери застосування законодавчих гарантій журналістських свобод може саме по собі спричинити непропорційне втручання у свободу преси, гарантовану статтею 10 Конвенції.

З моменту ухвалення рішення ЄСПЛ, національне законодавство не зазнало суттєвих змін. Більшість гарантій журналістської діяльності досі містяться у законодавстві, що регулює діяльність друкованих та аудіовізуальних медіа.

Водночас низка гарантій свободи вираження поглядів містяться в Законі України «Про інформацію» та поширюються на будь-яку особу, яка реалізує право на інформацію¹⁰⁹. Це стосується, зокрема, права на доступ і поширення інформації з обмеженим доступом, якщо вона є предметом суспільного інтересу, звільнення від відповідальності за оцінювальні судження та ін. Крім цього, статус журналіста може підтверджуватися не лише посвідченням, виданим відповідним медіа, але і посвідченням члена професійної чи творчої спілки журналістів. Хоча в цілому застосування гарантій аудіовізуальних та друкованих медіа до онлайн-медіа залишається проблематичним.

Законопроект № 2693-д «Про медіа», що був зареєстрований у липні 2020 року пропонує вдосконалити та увідповіднити європейським стандартам підстави щодо звільнення журналістів від відповідальності за розповсюдження недостовірної чи незаконної інформації, якщо вони діють добросовісно та з дотриманням етичних стандартів¹¹⁰. Такі норми поширюватимуться на усі типи медіа.

¹⁰⁹ Закон України «Про інформацію»: <https://zakon.rada.gov.ua/laws/show/2657-12>

¹¹⁰ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

2.3.3. Редакційна незалежність

Конституція України та національне законодавство забороняють цензуру та втручання у редакційну політику засобів масової інформації ¹¹¹. Водночас на практиці журналісти та редакції медіа досить часто стають об'єктами тиску з боку окремих нинішніх та колишніх посадових осіб державних органів.

У 2020 році такий тиск досить часто набував форми судових позовів до редакцій, зокрема, програм журналістських розслідувань з вимогами спростування чи видалення інформації та відшкодування моральної шкоди. У листопаді 2020 року правозахисні організації поширили заяву щодо загроз свободі вираження поглядів через невідповідність міжнародним стандартам захисту прав людини національної судової практики ¹¹².

Правозахисники відзначили почастищення випадків судових рішень, відповідно до яких журналісти-розслідувачі повинні спростувати інформацію про доведені в журналістських розслідуваннях факти. Наприклад, у справах проти команди журналістів програми «Наші гроші з Денисом Бігусом» за позовами фігурантів їхніх розслідувань — колишнього високопосадовця Сергія Семочка ¹¹³ та сім'ї Гладковських ¹¹⁴ — суд зобов'язав спростувати «оціночні судження», які ґрунтуються на показах свідків та офіційних документах, усупереч практиці Європейського суду з прав людини. Суд також забороняє ¹¹⁵ поширювати імена фігурантів гучних кримінальних справ, пов'язаних з корупцією, попри пряму норму закону про суспільний інтерес, який переважає в такому разі.

У заяві також згадується позасудова практика блокування сайтів та вебресурсів, зокрема у справах проти платформи Enigma, informantor.news, сайту «Кореспондент» та інших щодо накладення «арешту на майнові права інтелектуальної власності, які виникають у користувачів мережі “Інтернет” при використанні вебресурсів» ¹¹⁶.

¹¹¹ Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

¹¹² Низка судових рішень становить загрозу свободі слова — правозахисники. Інститут масової інформації. 19 листопада 2020 року: <https://imi.org.ua/news/nyzka-sudovyh-rishen-nesut-zagrozu-svobodi-slova-pravozahysnyky-i36306>

¹¹³ Семочко не зміг спростувати ні російські паспорти, ні багатомільйонне майно — але виграв суд, відірвавшись від родичів. Бігус.інфо. 12 листопада 2020 року: <https://bihus.info/semochko-ne-zmig-sprostuvaly-ani-rosijski-pasporty-ani-bagatomilijonne-majno-ale-vygrav-sud-vidrikshys-vid-rodyny/>

¹¹⁴ Скандал з Гладковським та Укроборонпромом: суд назвав розслідування неправдивим. BBC. 8 липня 2020 року: <https://www.bbc.com/ukrainian/features-53341299>

¹¹⁵ Безіменні Мартиненки та Труханови: Верховний суд проти поширення імен фігурантів резонансних справ. Центр протидії корупції. 13 листопада 2019 року: <https://antac.org.ua/news/bezimenni-martynenky-ta-trukhanovy-verkhovnyy-sud-proty-poshyrennia-imen-fihurantiv-rezonansnykh-sprav/>

¹¹⁶ Апеляційний суд підтримав блокування 17 українських сайтів, яке правозахисники назвали незаконним. ZMINA. 25 листопада 2019 року: <https://zmina.info/news/apelyacziyniy-sud-pidtrymav-blokuvannya-17-ukrayinskykh-sajtiv-yake-pravozahysnyky-nazyvaly-nezakonnym/>

Суд не пояснює, який контент на цих вебресурсах безпосередньо порушує «права інтелектуальної власності», про яке майно йдеться та як у користувачів мережі «Інтернет» воно набувається. Подібна практика створює ситуацію правової невизначеності, за якої журналістам загрожують серйозні судові позови, незалежно від законності поширеної ними інформації та дотримання вимог законодавства та професійної етики.

2.3.4. Захист від погроз і тиску

Українські медіа та журналісти часто стають жертвами кібератак та погроз онлайн. Розслідування таких випадків переважно затягнуті та неефективні, що створює атмосферу безкарності та сприяє вчиненню нових порушень.

Інститут масової інформації у 2020 році зафіксував дев'ять кіберзлочинів, про які стало відомо публічно. Найпоширенішими були DDoS-атаки — сім випадків¹¹⁷. Кібератак зазнавали як регіональні, так і національні медіа — «РІА Мелітополь», Politerno (Тернопіль), «Четверта влада» (Рівне) та Liga.net¹¹⁸, а також «Голос Карпат» (Закарпаття)¹¹⁹ та ін.

Журналісти онлайн-видань та проєктів журналістських розслідувань також нерідко стають об'єктами кібератак. За результатами моніторингу інцидентів у сфері цифрової безпеки, з якими стикаються українські журналісти та громадські активісти, що проводиться Лабораторією цифрової безпеки, лише з січня по червень 2020 року було зафіксовано понад 40 випадків цифрових атак¹²⁰. Найпоширенішими формами є фішинг (33,3 % випадків), скидання паролів (16,6 %), повторне використання паролів (13,3 %), перехоплення SMS для зламу месенджерів (6,6 %) ¹²¹.

Окремо слід зауважити, що згідно з анонімним опитуванням¹²², проведеним Інститутом масової інформації у 2020 році, 88 % українських медійників стикалися з інтернет-тиском.

¹¹⁷ Ірина Земляна. Кібержесть. Як журналістів переслідують в інтернеті. Інститут масової інформації. 25 лютого 2021 року: <https://imi.org.ua/monitorings/kiberzhest-yak-zhurnalistiv-peresliduyut-v-interneti-i37803>

¹¹⁸ Інститут масової інформації. Барометр свободи слова за жовтень 2020 року: <https://imi.org.ua/monitorings/barometr-svobody-slova-za-zhovten-2020-roku-i36006>

¹¹⁹ Закарпатський інформаційний сайт зазнав DDoS-атаки. Інститут масової інформації. 16 листопада 2020 року: <https://imi.org.ua/news/zakarpatskyj-informatsijnyj-sajt-zaznav-ddos-ataky-i36222>

¹²⁰ Лабораторія цифрової безпеки. Цифрові загрози для громадських активістів та журналістів: <https://dslua.org/publications/tsyvrovi-zahrozy-dlia-hromads-kykh-aktyvistiv-ta-zhurnalistiv-cherven-2020/>

¹²¹ Інститут масової інформації. Найпоширеніші цифрові атаки на журналістів у 2020-му: <https://imi.org.ua/monitorings/najposhyrenishi-tsyvrovi-ataky-na-zhurnalistiv-u-2020-i36844>

¹²² Переважна більшість українських журналістів стикалася з кібербулінгом — дослідження ІМІ: <https://imi.org.ua/news/perevazhna-bilshist-ukrains-kykh-zhurnalistiv-stykalysia-z-kiberbulinhom-doslidzhennia-imi-i29180>

І 87 % тих, хто піддавався кібербулінгу, пов'язують це зі своєю професійною діяльністю. Погрози та кібербулінг найчастіше набували форми цькування у соціальних мережах ¹²³, а також поширення образливих та сексистських коментарів ¹²⁴.

У жовтні 2020 року журналістка Любов Величко публічно звернулася до Національної поліції щодо погроз, які вона почала отримувати після розслідування про нелегальні казино, у якому фігурує компанія дружини заступника начальника слідчого управління Національної поліції, що було оприлюднене в онлайн-медіа ¹²⁵. У листопаді 2020 року до журналістки було також подано позов про захист честі, гідності та ділової репутації з вимогою спростувати недостовірну інформацію та виплатити моральну шкоду в розмірі 1 млн грн. ¹²⁶. Раніше за погрози журналістці Любов Величко, які вона почала отримувати після виходу її розслідування про російські телеграм-канали в онлайн-виданні Texty, було відкрите кримінальне провадження, розслідування по якому триває ¹²⁷.

За даними Інституту масової інформації, у 2020 році до судів з обвинувальним актом було передано лише дев'ять кримінальних проваджень: шість за статтею 171 Кримінального кодексу України («Перешкодження законній професійній діяльності журналістів») та три за статтею 345-1 ККУ («Погроза або насильство щодо журналіста»). А відповідно до реєстру судових рішень, українські суди у 2020 році ухвалили лише чотири вироки за перешкодження: три обвинувальних і один виправдувальний. Лише один вирок стосувався подій, які відбулися у 2020 році, всі інші — випадків попередніх років. Щодо статті 345-1 ККУ, то реєстр судових рішень містить лише два судових вироки за цією статтею. Водночас жоден з них не стосується подій 2020 року ¹²⁸.

¹²³ Запорізького журналіста цькують у Фейсбуці за новини про коронавірус. Інститут масової інформації. 10 листопада 2020 року: <https://imi.org.ua/news/u-zaporizhzh-zhurnalista-tskuyut-u-fejsbutsi-za-novyny-pro-koronavirus-i36114>

¹²⁴ Журналістка сайту 061.ua стала об'єктом кібербулінгу. Інститут масової інформації. 30 жовтня 2020 року: <https://imi.org.ua/news/zhurnalistka-sajtu-061-ua-stala-ob-yektom-kiberbulingu-i35959>

¹²⁵ Журналістка Любов Величко повідомила, що отримує погрози після розслідування про нелегальні казино. Інститут масової інформації. 28 жовтня 2020 року: <https://imi.org.ua/news/zhurnalistka-lyubov-velychko-povidomyla-shho-otrymuje-pogrozy-pislya-rozsliduvannya-pro-nelegalni-i35903>

¹²⁶ Суд призначив на 9 лютого розгляд справи за позовом Альони Шевцової на 1 млн проти журналістки Величко. Інститут масової інформації. 23 грудня 2020 року: <https://imi.org.ua/news/sud-pryznachyv-na-9-lyutogo-rozglyad-spravy-za-pozovom-alony-shevtsovoyi-na-1-mln-proty-i36839>

¹²⁷ У МВС повідомили, що шукають особу, яка погрозувала журналістці Любові Величко. Інститут масової інформації. 28 вересня 2020 року: <https://imi.org.ua/news/u-mvs-povidomyly-shho-shukayut-osobu-yaka-pogrozhuvala-zhurnalisttsi-lyubovi-velychko-i35202>

¹²⁸ Алі Сафаров. Погрози й насильство щодо журналістів: яке покарання отримують нападники. 5 листопада 2020 року: <https://imi.org.ua/monitorings/pogrozy-i-nasyllia-shhodo-zhurnalistiv-yake-pokarannya-otrymuyut-napadnyky-i36038>

2.4. Законність, легітимність та необхідність обмежень у демократичному суспільстві

2.4.1. Загальні принципи обмежень

Стаття 34 Конституції України гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір ¹²⁹. Ці гарантії поширюються як на реалізацію свободи вираження поглядів у фізичному світі, так і в онлайн-середовищі.

При цьому здійснення свободи вираження поглядів може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Конституція не містить безпосереднього посилання на критерій необхідності такого обмеження у демократичному суспільстві. Проте, така вимога є обов'язковою відповідно до Закону України “Про виконання рішень та застосування практики Європейського суду з прав людини”, який у статті 17 визначає, що суди застосовують Конвенцію про захист прав людини та основоположних свобод та практику ЄСПЛ як джерело права ¹³⁰.

Чинне законодавство не містить спеціальних заборон щодо реалізації свободи вираження поглядів онлайн. На отримання та розповсюдження інформації в інтернеті можуть поширюватися загальні обмеження, що здійснюються для захисту національної безпеки, прав інших людей та в інших легітимних інтересах, визначених конституцією України.

2.4.2. Свобода вираження поглядів та захист національної безпеки, територіальної цілісності, громадської безпеки, запобігання розголошенню конфіденційної інформації

Захист національної безпеки, територіальної цілісності, громадської безпеки, а також запобігання заворушенням чи злочинам є легітимними цілями обмеження свободи вираження поглядів відповідно до вимог статті 10 Європейської конвенції з прав людини ¹³¹ та статті 34 Конституції України ¹³². Варто зазначити, що чинне законодавство України не містить спеціальних норм, які б стосувалися обмежень на поширення інформації для різноманітних суб'єктів, що реалізують своє право на свободу вираження поглядів у мережі.

¹²⁹ Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

¹³⁰ Закон України «Про виконання рішень та застосування практики Європейського суду з прав людини»: <https://zakon.rada.gov.ua/laws/show/3477-15>

¹³¹ Конвенція про захист прав людини та основоположних свобод: https://zakon.rada.gov.ua/laws/show/995_004

¹³² Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

Загальна норма Закону України «Про інформацію» містить заборону на поширення закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини ¹³³, проте не містить механізмів притягнення до відповідальності за її порушення, хоча і відбиває потребу держави захищати згадані суспільні інтереси. Подібною є і норма Закону України «Про інформаційні агентства» ¹³⁴, яка, з огляду на відсутність регулювання онлайн-медіа в Україні, є застосовною до значної кількості онлайн-видань, зареєстрованих як інформаційні агентства, — та подібною вона є і щодо відсутності механізмів реалізації Закону на практиці.

У таких умовах варто звернути увагу на положення Кримінального кодексу України ¹³⁵, які можуть застосовуватися до осіб, що поширюють певну інформацію, зокрема в інтернеті. **Відповідними нормами та санкціями за їх порушення є:**

- **ст. 109** (публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади — до 3 років позбавлення волі, а у разі використання засобів масової інформації — до 5 років);
- **ст. 110** (публічні заклики чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України та порушення порядку, встановленого Конституцією України, — до 5 років позбавлення волі, а у разі, якщо вони призвели до загибелі людей чи інших тяжких наслідків, — аж до довічного позбавлення волі);
- **ст. 161** (умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, образа почуттів громадян у зв'язку з їхніми релігійними переконаннями — до 3 років позбавлення волі, а у разі, якщо вони поєднані з насильством, — до 5 років, якщо призвели до тяжких наслідків — до 8 років);
- **ст. 258-2** (публічні заклики до вчинення терористичного акту — до 3 років позбавлення волі, а у разі використання засобів масової інформації — до 5 років);
- **ст. 295** (публічні заклики до погромів, підпалів, знищення майна, захоплення будівель чи споруд, насильницького виселення громадян, що загрожують громадському порядку, — до 3 років обмеження волі);
- **ст. 436** (публічні заклики до агресивної війни або до розв'язування воєнного конфлікту — до 3 років позбавлення волі);

¹³³ Закон України «Про інформацію»: <https://zakon.rada.gov.ua/laws/show/2657-12>

¹³⁴ Закон України «Про інформаційні агентства»: <https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80>

¹³⁵ Кримінальний кодекс України: <https://zakon.rada.gov.ua/rada/show/2341-14>

- **ст. 436-1** (публічне використання символіки комуністичного, націонал-соціалістичного (нацистського) тоталітарних режимів — до 5 років позбавлення волі, а у разі використання засобів масової інформації — до 10 років позбавлення волі);
- **ст. 442** (публічні заклики до геноциду — до 5 років позбавлення волі).

Більшість цих норм сформульована з достатньою чіткістю та містить адекватні санкції, зважаючи на важливість інтересу, який захищається державою внаслідок застосування цих норм. Винятком є норма статті 436-1 Кримінального кодексу, надмірність санкцій в якій щодо ув'язнення за вираження поглядів, що не призводить до насильства, визнала Венеціанська комісія у своєму висновку в 2015 році ¹³⁶. Спроби адаптувати цю норму до стандартів пропорційності не були втілені в життя минулим складом парламенту ¹³⁷. Втім, пропорційність застосування санкцій має визначатися у кожній окремій справі.

Як впливає з аналізу Єдиного державного реєстру судових рішень, протягом 2020 року винесено 41 вирок за згаданими вище статтями щодо поширення контенту в інтернеті. З цих вироків 2 — виправдувальні, і лише у 2 випадках осіб було засуджено до позбавлення волі, причому одну особу — в рамках провадження *in absentia*. Це означає, що до безпосередньої відповідальності за контент у мережі було притягнуто лише одну особу. Підставою для цього став заклик у фейсбуці до захоплення Чугуївської міської ради, інших місцевих рад, а також спонукання до об'єднання з Російською Федерацією, за що особу засудили до одного року позбавлення волі ¹³⁸. З огляду на практику Європейського суду з прав людини, а саме рішення у справі *Smajic v Bosnia and Herzegovina* ¹³⁹, таке покарання можна вважати пропорційним.

Зі статистичної точки зору можна зробити висновок про те, що загалом застосування відповідних норм Кримінального кодексу не створює надмірних обмежень для вільних дискусій у цифровому просторі. Хоча відсутність осіб, які несуть реальне покарання за зловживання своїм правом на свободу вираження поглядів в інтернеті, є позитивним фактором, варто звернути увагу на негативні тенденції в рамках судової практики за відповідними нормами кримінального права, що вперше були окреслені в дослідженні Платформи прав людини у 2019 році ¹⁴⁰.

¹³⁶ Venice Commission. Joint Interim Opinion on the Law of Ukraine on the condemnation of the communist and national socialist (Nazi) regimes, and prohibition of propaganda of their symbols. 18 December 2015: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2015\)041-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)041-e)

¹³⁷ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_12pf3511=59178

¹³⁸ Вирок Дергачівського районного суду Харківської області від 18 червня 2020 року у справі № 619/946/20: <https://opendatabot.ua/court/89903668-9661b19343cfe620a3e58db3cec17b78>

¹³⁹ *Smajic v Bosnia and Herzegovina* (dec) App no 48657/17 (ECtHR, 16 January 2018): <http://hudoc.echr.coe.int/eng?i=001-180956>

¹⁴⁰ Л. Опришко, В. Володовська, М. Дворовий. Свобода слова в Інтернеті: законодавчі ініціативи та практика розгляду кримінальних справ в Україні в 2014-2018 роках: https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf

Стаття ККУ	Кількість вироків (тут і далі в дужках – сукупність злочинів)	Кількість угод про визнання винуватості	Кількість інших випадків звільнення від відбування покарання	Кількість випадків позбавлення волі	Виправдувальні вирoki
109	14 (4)	12 (4)	1	1	-
110	24 (4)	17 (3)	7 (1)	-	2
161	1 (1)	1 (1)	-	-	-
258-2	-	-	-	-	-
295	-	-	-	-	-
436	2 (1)	-	1 (1)	1 (in absentia)	-
436-1	3 (1)	2	1 (1)	-	-
442	-	-	-	-	-

Суди все ще відмовляються від самостійного аналізу висловлювань, які є предметом розгляду, найчастіше зупиняючи власну аргументацію на дублюванні висновків експертів до вироків. Яскравим прикладом протилежного підходу є рішення Октябрського районного суду в Полтаві від 7 серпня 2020 року, де аналіз змісту коментарів призвів до постановлення виправдувального вироку на підставі того, що «інкриміновані ОСОБА_1 висловлювання не містять фактичних даних, а є особистісними оціночними судженнями, думками та переконаннями, у сатиричній формі, з застосуванням мовних засобів щодо подій, які відбуваються в державі, де він проживає та громадянином якої являється»¹⁴¹.

Також суди не аналізують, наскільки контент, за який особу притягують до відповідальності, впливав на інших користувачів мережі, що мали можливість з ним ознайомитися. На відміну від цитованого дослідження, в жодному з аналізованих вироків суди не звернули увагу на кількість друзів чи підписників у тій чи іншій соціальній мережі, а також не робили розрізнення щодо того, чи це був власний допис чи репост іншого допису. Варто нагадати, що відповідно до практики Європейського суду з прав людини у справі Savva Terentyev v Russia, «**потенційний вплив висловлювання, зробленого онлайн для незначної кількості читачів, є відмінним від впливу висловлювання, опублікованого на мейнстрімних або часто відвідуваних вебсторінках**»¹⁴². Така ситуація з неналежною мотивацією судових рішень, хоча й не спричиняє непропорційних покарань, але суттєво обмежує можливості для оскарження вироків та не відповідає стандартам права на справедливий судовий захист, гарантованого на міжнародно-правовому та конституційному рівнях.

¹⁴¹ Вирок Октябрського районного суду міста Полтави від 7 серпня 2020 року у справі № 554/1848/19: <https://opendatabot.ua/court/90823974-c169b42f8e0543b35d612ce3782c77cd>

¹⁴² 3Savva Terentyev v Russia App no 10692/09 (ECtHR, 28 August 2018): <http://hudoc.echr.coe.int/eng?i=001-185307>

Насамкінець, варто звернути увагу на ще один аспект неоднозначності застосування цих норм кримінального права. Статті 109 та 110 Кримінального кодексу містять таку обтяжувальну обставину як використання засобів масової інформації, що збільшує потенційне покарання за поширення закликів до насильницької зміни чи повалення конституційного ладу або ж змін меж території України. Окремі суди стверджують, що таким засобом масової інформації є «аудіовізуальний (електронний) засіб масової інформації — всесвітня мережа “Інтернет”». Яскравим прикладом неоднomanітності тлумачення цієї обставини є рішення Хмельницького міськрайонного суду Хмельницької області, в якому особу притягнули до відповідальності за два пости у фейсбуці за статтями 109 та 110 Кримінального кодексу: щодо статті 109 його дії були кваліфіковані з врахуванням обтяжуючої обставини, а щодо статті 110 — ні ¹⁴³. Попри те, що у справі було затверджено угоду про визнання вини, а тому кваліфікація не мала фактичного впливу на засудженого, таке тлумачення є потенційно небезпечним. Варто нагадати, що інтернет є лише платформою, за допомогою якої особи реалізують власне право на свободу вираження поглядів, а тому поширення окремих висловів лише за його допомогою не може ставати підставою для застосування жорсткіших заходів відповідальності.

Протягом 2020 року народні депутати України також робили окремі спроби закріпити нові склади злочинів, які були б спрямовані на захист інтересів територіальної цілісності та національної безпеки, — від криміналізації заперечення Голодомору та геноциду кримських татар ¹⁴⁴ до криміналізації публічного заперечення окупації частини території України ¹⁴⁵. Втім, жоден із законопроектів не прийняли, а станом на лютий 2021 року вони були зняті з розгляду. Серед актуальних законопроектів можна відзначити проєкт закону про внесення змін до деяких законодавчих актів України щодо запобігання героїзації військових злочинців та легалізації нацизму (№ 2797) ¹⁴⁶, що спрямований на деталізацію положень декомунізаційних законів та їх поширення на заперечення Голокосту, однак без змін надмірних санкцій. Проєкт закону про узгодження із Конституцією України положень статті 161 Кримінального кодексу України щодо забезпечення рівноправності громадян (№ 3111) ¹⁴⁷ розширює перелік підстав для розпалювання ворожнечі, за які можна притягувати до відповідальності. Обидва законопроекти в цілому відповідають міжнародним стандартам у сфері прав людини, зважаючи на заборони в рамках статті 20 МПГПП ¹⁴⁸ та практики Європейського суду з прав людини у сфері заперечення Голокосту, що не захищається Конвенцією ¹⁴⁹.

¹⁴³ Вирок Хмельницького міськрайонного суду Хмельницької області від 6 листопада 2020 року у справі № 686/22028/20: <https://opendatabot.ua/court/92761683-b96a746f7c50c9b44cbfc950fb13722c>

¹⁴⁴ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69917

¹⁴⁵ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69919

¹⁴⁶ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=67974

¹⁴⁷ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=68214

¹⁴⁸ Міжнародний пакт про громадянські та політичні права: https://zakon.rada.gov.ua/laws/show/995_043

¹⁴⁹ *Williamson v Germany* (dec) App no 64496/17 (ECtHR, 8 January 2019): <http://hudoc.echr.coe.int/eng?i=001-189777>

Окремо варто згадати проєкт закону «Про медіа», який містить низку категорій забороненого контенту, що поширюватимуться і на онлайн-медіа ¹⁵⁰. За їх недотримання онлайн-медіа може загрозовувати штраф у розмірі від 1 до 5 мінімальних заробітних плат, а також заборона розповсюдження. Серед нових категорій забороненого для поширення в онлайн контенту варто відзначити «недостовірні матеріали щодо збройної агресії та діянь держави-агресора (держави-окупанта), її посадових осіб, осіб та організацій, що контролюються державою-агресором (державою-окупантом), у разі, якщо наслідком цього є розпалювання ворожнечі та ненависті або заклики до насильницької зміни територіальної цілісності чи конституційного ладу».

Що ж до втручання у свободу вираження поглядів задля запобігання поширенню конфіденційної інформації, то притягнення до відповідальності за розповсюдження охоронюваних законом таємниць міститься у Кримінальному кодексі України та створює можливість для потенційно протиправних дій зі сторони осіб, що хочуть змусити критиків замовкнути під прикриттям, наприклад, захисту державної таємниці. Так, стаття 232 Кримінального кодексу передбачає відповідальність за розголошення комерційної чи банківської таємниці в розмірі до 3000 НМДГ, а стаття 328 — відповідальність за розголошення державної таємниці (позбавлення волі до 5 років, а якщо розголошення спричинило тяжкі наслідки — до 8 років) ¹⁵¹.

Втім, за даними Єдиного державного реєстру судових рішень, жодного вироку щодо поширення такої інформації в інтернеті протягом 2020 року винесено не було. Відсутність втручань до свободи вираження поглядів в інтернеті на підставі необхідності захисту конфіденційної інформації поза контекстом відмов надання доступу до публічної інформації також зафіксована моніторингами порушень цифрових прав, що проводиться Платформою прав людини ¹⁵².

2.4.3. Свобода вираження поглядів та охорона здоров'я чи моралі

Законодавство України в цілому не встановлює надмірних обмежень свободи вираження поглядів, що були б пов'язані з інтересами охорони здоров'я чи моралі. Водночас застосування наявних обмежень в окремих випадках може суперечити принципам пропорційності та необхідності в демократичному суспільстві.

Закон України «Про захист суспільної моралі» ¹⁵³ встановлює досить широкі категорії контенту, виробництво та розповсюдження якого забороняється. Зокрема ідеться про продукцію, яка:

- **має порнографічний характер;**

¹⁵⁰ Картка законопроєкту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

¹⁵¹ Кримінальний кодекс України: <https://zakon.rada.gov.ua/rada/show/2341-14>

¹⁵² Платформа прав людини. Моніторинг цифрових прав: <https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav>

¹⁵³ Закон України «Про захист суспільної моралі»: <https://zakon.rada.gov.ua/laws/show/1296-15>

- **пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України;**
- **пропагує фашизм та неофашизм;**
- **принижує або ображає націю чи особистість за національною ознакою;**
- **пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святинь;**
- **принижує особистість, є проявом знущання з приводу фізичних вад (каліцтва), з душевнохворих, літніх людей;**
- **пропагує невігластво, неповагу до батьків;**
- **пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички.**

Водночас закон не встановлює відповідальності за поширення такої інформації онлайн, крім випадків, коли ідеться про кримінальні правопорушення. Зокрема щодо заборони дитячої порнографії.

У 2020 році захист прав дітей в онлайн-сфері став одним з пріоритетних напрямків створення політик для Міністерства цифрової трансформації України. Протягом 2020 року Міністерство розробило проєкт Національної стратегії з захисту дітей у цифровому середовищі на період до 2025 року ¹⁵⁴. Проєкт пройшов громадське обговорення, однак не був прийнятий урядом. Проте він став основою для подальших напрацювань міністерства в цій сфері вже на початку 2021 року ¹⁵⁵. Стратегія загалом передбачала якісний виклад проблематики, пов'язаної з боротьбою з сексуальною експлуатацією та насильством над дітьми в онлайні. Однак були зауваження, що стосувалися позасудового обмеження доступу до такого контенту, а також недостатнього залучення громадськості до розроблення галузевих стандартів відповідальності у цій сфері ¹⁵⁶.

¹⁵⁴ Міністерство цифрової трансформації. Мінцифра ініціює громадське обговорення проєкту Національної Стратегії з захисту дітей у цифровому середовищі на період до 2025 року:
<https://thedigital.gov.ua/news/mincifra-iniciyuye-gromadske-obgovorenniya-proyektu-nacionalnoyi-strategiyi-z-zahistu-ditej-u-ci-frovomu-seredovishi-na-period-do-2025-roku>

¹⁵⁵ Міністерство цифрової трансформації. Мінцифра запрошує до громадського обговорення концепції та плану заходів з розвитку цифрових прав дітей:
<https://thedigital.gov.ua/news/mintsifra-zaproshue-do-gromadskogo-obgovorenniya-kontseptsii-ta-planu-zakhodiv-z-rozvitku-tsifrovikh-prav-ditey>

¹⁵⁶ Лабораторія цифрової безпеки. Захист дітей у цифровому середовищі: що настратегувало Мінцифру:
<https://dslua.org/publications/zakhyst-ditey-u-tsyfrovomu-seredovyshchi-shcho-nastratehuvalo-mintsyfyry/>

У жовтні 2020 року Мінцифри презентували словник термінів з онлайн-безпеки, у якому пояснювалася низка термінів у сфері захисту дітей онлайн (діпфейк, жертводорікання, порнопомста тощо) ¹⁵⁷. У продовження цієї тематики, міністерство за допомогою партнерських організацій провело декілька досліджень щодо криміналізації порнопомсти ¹⁵⁸ в українському законодавстві, що можуть стати підґрунтям для криміналізації такої діяльності в майбутньому.

У 2020 році Верховна Рада України ухвалила у першому читанні проєкт закону № 3055 «Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції)» ¹⁵⁹. Законопроєкт запропонував криміналізувати низку діянь, пов'язаних із сексуальною експлуатацією та насильством в онлайні, зокрема домагання дитини в онлайні, втягнення її в участь у заходах сексуального характеру та їхній публічний показ тощо ¹⁶⁰.

У 2020 році, у зв'язку з поширенням Covid-19 в Україні та введенням карантинних заходів, стало актуальним питання пошуку балансу між інтересами свободи вираження поглядів та охороною здоров'я, зокрема у зв'язку з оприлюдненням у соціальних мережах неправдивої інформації та теорій змови щодо походження вірусу, статистики захворюваності, методів лікування тощо. Це призвело до безпрецедентної кількості випадків притягнення користувачів інтернету до адміністративної відповідальності за поширювання неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку (стаття 173-1 Кодексу України про адміністративні правопорушення) ¹⁶¹.

За 2020 рік до Єдиного державного реєстру судових рішень внесено понад 3700 постанов у справах щодо поширювання неправдивих чуток, переважна більшість яких стосується розгляду справ стосовно розповсюдження інформації в інтернеті, зокрема в соціальній мережі «Фейсбук». Попри те, що санкція за порушення є незначною — може тягнути за собою штраф від 170 до 255 грн або виправні роботи на строк до одного місяця з відрахуванням 20 % заробітку, — практика притягнення до відповідальності за поширення публікацій в інтернеті, зокрема соціальних мережах, викликає стурбованість.

¹⁵⁷ Міністерство цифрової трансформації. Від діпфейку до фішингу. Мінцифра розпочинає освітню кампанію з тлумачення термінів онлайн-безпеки:

<https://thedigital.gov.ua/news/vid-dipfeyku-do-fishingu-mintsifra-rozpochinae-osvitnyu-kampaniyu-z-tlumachennya-terminiv-onlayn-bezpeki>

¹⁵⁸ Максим Дворовий. Відповідальність за порнопомсту: міжнародний досвід, підхід технологічних компаній та українські реалії. Лабораторія цифрової безпеки:

<https://dslua.org/publications/vidpovidalnist-za-pornopomstu-mizhnarodnyy-dosvid-pidkhid-tekhnologichnykh-kompaniy-ta-ukrainski-realii/>

¹⁵⁹ Картка законопроєкту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68122

¹⁶⁰ Закон було ухвалено 18 лютого 2021 року: <https://zakon.rada.gov.ua/laws/show/1256-IX#Text>

¹⁶¹ Кодекс України про адміністративні правопорушення: <https://zakon.rada.gov.ua/rada/show/80731-10>

Аналіз ГО «Платформа прав людини»¹⁶² засвідчив суперечливість судової практики у категорії справ, що можуть призводити до необґрунтованого обмеження свободи вираження поглядів онлайн. Правозахисники, зокрема, відзначили такі проблеми, як недостатнє вивчення судами обставин справи, неналежну оцінку доказів неправдивості поширеної інформації та існування потенційної можливості спричинення паніки чи порушення громадського порядку внаслідок її поширення; використання листів СБУ як доказів вини особи; неоднакову оцінку одних й тих самих обставин різними судами, що зрештою призводить до кардинально протилежних висновків та рішень в ідентичних ситуаціях; визнання особи винуватою у вчиненні правопорушення на підставі неналежної або недостатньої доказової бази; нехтування стандартами статті 10 Європейської Конвенції про захист прав людини й основоположних свобод та ін.

2.4.4. Свобода вираження поглядів та захист репутації чи прав інших осіб

Українське законодавство не передбачає кримінальної відповідальності за дифамацію. Періодично до парламенту подаються ініціативи, спрямовані на повернення криміналізації наклепу¹⁶³, однак у 2020 році таких законопроектів зареєстровано не було.

У разі поширення недостовірної інформації про особу чи образливих суджень, особа може звернутися до суду щодо захисту своєї честі, гідності або ділової репутації в порядку цивільного судочинства, а підприємці — також у порядку, визначеному Господарським кодексом України.

З метою забезпечення правильного й однакового застосування судами законодавства, що регулює захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи Пленум Верховного Суду України ще у 2009 році підготував роз'яснення, які в цілому відповідають вимогам Конвенції про захист прав людини та основоположних свобод та практиці Європейського суду з прав людини¹⁶⁴. Однак постанова не враховує особливостей поширення інформації в інтернеті.

Аналіз судової практики про захист честі, гідності та ділової репутації, проведений ГО «Платформа прав людини» дозволив виявити низку проблем, що виникають при застосуванні судами норм законодавства та можуть призвести до необґрунтованого обмеження свободи вираження поглядів в онлайн-середовищі.

¹⁶² Судова практика у справах про поширення інформації в інтернеті: тенденції та проблеми правозастосовної практики / Бурмагін О.О., Опришко Л.В. — Київ: ГО «Платформа прав людини», 2020 р.

¹⁶³ Коаліція «За вільний Інтернет» просить нардепів відкликати законопроект про криміналізацію наклепу: <https://detector.media/infospace/article/142739/2018-11-21-koalitsiya-za-vilnyy-internet-prosytt-nardepiv-vidklykaty-zakonoproekt-pro-kryminalizatsiyu-naklepu/>

¹⁶⁴ Постанова Пленуму Верховного Суду України № 1 від 27 лютого 2009 року «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи»: https://zakon.rada.gov.ua/laws/show/v_001700-09

Експерти виявили поширення практики одночасного застосування вимог щодо спростування недостовірної інформації та її видалення. Занепокоєння викликає відсутність належного обґрунтування як щодо поєднання цих способів, так і стосовно пропорційності застосування такого засобу правового захисту як видалення в цілому, адже вилучення усієї публікації може бути надмірним та вести до цензури¹⁶⁵.

Ще одним суперечливим способом судового захисту є покладення на відповідача обов'язку оприлюднити текст рішення суду¹⁶⁶. У деяких випадках це призводить до того, що обсяг спростування суттєво перевищує обсяг відповідної спірної інформації. Крім цього, зобов'язання оприлюднити фотокопію рішення суду здатне спричинити вимушене порушення відповідачем вимог законодавства щодо захисту конфіденційної інформації про особу, адже текст рішення може містити персональні дані сторін.

Іншим небезпечним підходом судів є зобов'язання оприлюднити текст спростування шляхом розміщення між заголовком та першим абзацом спірної публікації. На думку експертів, це призводить до необґрунтованого втручання у авторські права — суд фактично вносить зміни у твір, спотворюючи його, і тим самим порушує особисті немайнові права автора на збереження цілісності твору, гарантовані статтею 14 Закону України «Про авторське право і суміжні права» та іншими міжнародними правовими актами¹⁶⁷.

Варто також зауважити, що чинне цивільне законодавство встановлює скорочений строк позовної давності в один рік для вимог про спростування недостовірної інформації, поміщеної у засобах масової інформації. Водночас жодних обмежень щодо заявлення вимог про відшкодування моральної шкоди, заподіяної поширенням недостовірної інформації, Цивільний кодекс України не містить, чим можуть скористатися недобросовісні позивачі.

Власне подання позовів про захист честі, гідності та ділової репутації все ще залишається інструментом тиску на журналістів з боку чинних та колишніх високопосадовців¹⁶⁸.

Зважаючи на виявлені колізії та недоліки в судовій практиці, доцільно переглянути чинне законодавство з метою чіткішого врегулювання питання захисту честі, гідності та репутації, з дотриманням балансу щодо свободи вираження поглядів в інтернеті. Певні спроби в цьому напрямку були здійснені у проєкті закону «Про медіа» № 2693-д, що був зареєстрований у Верховній Раді України 2 липня 2020 року і зараз очікує на розгляд¹⁶⁹.

¹⁶⁵ Судова практика у справах про поширення інформації в інтернеті: тенденції та проблеми правозастосовної практики / Бурмагін О.О., Опришко Л.В. — Київ: ГО «Платформа прав людини», 2020 р. — стор. 25-26.

¹⁶⁶ Судова практика у справах про поширення інформації в інтернеті: тенденції та проблеми правозастосовної практики / Бурмагін О.О., Опришко Л.В. — Київ: ГО «Платформа прав людини», 2020 р. — стор. 30.

¹⁶⁷ Судова практика у справах про поширення інформації в інтернеті: тенденції та проблеми правозастосовної практики / Бурмагін О.О., Опришко Л.В. — Київ: ГО «Платформа прав людини», 2020 р. — стор. 29.

¹⁶⁸ Див. п. 2.3.3.

¹⁶⁹ Картка законопроєкту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

У документі пропонується врегулювати порядок розгляду заяв про право на відповідь чи спростування у разі поширення недостовірної інформації про особу в онлайн-медіа. Поширення тексту спростування або відповіді в онлайн-медіа має відбуватись у спосіб, максимально наближений до способу поширення інформації, щодо якої надійшла заява про спростування або реалізацію права на відповідь (у тому самому обсязі, на тій самій вебсторінці або у тому самому розділі вебсайту тощо). Якщо текст спростування або відповіді неможливо розмістити на одній вебсторінці з оригінальною публікацією, суб'єкт у сфері онлайн-медіа має забезпечити перехресні посилання між відповідними публікаціями та розмістити поряд з оригінальним текстом повідомлення про те, що інформація з цієї публікації була спростована або стала предметом реалізації права на відповідь. Суб'єкт у сфері онлайн-медіа зобов'язаний розглянути заяву та повідомити заявника про прийняте ним рішення невідкладно, але не пізніше п'яти робочих днів з дня отримання заяви.

При цьому законопроект встановлює низку підстав, за яких редакція онлайн-медіа може обґрунтовано відмовити в поширенні спростування та відповіді. Наприклад, якщо розповсюджена інформація є оцінними судженнями або наявні достатні докази того, що інформація відповідає дійсності, повно та точно відображає факти, про які йдеться; якщо поширена інформація є дослівним відтворенням публічних виступів або повідомлень, публічної інформації державних органів, органів місцевого самоврядування, їхніх посадових і службових осіб; якщо поширена інформація є дослівним відтворенням матеріалів, розповсюджених іншим зареєстрованим медіа або медіа, щодо якого не існує вимог обов'язкової реєстрації, за наявності інформації про осіб, що здійснюють редакційний контроль, їхнє місцезнаходження та актуальні контакти та з посиланням на таке медіа; якщо поширена інформація стосується незначної фактичної помилки, яка не завдає шкоди правам і законним інтересам заявника.

Для захисту прав інших осіб Кримінальний кодекс України встановлює відповідальність за розпалювання національної, расової чи релігійної ворожнечі та ненависті, приниження національної честі та гідності, образи почуттів громадян у зв'язку з їхніми релігійними переконаннями, а також пряме чи непряме обмеження прав чи встановлення прямих чи непрямих привілеїв громадян за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, інвалідності, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками (стаття 161 ККУ). За такі дії може застосовуватися покарання у формі позбавлення волі на строк до трьох років, а у разі спричинення тяжких наслідків — до восьми років ¹⁷⁰.

Кримінальна відповідальність передбачена також за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (стаття 163 ККУ). Покарання у формі позбавлення волі на строк до семи років може застосовуватись у разі, якщо такі дії вчинені щодо державних чи громадських діячів, журналістів або при цьому використовувалися спеціальні засоби для негласного зняття інформації.

¹⁷⁰ Кримінальний кодекс України: <https://zakon.rada.gov.ua/rada/show/2341-14>

Кримінальний кодекс України також встановлює кримінальну відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу. У випадку, якщо такі дії заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, покарання може сягати позбавлення волі на строк до 5 років.

Втім судова практика за цими статтями є поодиноким. У 2020 році винесено лише 8 вироків, тільки один з яких стосувався оцінювання та встановлення балансу між свободою вираження поглядів в онлайн-середовищі та захистом прав інших осіб. Коростишівський районний суд Житомирської області визнав винною особу в поширенні дискримінаційних висловлювань, а також у розповсюдженні матеріалів із закликами до насильницької зміни та повалення конституційного ладу, до захоплення державної влади в соціальній мережі ¹⁷¹. При цьому останнє прокуратура кваліфікувала як вчинене повторно, з використанням засобів масової інформації (частина третя статті 109 ККУ). Оскільки суд фактично затвердив угоду про визнання винуватості між прокурором та обвинуваченим, жодної оцінки щодо того, чи справді поширені висловлювання загрожують легітимним інтересам, а застосована санкція у формі позбавлення волі на 3 роки з іспитовим строком в 1 рік є необхідною в демократичному суспільстві, не здійснено.

Варто відзначити, що у 2020 році склалася нова небезпечна судова практика, що може призвести до зростання тиску на журналістів через зловживання з боку фігурантів їхніх розслідувань шляхом оприлюднення персональних даних журналістів та працівників редакцій.

Так, у листопаді 2019 року колишній депутат та посадовець Адміністрації президента Віктора Януковича Андрій Портнов виклав ¹⁷² у своєму телеграм-каналі персональні дані водіїв (паспортні дані, домашня адреса, номери авто та ін.) знімальної групи проєкту журналістських розслідувань «Схеми» у відповідь на журналістське розслідування щодо впливу та можливих зв'язків Портнова з чинною владою. Адвокати редакції звернулися з цивільними позовами до суду з вимогою припинити поширення персональних даних водіїв програми «Схеми». У серпні 2020 року здійснено підпал автомобіля одного із водіїв «Схем» Бориса Мазура.

31 серпня суддя Печерського районного суду міста Києва Світлана Волкова без запрошення сторін винесла рішення, яким відмовила водію «Схем» Борису Мазуру в задоволенні позову про захист права на приватність та прохання зобов'язати Андрія Портнова вилучити з публічного простору його персональні дані. Окрім відмови у задоволенні позову, суддя також постановила стягнути з водія «Схем» витрати Портнова на адвокатів у розмірі 52 500 гривень. У грудні 2020 року це рішення залишив без змін Апеляційний суд міста Києва ¹⁷³.

¹⁷¹ Вирок Коростишівського районного суду Житомирської області від 11 червня 2020 року у справі № 935/1251/20: <https://reyestr.court.gov.ua/Review/89742100>

¹⁷² Поліція взялася за дописи Портнова про журналістів «Радіо Свобода». Українська правда. 7 листопада 2019 року: <https://www.pravda.com.ua/news/2019/11/7/7231236/>

¹⁷³ Апеляційний суд став на сторону Портнова, який оприлюднив персональні дані членів команди редакції «Схем». Радіо Свобода. 14 грудня 2020 року: <https://www.radiosvoboda.org/a/news-schemes-portnov-apeliatsiya/31000535.html>

Небезпека цього судового рішення полягає у тому, що суд фактично визнав допустимість поширення конфіденційних персональних даних будь-якої особи як способу захисту своїх прав, попри вимоги Конституції та законів України. Крім цього, зобов'язання відшкодувати значну суму витрат на правовий захист ексчиновника на практиці може мати «охолоджувальний ефект» та призвести до цензури, адже створює серйозні перешкоди для звернення журналістами за захистом своїх прав до суду. На момент написання цього звіту у справі подано касаційну скаргу до Верховного Суду ¹⁷⁴.

2.4.5. Свобода вираження поглядів та підтримання авторитету і безсторонності суду

Українське законодавство в цілому відповідає європейським стандартам щодо підстав обмеження свободи вираження поглядів в інтересах захисту авторитету і безсторонності суду. Стаття 6 Закону України «Про судоустрій і статус суддів» ¹⁷⁵ передбачає, що втручання у здійснення правосуддя, вплив на суд або суддів у будь-який спосіб, неповага до суду чи суддів, збирання, зберігання, використання і поширення інформації усно, письмово або в інший спосіб з метою дискредитації суду або впливу на безсторонність суду, заклики до невиконання судових рішень забороняються і мають наслідком відповідальність, установлену законом. Кримінальний кодекс України встановлює кримінальну відповідальність виключно в разі, якщо втручання в діяльність судді здійснюється з метою перешкодити виконанню ним службових обов'язків або добитися винесення неправосудного рішення.

Отже, законодавство не містить загроз публічним дебатам навколо резонансних судових справ та функціонування судової системи як такої та не використовується задля притягнення до відповідальності критиків суду.

Водночас варто звернути увагу, що відкритість судових органів є важливим елементом права на отримання громадянами суспільно необхідної інформації. Зважаючи на це, українське законодавство зобов'язує Державну судову адміністрацію України, Вищу кваліфікаційну комісію суддів України та Вищу раду правосуддя оприлюднювати публічну інформацію у сфері судочинства та судоустрою у форматі відкритих даних, тобто, у форматі, який дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання для будь-яких цілей. Згідно з Постановою Кабінету Міністрів України № 835 від 21 жовтня 2015 з наступними змінами ¹⁷⁶ відповідні органи повинні оприлюднювати низку загальнообов'язкових для всіх та спеціальних для кожного переліків наборів даних.

¹⁷⁴ Захист співробітника «Схем» звернувся до Верховного суду через Портнова. Радіо Свобода. 15 січня 2020 року: <https://www.radiosvoboda.org/a/new-schemes-portnov-verkhovny-sud/31047463.html>

¹⁷⁵ Закон України «Про судоустрій і статус суддів»: <https://zakon.rada.gov.ua/laws/show/1402-19>

¹⁷⁶ Постанова Кабінету Міністрів України № 835 від 21 жовтня 2015 року «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних»: <https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF>

Аналітичний звіт Фондації DEJURE ¹⁷⁷ підтверджує, що лише Державна судова адміністрація так чи інакше оприлюднила всі спеціальні набори даних, тоді як Вища кваліфікаційна комісія суддів, порушуючи законодавчо визначений термін, так і не опублікувала у форматі відкритих даних власні рішення і Реєстр декларацій родинних зв'язків та доброчесності, а Вища рада правосуддя не оприлюднила власні рішення у форматі відкритих даних, як і будь-які інші набори із загальнообов'язкового для всіх розпорядників переліку, окрім звітів щодо задоволення запитів на інформацію.

В умовах судової реформи, яка триває в Україні, відкритість судової влади є важливою складовою отримання громадянами достовірної та об'єктивної інформації про здійснення правосуддя та побудови довіри суспільства до суддів. Зважаючи на це, повноцінна реалізація прав громадян на свободу вираження поглядів вимагає належного виконання судами та іншими органами у сфері судоустрою вимог щодо доступу до публічної інформації.

¹⁷⁷ Химчук А. В. Відкриті дані судової влади. Аналітичний звіт. — Київ, 2020. — 22 с.: <https://dejure.foundation/library/vidkryti-dani-sudovoi-vlady>

РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 2:

2.1. Доступ до інтернету

КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ТА МІНІСТЕРСТВУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ:

— забезпечити розроблення та прийняття підзаконних актів для реалізації положень нового Закону України «Про електронні комунікації» щодо забезпечення доступу до інтернету, зокрема і вразливим категоріям населення вже з моменту набрання ним чинності.

КАБІНЕТУ МІНІСТРІВ УКРАЇНИ:

— забезпечити прийняття Національної стратегії розвитку широкосмужового доступу до інтернету та початку реалізації її положень, зокрема щодо проведення тендерів задля розгортання мережі 5G.

НАЦІОНАЛЬНІЙ КОМІСІЇ, ЩО ЗДІЙСНЮЄ ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ:

— опублікувати у режимі відкритих даних інформацію про покриття території України доступом до інтернету.

МІНІСТЕРСТВУ ЮСТИЦІЇ УКРАЇНИ:

— узгодити Порядок організації надання засудженим доступу до глобальної мережі інтернет з гарантіями таємниці листування між засудженими та захисниками.

2.2. Свобода думки, право поширювати інформацію

СУБ'ЄКТАМ ЗАКОНОДАВЧОЇ ІНІЦІАТИВИ:

— утриматися від розроблення законодавчих ініціатив, які б створювали загрози позасудового блокування доступу до інтернет-ресурсів у разі, якщо контент, на підставі якого пропонується заблокувати ресурс, не є очевидно неправомірним (дитяча порнографія тощо);

– запропонувати зміни до Закону України «Про санкції», які б узгоджували практику їхнього застосування щодо інтернет-ресурсів з вимогами правової визначеності;

– при розробленні законодавчих ініціатив, спрямованих на обмеження шкідливого контенту в інтернеті, враховувати практику Європейського суду з прав людини, передбачати окрему оцінку необхідності обмеження доступу до контенту і до інтернет-ресурсу загалом та концентруватися на потребі блокувати саме незаконний контент, а не ресурс;

– забезпечити законодавчі гарантії ефективного розгляду справ про блокування інтернет-ресурсів та обмеження доступу до контенту в судовому порядку.

**КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ
ГУМАНІТАРНОЇ ТА ІНФОРМАЦІЙНОЇ ПОЛІТИКИ:**

– доопрацювати положення проєкту Закону України «Про медіа» № 2693-д перед їхнім прийняттям за основу та в цілому щодо обмеження доступу до онлайн-медіа з урахуванням практики Європейського суду з прав людини.

**КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ
НАЦІОНАЛЬНОЇ БЕЗПЕКИ, ОБОРОНИ ТА РОЗВІДКИ:**

– доопрацювати проєкт закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України № 3196-д та привести вимоги стосовно можливого обмеження доступу до вебсайтів, які загрожують інтересам національної безпеки, у відповідність з європейськими стандартами.

МІНІСТЕРСТВУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ:

– враховувати міжнародні стандарти та практику Європейського суду з прав людини щодо обмеження доступу до контенту в інтернеті при розробленні та впровадженні ініціатив у сфері захисту дітей в онлайн-середовищі.

**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.

ВЕРХОВНОМУ СУДУ:

— здійснити узагальнення судової практики щодо накладення арешту на майнові права інтелектуальної власності, які виникають у користувачів мережі «Інтернет» при використанні вебсайтів, з метою обмеження доступу до інтернет-ресурсів та надати відповідні роз'яснення судам стосовно розгляду таких клопотань, з урахуванням системного тлумачення національного законодавства та практики Європейського суду з прав людини.

2.3. Свобода онлайн-медіа ¹⁷⁸

**КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ
З ПИТАНЬ ГУМАНІТАРНОЇ ТА ІНФОРМАЦІЙНОЇ ПОЛІТИКИ:**

— доопрацювати проєкт Закону України «Про медіа» № 2693-д у частині визначення правового статусу онлайн-медіа та журналістів онлайн-медіа, гарантувати добровільність реєстрації онлайн-видань та виключити надмірні обмеження щодо контенту та інших вимог до їхньої діяльності, поширити гарантії свободи журналістської діяльності на журналістів онлайн-медіа.

КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ СВОБОДИ СЛОВА:

— за участю зацікавлених органів Верховної Ради України та інститутів громадянського суспільства забезпечити підготовку та розгляд законодавчих ініціатив, спрямованих на підвищення захисту законної професійної діяльності журналістів та інших медіаучасників, а також на посилення відповідальності за вчинення кримінальних правопорушень стосовно журналістів.

¹⁷⁸ Чимало рекомендацій щодо захисту діяльності журналістів в Україні були сформульовані за результатами Парламентських слухань на тему: «Безпека діяльності журналістів в Україні: стан, проблеми і шляхи їх вирішення». Доцільно наголосити на важливості імплементації вказаних рекомендацій: <https://zakon.rada.gov.ua/laws/show/456-IX#Text>

ОФІСУ ГЕНЕРАЛЬНОГО ПРОКУРОРА:

– посилити нагляд за додержанням законодавства під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням злочинів, вчинених стосовно журналістів та інших працівників ЗМІ, а також інших осіб у зв'язку з реалізацією ними права на свободу слова, зокрема за своєчасністю внесення відомостей про кримінальні правопорушення до Єдиного реєстру досудових розслідувань, правильністю правової кваліфікації, повнотою (ретельністю) досудового слідства, включаючи дослідження мотивів вчиненого злочину та встановлення наявності або відсутності зв'язку між протиправним діянням та створенням перешкод у реалізації права на свободу слова, дотриманням розумних строків досудового слідства та забезпеченням прав потерпілих під час досудового розслідування;

– включити до обов'язкової програми підготовки, перепідготовки (підвищення кваліфікації) прокурорів, слідчих вивчення спецкурсу з питань захисту професійної діяльності журналістів та інших медіаучасників, ефективного розслідування злочинів, вчинених стосовно таких осіб, розробленого з урахуванням європейських стандартів у сфері захисту прав людини, та забезпечити його подальше практичне втілення.

**МІНІСТЕРСТВУ ВНУТРІШНІХ СПРАВ УКРАЇНИ
СПІЛЬНО З ОФІСОМ ГЕНЕРАЛЬНОГО ПРОКУРОРА
ТА/АБО ДЕРЖАВНИМ БЮРО РОЗСЛІДУВАНЬ:**

– узгодити методичні рекомендації щодо розслідування злочинів проти свободи слова;

– забезпечити оприлюднення щоквартальних звітів про результати розслідування злочинів, скоєних стосовно журналістів;

– забезпечити під час розслідування злочинів, вчинених стосовно журналістів, інших працівників ЗМІ, а також інших осіб у зв'язку з реалізацією ними права на свободу слова, своєчасне внесення відомостей про кримінальні правопорушення до Єдиного реєстру досудових розслідувань, належну правову кваліфікацію вчинених діянь, повноту (ретельність) досудового слідства, включаючи дослідження мотивів вчиненого злочину та встановлення наявності або відсутності зв'язку між протиправним діянням та створенням перешкод у реалізації права на свободу слова, дотримання розумних строків досудового слідства та забезпечення прав потерпілих під час досудового розслідування.

2.4. Законність, легітимність та необхідність обмежень у демократичному суспільстві

СУБ'ЄКТАМ ЗАКОНОДАВЧОЇ ІНІЦІАТИВИ:

– при розробленні 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, з достатньою визначеністю та чіткістю формулювати заборонені категорії контенту задля уникнення зловживань щодо притягнення до відповідальності за їхнє порушення та невиправданого втручання у свободу вираження поглядів;

– переглянути норми кримінального законодавства та декриміналізувати або виключити покарання у формі позбавлення волі за окремі види висловлювань, що не містять закликів до насильницьких дій, наприклад, використання певної символіки як пропаганди тоталітарних режимів. Лише дії, що становлять реальну загрозу суспільству, повинні тягти за собою кримінальну відповідальність, пропорційну тяжкості вчиненого злочину. Ненасильницькі прояви свободи вираження поглядів не мають каратися позбавленням волі.

КАБІНЕТУ МІНІСТРІВ УКРАЇНИ:

– прийняти оновлену концепцію або стратегію щодо захисту дітей в онлайн-просторі та забезпечити її реалізацію, з дотриманням гарантій свободи вираження поглядів.

ВЕРХОВНОМУ СУДУ:

– забезпечити єдність судової практики у справах про адміністративні порушення за статтею 173-1 КУпАП щодо поширення чуток, зокрема стосовно здійснення належної оцінки усього змісту публікації, контексту її поширення та мети, оцінки належності доказової бази щодо недостовірності поширеної інформації та імовірності потенційних наслідків (паніки чи порушення громадського порядку), а також застосування практики Європейського суду з прав людини при встановленні балансу між правом особи поширювати інформацію та захистом легітимних інтересів охорони здоров'я чи громадського порядку;

– оновити роз'яснення щодо застосування законодавства у сфері захисту честі, гідності та ділової репутації, приділивши увагу особливостям застосування встановлених цивільним законодавством способів захисту особистих немайнових прав у онлайн-середовищі;

– сприяти єдності судової практики у справах щодо притягнення до кримінальної відповідальності за поширення інформації, що загрожує інтересам національної безпеки, в інтернеті, та її відповідності міжнародним стандартам у сфері свободи вираження поглядів, зокрема через належне здійснення аналізу змісту, контексту та мети поширеної публікації, ретельну оцінку належності та допустимості доказів, забезпечення пропорційності призначеного покарання та ін.

***ДЕРЖАВНІЙ СУДОВІЙ АДМІНІСТРАЦІЇ УКРАЇНИ,
ВИЩІЙ КВАЛІФІКАЦІЙНІЙ КОМІСІЇ УКРАЇНИ,
ВИЩІЙ РАДІ ПРАВОСУДДЯ:***

– своєчасно та повною мірою оприлюднювати публічну інформацію у форматі відкритих даних, відповідно до визначеного законодавством переліку, задля забезпечення належної відкритості та прозорості судової влади в Україні.

РОЗДІЛ 3.

Свобода мирних зібрань та об'єднань

3.1. Свобода використовувати інтернет-платформи

Свобода мирних зібрань та об'єднань, а також використання для реалізації цього права інтернет-платформ гарантована Конституцією України та її статтями 34, 36 та 39¹⁷⁹. Втім, ці права закріплені в загальних рисах та передбачають лише загальні обмеження. Оскільки Конституцію було прийнято у 1996 році, коли розвиток інтернету в Україні лише починався, важко очікувати, що Конституція закріпила б детальні положення з питань цифрових прав. Змін до розділу, що регулює права людини, з того часу не вносилося.

Конституцією закріплено повідомний порядок проведення мирних зібрань: для того, аби мати можливість зібратися, громадяни мають завчасно повідомити органи виконавчої влади чи органи місцевого самоврядування. Щонайменше до кінця Революції Гідності існувала практика застосування радянського законодавства, яке передбачало дозвільний порядок¹⁸⁰.

Європейський суд з прав людини у 2013 році визнав застосування відповідних норм такими, що суперечать положенням статті 11 Європейської конвенції з прав людини¹⁸¹, а у 2016 році Конституційний Суд наголосив на їхній неконституційності¹⁸². Окремого закону, що регулював би свободу мирних зібрань, в Україні не прийнято.

3.2. Обмеження свободи зібрань та об'єднань в інтернеті.

В Україні невідомо про застосування прямої конституційної норми про потребу в повідомленні щодо проведення мирних заходів задля обмежень цього права. Крім того, прямою нормою передбачено, що таке обмеження може бути застосоване лише судом відповідно до закону і лише в інтересах національної безпеки та громадського порядку — з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення або захисту прав і свобод інших людей¹⁸³.

¹⁷⁹ Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

¹⁸⁰ Указ Президії Верховної Ради СРСР «Про порядок організації та проведення зборів, мітингів, вуличних походів і демонстрацій в СРСР»: <https://zakon.rada.gov.ua/laws/show/v9306400-88>

¹⁸¹ Справа «Веренцов проти України» (Заява № 20372/11): https://zakon.rada.gov.ua/laws/show/974_945

¹⁸² Рішення Конституційного Суду України № 6-рп/2016 у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) положень частини п'ятої статті 21 Закону України «Про свободу совісті та релігійні організації» (справа про завчасне сповіщення про проведення публічних богослужінь, релігійних обрядів, церемоній та процесій) від 8 вересня 2016 року: <https://zakon.rada.gov.ua/laws/show/v006p710-16>

¹⁸³ Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

Інші норми законодавства, які б обмежували це право, відсутні. Так само не передбачені окремі заходи щодо блокування використання інтернет-платформ у контексті реалізації права на свободу зібрань, відмінні від описаних у розділі 2.2 цього звіту. Хоча, безумовно, неправомірне блокування російських соціальних медіа має прямі негативні наслідки на реалізацію українськими користувачами прав на свободу об'єднань на відповідних платформах.

Спроб законодавчо врегулювати відповідну сферу теж немає. Єдиний законопроект, який стосувався регулювання свободи мирних зібрань у цьому скликанні парламенту, був поданий народними депутатами ще у серпні 2019 року — та вже за тиждень проект був відкликаний¹⁸⁴. Втім, він не містив жодних загроз реалізації цього права в інтернеті.

Варто окремо згадати про обмеження свободи зібрань самими інтернет-платформами, які застосовують цей захід щодо груп, що порушують стандарти спільноти. В українському контексті є прецедент видалення у лютому 2020 року кількох груп у фейсбуці через поширення ними дезінформації про війну на Сході України¹⁸⁵. Такий захід слід вважати належним та пропорційним.

РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 3:

ПРАВООХОРОННИМ ОРГАНАМ:

— не застосовувати чинне законодавство для обмеження свободи мирних зібрань та об'єднань в інтернеті.

СУБ'ЄКТАМ ЗАКОНОДАВЧОЇ ІНІЦІАТИВИ:

— утриматися від внесення законодавчих ініціатив, що уможлилювали б обмеження свободи мирних зібрань та об'єднань в інтернеті, зокрема шляхом блокування платформ, а також криміналізації відвідування ресурсів, доступ до яких обмежено.

¹⁸⁴ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66509

¹⁸⁵ Анна Журба. Facebook заблокував акаунти, якими розвідка Росії поширювала дезінформацію про Україну. *Zaxid.net*. 12 лютого 2020 року: https://zaxid.net/facebook_zablokuvav_akaunti_yakimi_rozvidka_rosiyi_poshiryuvala_dezinformatsiyu_pro_ukrayinu_n1497610

РОЗДІЛ 4. Право на повагу до приватного і сімейного життя

4.1.1. Законодавча основа

Закон України «Про захист персональних даних»¹⁸⁶ набрав чинності 1 січня 2011 року. Цей закон вперше систематизував підходи до визначення і ключові засади оброблення персональних даних в Україні та мав на меті гармонізувати національне законодавство з вимогами Конвенції про захист осіб у зв'язку з автоматизованим обробленням персональних даних¹⁸⁷, Директивою 95/46/ЄС Європейського парламенту і Ради від 24.10.1995 р. стосовно захисту фізичних осіб у питаннях оброблення персональних даних і вільного обігу цих даних¹⁸⁸ та Директивою 97/66/ЄС¹⁸⁹ Європейського парламенту і Ради від 15.12.1997 р. щодо оброблення персональних даних і захисту приватності в телекомунікаційному секторі¹⁹⁰.

Чинна редакція закону імплементує ключові вимоги та принципи оброблення персональних даних, визначені Конвенцією про захист осіб у зв'язку з автоматизованим обробленням персональних даних. Конвенція була істотно модернізована у травні 2018 року відповідним Протоколом СМ(2018)2¹⁹¹. Україна поки що не приєдналася до Протоколу, але взяла на себе зобов'язання погодити законодавство про захист персональних даних із вимогами ЄС. Так, відповідно до пункту 11 Плану заходів щодо виконання Угоди про асоціацію з ЄС, затвердженого Постановою Кабінету Міністрів України № 1106 від 25.10.2017¹⁹², передбачено вдосконалення законодавства про захист персональних даних для узгодження його із Загальним регламентом захисту даних, що набув сили 25 травня 2018 року¹⁹³.

Робота над оновленою редакцією Закону України «Про захист персональних даних» розпочалася ще у 2018 та продовжилася у 2020 році. Відповідна робоча група з реформування законодавства України щодо оброблення та захисту персональних даних була створена спільно Комітетом Верховної Ради України з питань цифрової трансформації та Комітетом Верховної Ради України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій у Донецькій, Луганській областях та Автономної Республіки Крим, міста Севастополя, національних меншин і міжнаціональних відносин.

¹⁸⁶ Закон України «Про захист персональних даних»: <https://zakon.rada.gov.ua/laws/show/2297-17>

¹⁸⁷ Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: https://zakon.rada.gov.ua/laws/show/994_326

¹⁸⁸ Директива 95/46/ЄС: https://zakon.rada.gov.ua/laws/show/994_242

¹⁸⁹ Директива 97/66/ЄС: https://zakon.rada.gov.ua/laws/show/994_243

¹⁹⁰ Див. Пояснювальна записка до проекту закону про захист персональних даних: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2273&skl=7

¹⁹¹ Протокол СМ (2018)2: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>

¹⁹² 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%BE>

¹⁹³ Загальний регламент захисту даних: <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>

До складу робочої групи входять народні депутати та їхні помічники, представники Міністерства цифрової трансформації України, представники Секретаріату Уповноваженого Верховної Ради України з прав людини, експерти міжнародних організацій, правники, представники громадянського суспільства.

У листопаді 2020 року свій висновок щодо напрацьованих положень майбутнього законопроекту надали експертки проекту «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини» Наташа Пірч Мусар та Діяна Шинкунене, які вказали на необхідність передбачити в законопроекті, зокрема: зобов'язання державних установ, залучених у законодавчий процес, включати до законодавчих актів, що регулюють оброблення персональних даних, ціль оброблення та іншу відповідну інформацію залежно від обставин; процедуру здійснення контролерами даних оцінки впливу на захист даних у процесі ухвалення законодавчого акта; встановити основні принципи оброблення персональних даних органами державного сектору, а також передбачити в законопроекті створення незалежного органу контролю щодо захисту персональних даних. Окрему увагу також звернули на необхідність вдосконалити норми щодо оброблення персональних даних для цілей журналістської чи творчої діяльності ¹⁹⁴.

4.1.2. Принципи оброблення персональних даних

Закон України «Про захист персональних даних» ¹⁹⁵ визначає ключові принципи оброблення персональних даних, що відповідають вимогам Конвенції про захист осіб у зв'язку з автоматизованим обробленням персональних даних, але поки що не деталізує та не уточнює зазначені вимоги з урахуванням останніх змін, запропонованих Протоколом до Конвенції ¹⁹⁶.

Відповідно до статті 6 Закону України «Про захист персональних даних», оброблення персональних даних має здійснюватися для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних або на підставі закону. Згода має відповідати таким принципам як добровільність, однозначність та поінформованість.

У разі зміни визначеної мети оброблення персональних даних на нову мету, яка є несумісною з попередньою, для подальшого оброблення даних володілець персональних даних повинен отримати згоду суб'єкта персональних даних на оброблення його даних відповідно до зміненої мети, якщо інше не передбачено законом.

¹⁹⁴ Консультації експертів щодо законопроекту про захист персональних даних:

<https://www.coe.int/uk/web/kyiv/-/new-draft-law-of-ukraine-on-personal-data-protection-expert-consultations-with-support-of-join-eu-and-coe-project>

¹⁹⁵ Закон України «Про захист персональних даних»: <https://zakon.rada.gov.ua/laws/show/2297-17>

про Україну. Zaxid.net. 12 лютого 2020 року:

https://zaxid.net/facebook_zablokuvav_akaunti_yakimi_rozvidka_rosiyi_poshiryuvala_dezinformatsiyu_pro_ukrayinu_n1497610

¹⁹⁶ Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e

Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх оброблення, а склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх оброблення.

Стаття 24 Закону «Про захист персональних даних» передбачає обов'язок осіб, що здійснюють оброблення персональних даних, забезпечувати захист цих даних від випадкових втрати або знищення, від незаконного оброблення, зокрема незаконного знищення чи доступу до персональних даних.

На практиці оброблення персональних даних часто здійснюється з порушенням зазначених принципів, не лише з боку приватних суб'єктів, а і з боку органів державної влади.

За даними Щорічної доповіді Уповноваженого Верховної Ради України про стан дотримання та захисту прав і свобод людини і громадянина в Україні, у 2020 році до Уповноваженого надійшло майже 1500 скарг, які стосувалися порушення права людини на невтручання в особисте і сімейне життя під час здійснення діяльності зі стягнення заборгованості за грошовими зобов'язаннями фізичних осіб (колекторська діяльність). Більшість виявлених порушень зачіпали саме невизначення правових підстав для оброблення персональних даних суб'єктів та неправомірного оброблення персональних даних третіх (контактних) осіб, а також неповідомлення суб'єкта про його права, не надання інформації щодо володільця, мети оброблення, складу та змісту зібраних персональних даних, здійснення їх трансграничної передачі.¹⁹⁷

У жовтні 2020 року в парламенті зареєстрували проєкт закону № 4241 «Про внесення змін до деяких законодавчих актів України щодо захисту боржників при врегулюванні простроченої заборгованості»¹⁹⁸, що має встановити правила роботи колекторів, зокрема порядок реєстрації колекторської компанії, вимоги до етичної поведінки з боржниками, форми і порядок комунікації, вичерпний перелік персональних даних для оброблення, нагляд за колекторською діяльністю, санкції за порушення¹⁹⁹.

Уповноважений з прав людини у своїй доповіді також звернула увагу на незаконне поширення персональних даних, що були допущені державними органами, а також на практику неправомірного витребовування згоди на оброблення персональних даних від особи, що призводить до створення штучних перешкод для людини під час реалізації її конституційних прав (на освіту, на працю, охорону здоров'я тощо).

Окремі законодавчі ініціативи, внесені до парламенту у 2020 році також суперечили визначеним принципам оброблення персональних даних. Наприклад, 26 жовтня 2020 року у Верховній Раді України було зареєстровано проєкт закону «Про державну реєстрацію геномної інформації людини» № 4265²⁰⁰.

¹⁹⁷ Щорічна доповідь Уповноваженого Верховної Ради України про стан дотримання та захисту прав і свобод людини і громадянина в Україні у 2020 році: https://ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf

¹⁹⁸ Картка законопроєкту: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70219

¹⁹⁹ Закон прийнято 19 березня 2021 року.

²⁰⁰ Картка законопроєкту: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70249

Законопроект передбачає створення Баз даних геномної інформації людини, держателем якої буде Міністерство внутрішніх справ України, а адміністратором Державний науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України. Цілями державної реєстрації геномної інформації визначено профілактику кримінальних правопорушень; встановлення осіб, які вчинили кримінальні правопорушення; розшук осіб, зниклих безвісти; ідентифікація невпізнаних тіл (останків) чи людини, яка за станом здоров'я чи за віком не може повідомити відомості про себе.

Водночас законопроект не визначає належного порядку оброблення персональних даних, що відповідав би засадничим принципам, визначеним законом ²⁰¹. Передбачається, що порядок оброблення геномної інформації та ведення Баз даних буде встановлено Кабінетом Міністрів України ²⁰², тоді як, зважаючи на чутливий характер геномної інформації, порядок збору, використання та захисту таких персональних даних доцільно визначити на рівні закону, не залишаючи виконавчим органам широкі межі для дискреції. Закон не визначає з належною чіткістю, які біологічні матеріали підлягають збору та в яких випадках, як і процедуру їх збору, що гарантувала б належний рівень захисту. Наостанок, доступ до «ключів» та біологічних матеріалів, за допомогою яких можна буде розшифрувати дані з цієї бази, отримає низка державних експертних установ, установ виконання покарань та спеціалізованих медичних установ, що створює значні ризики витоку інформації, а концентрація збору, зберігання та управління доступом до таких даних у Міністерстві внутрішніх справ створює значні корупційні ризики ²⁰³.

Проект закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України № 3196-д ²⁰⁴, ухвалений у першому читанні у січні 2021 року, пропонує наділити СБУ необмеженим доступом до будь-яких персональних даних громадян, зокрема тих, що зберігаються не лише в державних реєстрах, але і у приватних базах даних та збираються за допомогою систем відеоспостереження. Водночас СБУ може створювати на їхній основі власні бази та банки даних, інформаційні масиви, інформаційні та інформаційно-телекомунікаційні системи, вести спеціальний оперативний облік. Жодних вимог чи деталей щодо порядку внесення та зберігання персональної інформації у таких базах даних СБУ законопроект не містить. Отже, СБУ отримає безперешкодний доступ до величезних масивів персональних даних осіб, безвідносно до того, чи є підстави здійснювати щодо таких осіб контррозвідувальні, оперативно-розшукові чи інші заходи, які належать до компетенції СБУ.

²⁰¹ Що не так з обробкою геномної інформації в законопроекті № 4265? – Лабораторія цифрової безпеки: <https://dslua.org/publications/shcho-ne-tak-z-obrobkoiu-henomnoi-informatsii-v-zakonoproekti-4265/>

²⁰³ Висновок Головного науково-експертного управління: <https://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=70249&pf35401=538372>

²⁰⁴ Картка законопроекту: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243

Порядок доступу СБУ до державних баз персональних даних пропонується визначити указами Президента України та постановами Кабінету Міністрів України. Такий підхід суперечить вимогам закону «Про захист персональних даних», який передбачає, що зазначений порядок має регулюватися законом та відповідати принципам законності, пропорційності, мінімізації, підзвітності оброблення даних та іншим. Умови та порядок передачі такої інформації мають бути чітко врегульовані законом ²⁰⁵.

Українське законодавство на сьогодні також не містить спеціальних обмежень чи вимог щодо здійснення «профайлінгу» — техніки автоматичного оброблення персональних даних, що передбачає збір та використання інформації про особу з метою ідентифікації, аналізу та передбачення її вподобань, поведінки та ставлення.

Концепція розвитку штучного інтелекту в Україні ²⁰⁶, що була схвалена Кабінетом Міністрів України 2 грудня 2020 року, серед основних принципів розвитку та використання технологій штучного інтелекту передбачає забезпечення відповідності діяльності та алгоритмів рішень систем штучного інтелекту вимогам законодавства про захист персональних даних, а також дотримання конституційного права кожного на невтручання в особисте та сімейне життя у зв'язку з обробленням персональних даних ²⁰⁷.

4.1.3. Права осіб у зв'язку з обробленням їхніх даних

Закон України «Про захист персональних даних» гарантує кожній особі низку прав, пов'язаних зі здійсненням автоматизованого оброблення її даних, зокрема:

- 1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх оброблення, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим нею особам, крім випадків, встановлених законом;
- 2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються її персональні дані;
- 3) право на доступ до своїх персональних даних;
- 4) отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

²⁰⁵ Лабораторія цифрової безпеки. Блокування сайтів, масове стеження, фільтрування кандидатів на виборах, або Нові повноваження СБУ: <https://dslua.org/publications/blokuvannia-saytiv-masove-stezhennia-filtruvannia-kandydativ-na-vyborakh-abo-novi-povnovazhennia-sbu/>

²⁰⁶ Розпорядження КМУ від 02 грудня 2020 р. № 1556-р «Про схвалення концепції розвитку штучного інтелекту в Україні»: <https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text>

²⁰⁷ Лабораторія цифрової безпеки. Уряд затвердив Концепцію розвитку штучного інтелекту в Україні з урахуванням пропозицій Цифролаби: <https://dslua.org/publications/uriad-zatverdyy-kontseptsiiu-rozvytku-shtuchnoho-intelektu-v-ukraini-z-urakhuvanniam-propozytisyi-tsyfrolaby/>

- 5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти оброблення своїх персональних даних;
- 6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- 7) на захист своїх персональних даних від незаконного оброблення та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- 8) звертатися із скаргами на оброблення своїх персональних даних до Уповноваженого або до суду;
- 9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
- 10) вносити застереження стосовно обмеження права на оброблення своїх персональних даних під час надання згоди;
- 11) відкликати згоду на оброблення персональних даних;
- 12) знати механізм автоматичного оброблення персональних даних;
- 13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Водночас закріплення в законі прав володільця персональних даних на практиці не завжди гарантує їх повноцінну реалізацію. Держава має також забезпечувати ефективні механізми захисту в разі порушення прав особи. На сьогодні, особа, чії особисті немайнові права були порушені у зв'язку з неправомірним обробленням її персональних даних, може звернутися зі скаргою до Уповноваженого Верховної Ради України з прав людини, безпосередньо до суду або ж до поліції, у разі, якщо мало місце незаконне збирання, зберігання, використання, знищення чи поширення конфіденційної інформації про особу (стаття 182 Кримінального кодексу України). Проте жоден із зазначених способів на сьогодні не гарантує ефективного захисту порушеного права. Так Офіс Уповноваженого не має достатніх ресурсів для ефективного розгляду усіх отриманих скарг, а процедура судового розгляду та кримінального розслідування можуть тривати кілька місяців чи навіть більше року. Зважаючи на це, одним із актуальних питань залишається створення окремого спеціалізованого органу з контролю за дотриманням законодавства та прав громадян щодо захисту персональних даних.

Окремо слід звернути увагу на судову практику, яка свідчить про наявність системних порушень, пов'язаних зі зловживанням державними службовцями доступом до державних реєстрів та баз даних, що містять персональні дані особи.

Так, у 2020 році було винесено 6 вироків ²⁰⁸ у кримінальних справах щодо несанкціонованого розповсюдження інформації з обмеженим доступом, яка зберігається в автоматизованих системах Державної фіскальної служби України та Державної прикордонної служби України (статті 361-2 та 362 Кримінального кодексу України). Зважаючи на це, законодавцю варто розглянути посилення механізмів захисту від можливих зловживань, пов'язаних із обробленням персональних даних у державних реєстрах.

Протидія незаконному продажу персональних даних громадян, що набуває поширення в Telegram ²⁰⁹, потребує вироблення системних підходів, як щодо посилення вимог до безпеки державних та комерційних баз даних, так і щодо методів розслідування такої незаконної діяльності. Окреме занепокоєння викликає відсутність ефективних державних заходів щодо припинення незаконного поширення персональних даних на сайті «Миротворець» ²¹⁰. У 2020 році «Миротворець» вніс журналіста розслідувального проєкту «Наші гроші з Денисом Бігусом» до своєї бази «людей, які становлять загрозу українській державі та суспільству, скоїли злочини проти основ національної безпеки» через сюжет про розкрадання в оборонній промисловості ²¹¹.

Варто зауважити, що права володільців персональних даних не є абсолютними і можуть підлягати обмеженням, встановленим законом у легітимних інтересах. Українське законодавство, зокрема, належним чином балансує вимоги захисту персональних даних із вимогами щодо забезпечення доступу до публічної інформації та свободи вираження поглядів.

Зокрема, стаття 5 Закону України «Про захист персональних даних» передбачає, що не є конфіденційною інформацією персональні дані, які стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень. Не належать до інформації з обмеженим доступом також персональні дані, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, оформленій за формою, визначеною відповідно до Закону України «Про запобігання корупції», крім відомостей щодо реєстраційного номера облікової картки платника податків або серії та номера паспорта громадянина України, унікального номера запису в Єдиному державному демографічному реєстрі, місця проживання, дати народження фізичних осіб, щодо яких зазначається інформація в декларації, місцезнаходження об'єктів,

²⁰⁸ Див., наприклад:

Вирок у справі № 641/3658/20: <https://reyestr.court.gov.ua/Review/93639586>;

Вирок у справі № 686/6670/20: <https://reyestr.court.gov.ua/Review/88730915>;

Вирок у справі № 711/870/20: <https://reyestr.court.gov.ua/Review/88115992>;

Вирок у справі № 344/8068/20: <https://reyestr.court.gov.ua/Review/93809770>

²⁰⁹ MediaSapiens.Telegram-бот продає особисті дані українців. СБУ розпочала розслідування:

<https://ms.detector.media/kiberbezpeka/post/24656/2020-05-12-telegram-bot-prodaie-osobysti-dani-ukraintsiv-sbu-rozpochala-rozsliduvannya/>

²¹⁰ Сайт Центру «Миротворець»: <https://myrotvorets.center/>

²¹¹ Інститут Масової інформації – Бігуса внесли до бази «Миротворця»:

<https://imi.org.ua/news/bigusa-vnesly-v-bazu-myrotvortsya-i34627>

які наводяться в декларації (крім області, району, населеного пункту, де розташований об'єкт), номера рахунку в банківській чи іншій фінансовій установі ²¹². Законодавство передбачає також низку інших випадків, за яких персональні дані можуть поширюватися без згоди особи, якщо це є предметом суспільного інтересу, що переважає можливу шкоду, заподіяну розголошенням.

4.1.4. Наглядовий орган

Одним із ключових елементів ефективного механізму захисту персональних даних є діяльність незалежного наглядового органу у сфері персональних даних та створення для користувачів дієвих механізмів захисту їхніх прав.

В Україні система захисту персональних даних, яка б повністю відповідала міжнародним стандартам наразі відсутня. Відповідно до статті 22 Закону України «Про захист персональних даних» нагляд та контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснює Уповноважений Верховної Ради України з прав людини (Омбудсман). Громадяни також можуть оскаржувати порушення їхнього права на доступ безпосередньо в судовому порядку.

Відповідно до звіту Уповноваженого Верховної Ради України з прав людини, у 2020 році до Уповноваженого надійшло 2 031 повідомлення про порушення прав людини на захист персональних даних, що у порівнянні з 2019 роком (1061) майже удвічі більше. За результатами аналізу отриманих Уповноваженим повідомлень вбачається, що більшість з них (майже 1 500) стосувалися порушення права людини на невтручання в особисте і сімейне життя під час здійснення діяльності зі стягнення заборгованості за грошовими зобов'язаннями фізичних осіб (колекторська діяльність). Отримані повідомлення також стосувались незаконного поширення персональних даних через мережу «Інтернет», месенджери та соціальні мережі, порушення права на захист персональних даних під час впровадження електронних сервісів. З метою здійснення парламентського контролю за додержанням права на захист персональних даних проведено 67 перевірок підприємств, установ і організацій, органів державної влади та місцевого самоврядування, що є володільцями та/або розпорядниками персональних даних, відкрито 62 провадження Уповноваженого, складено та передано до суду 9 протоколів про адміністративне правопорушення за частиною четвертою статті 188-39 КУпАП ²¹³.

Попри те, що Омбудсман наділений повноваженнями щодо проведення перевірок дотримання законодавства про захист персональних даних та може виносити обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, зокрема щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення оброблення персональних даних, мандат Уповноваженого обмежений функціями парламентського контролю, як це передбачено Конституцією України.

²¹² Закон України «Про запобігання корупції»: <https://zakon.rada.gov.ua/laws/show/1700-18>

²¹³ Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2020 рік

Власне, як зауважує чинна Уповноважена, частина повноважень, які мають здійснюватися наглядовим органом відповідно до статті 58 Загального регламенту захисту даних ЄС (зокрема проведення розслідувань, накладення адміністративних штрафів), не повною мірою узгоджуються з природою конституційно-правового статусу Уповноваженого Верховної Ради України з прав людини, який відповідно до статті 101 Конституції України здійснює «парламентський контроль за дотриманням конституційних прав і свобод людини і громадянина». Зважаючи на викладене, Уповноважений підтримує необхідність створення окремого наглядового органу в сфері захисту персональних даних та доступу до публічної інформації. Відповідно до Загального регламенту захисту даних ЄС, під час створення наглядового органу важливо забезпечити на відповідному законодавчому та конституційному рівнях високий ступінь його незалежності. Повністю уникнути будь-яких можливостей впливу на рішення наглядового органу, а також ймовірних підозр щодо упередженості можна лише шляхом створення нової інституції, що не входить до складу виконавчої гілки влади ²¹⁴.

Поки що ніяких пропозицій про створення нової інституції у сфері нагляду за дотриманням законодавства у сфері персональних даних представлено не було. Серед моделей, що можуть розглядатися, виділяють такі, як створення окремого державного органу, що не належить до жодної з гілок державної влади України; створення окремого самостійного центрального органу виконавчої влади або ж наділення повноваженнями контролю кількох різних державних органів ²¹⁵. У будь-якому разі, має бути дотримано ключовий критерій щодо незалежності такої інституції.

4.1.5. Обмеження

Українське законодавство за загальним правилом передбачає, що будь-які втручання в право особи на повагу до приватного і сімейного життя мають бути передбачені законом, переслідувати легітимну ціль та бути необхідними у демократичному суспільстві. Водночас нещодавні законодавчі зміни та окремі законодавчі ініціативи, що вносяться до парламенту, викликають занепокоєння щодо відступу від таких стандартів.

Держава не встановлює заборон, щодо анонімності, псевдонімізації, таємниці приватних комунікацій чи застосування технологій шифрування. Обмеження анонімності здійснюється за загальним правилом відповідно до кримінального процесуального законодавства.

²¹⁴ Щодо створення наглядового органу у сфері захисту персональних даних: <https://www.ombudsman.gov.ua/ua/all-news/pr/shhodo-stvorenniya-naglyadovogo-organu-u-sfer%d1%96-zaxistu-personalnih-danix-ta-dostupu-do-publ%d1%96chno%d1%97-%d1%96nformacz%d1%96%d1%97/>

²¹⁵ Правовий аналіз основних моделей інституалізації державного контролю у сфері персональних даних та доступу до публічної інформації в Україні. Володимир Венгер, Олег Зяярний. 2020 р.: <https://rm.coe.int/legal-analysis-data-ua/16809ee077>

На початку 2020 року Міністерство культури, молоді та спорту України ініціювало обговорення проєкту Закону України «Про внесення змін до деяких законодавчих актів України щодо забезпечення національної інформаційної безпеки та права на доступ до достовірної інформації», який, серед іншого, встановлював вимоги щодо обов'язкового публічного розкриття інформації про особу усіх поширювачів масової інформації, що суперечить міжнародним принципам анонімності²¹⁶. Документ був різко розкритикований громадськістю та міжнародними організаціями²¹⁷, жодних кроків щодо його подальшого просування чи внесення до парламенту Міністерство не здійснювало.

Навесні 2020 року, у зв'язку з поширенням на території України Covid-19, питання захисту персональних даних набули особливої актуальності в умовах введення протиепідемічних заходів. 13 квітня 2020 року Верховна Рада ухвалила Закон України «Про внесення змін до Закону України “Про захист населення від інфекційних хвороб” щодо запобігання поширенню коронавірусної хвороби (COVID-19)»²¹⁸. Серед новел — дозвіл на період карантину, з метою протидії поширенню коронавірусної хвороби, обробляти дані про стан здоров'я, місце госпіталізації або самоізоляції, прізвище, ім'я, по батькові, дату народження, місце проживання, роботи (навчання) особи без її згоди.

Ухвалений закон суперечить загальним вимогам та принципам у сфері захисту персональних даних. Попри наявність очевидного легітимного інтересу в обмеженні прав особи в інтересах охорони здоров'я, ухвалений закон не містить належної правової визначеності, зокрема, не встановлює, які саме державні органи отримують повноваження здійснювати оброблення персональних даних без згоди особи та в якому обсязі (щодо кожного державного органу окремо). Закон також не містить жодних запобіжників від зловживань, хоча йдеться про особливо чутливу інформацію про стан здоров'я особи. При цьому коло осіб, залучених до протиепідемічних заходів надзвичайно широке. Тому надання їм повноважень отримувати доступ до усієї переліченої вище інформації не є виправданим²¹⁹.

Лабораторія цифрової безпеки також аналізувала дотримання принципів оброблення персональних даних при впровадженні додатку «Вдома» («Дій вдома»), що був створений Міністерством цифрової трансформації для моніторингу дотримання громадянами карантинних обмежень²²⁰.

²¹⁶ Лабораторія цифрової безпеки. Юридичний аналіз законопроекту про дезінформацію: <https://dslua.org/publications/yurydychnyy-analiz-zakonoprojektu-pro-dezinformatsiiu/>

²¹⁷ Детектор медіа. ЕФJ виступила проти регулювання діяльності журналістів з боку української влади: <https://detector.media/community/article/174120/2020-01-22-efj-vystupyla-proty-regulyuvannya-diyalnosti-zhurnalistiv-z-boku-ukrainskoi-vlady/>

²¹⁸ Закон України «Про внесення змін до Закону України “Про захист населення від інфекційних хвороб” щодо запобігання поширенню коронавірусної хвороби (COVID-19)» <https://zakon.rada.gov.ua/Laws/show/555-IX>

²¹⁹ Лабораторія цифрової безпеки. «Не час для згоди»: що не так із новим «антивірусним» законом: <https://dslua.org/publications/ne-chas-dlia-zghody-shcho-ne-tak-iz-novym-antivirusnym-zakonom/>

²²⁰ Лабораторія цифрової безпеки. Кабмін деталізував умови застосування «Дій вдома»: <https://dslua.org/publications/kabmin-detalizuvav-umovy-zastosuvannia-diy-vdoma/>

Попри те, що встановлення додатку є добровільним, обмін інформацією в системі між Міністерством охорони здоров'я, МВС та Мінцифри здійснюється не у порядку, визначеному законом, а на підставі окремих угод, що укладені між міністерствами. Це не забезпечує належної прозорості щодо того, хто і в якому обсязі має доступ до персональних даних осіб хворих чи з підозрою на Covid-19 та не гарантує достатніх обмежень дискреції органів влади щодо використання таких даних.

Серйозне занепокоєння щодо втручання держави в право на інформаційну приватність особи та можливого профайлінгу викликає також «експериментальний» проєкт щодо верифікації даних державних реєстрів. Так, 4 грудня 2019 року Кабінет Міністрів України затвердив Постанову № 1078 «Про реалізацію експериментального проєкту верифікації даних про фізичних осіб, що обробляються в деяких національних електронних інформаційних ресурсах»²²¹.

Відповідно до Постанови верифікації підлягають дані про фізичних осіб, що обробляються у Державному реєстрі актів цивільного стану громадян, Державному реєстрі фізичних осіб — платників податків, Реєстрі застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування, Єдиній державній електронній базі з питань освіти, а також у Реєстрі пацієнтів електронної системи охорони здоров'я. Верифікація має здійснюватися шляхом передачі визначених категорій даних з відповідних реєстрів до МВС, які мають здійснити установлення тотожності між даними різних реєстрів, за допомогою власної інформаційної системи. Міністерство фінансів з метою проведення верифікації даних про фізичних осіб, що обробляються в національних електронних інформаційних ресурсах, має передати МВС у користування відповідні програмні розробки та технічні рішення, на базі яких створено Інформаційно-аналітичну платформу електронної верифікації та моніторингу.

Варто зауважити, що встановлення достовірності даних національних реєстрів не є єдиною метою «верифікації». Так отримана інформація буде використана для наповнення Єдиного державного демографічного реєстру. Відповідно до пункту 5 Постанови № 1078 МВС та Державна міграційна служба мають забезпечити верифікацію отриманих даних з даними Єдиного державного демографічного реєстру, а також наповнення Єдиного державного демографічного реєстру даними про фізичну особу, що пройшли верифікацію, з одночасним формуванням тимчасового номера унікального номера запису в реєстрі. А відповідно до пункту 6 Постанови МВС має запровадити електронний сервіс ідентифікації фізичних осіб засобами єдиної інформаційної системи Міністерства внутрішніх справ з метою подальшого узгодження інформації в інших національних електронних інформаційних ресурсах з єдиним ідентифікатором.

²²¹ Постанова № 1078: <https://www.kmu.gov.ua/npas/pro-realizaciyu-eksperimentalnogo-p-a1078>

Відповідно до строків та етапів реалізації експериментального проекту, визначених у Додатку 2 до Постанови, уже наприкінці травня 2020 року Мінцифри, що забезпечує координацію процесу верифікації, спільно з МВС мали підготувати звіт про результати проведеної верифікації достовірності, актуальності, повноти та ненадмірності даних про фізичних осіб та надати пропозиції щодо «забезпечення комплексного уніфікованого підходу до правових та організаційних засад функціонування національних електронних інформаційних ресурсів». Однак, у 2020 році МВС все ще не оприлюднило методологію проведення верифікації, що не зупиняє МВС отримувати дані від адміністраторів відповідних реєстрів, на практиці.

Безумовно, перевірка достовірності інформації, що вноситься до державних реєстрів, є важливою. Водночас, зважаючи на масштаби перевірки та те, що така функція покладена на правоохоронний орган, процедура здійснення верифікації повинна мати чітке законне підґрунтя, відповідати вимогам законодавства про захист персональних даних, бути прозорою та здійснюватися із дотриманням усіх необхідних заходів безпеки. Однак, запропонований Постановою № 1078 механізм верифікації прямо суперечить чинному законодавству України, яке визначає інший порядок оброблення та верифікації персональних даних у перелічених реєстрах ²²². Отже, процедура верифікації даних реєстрів потребує негайного узгодження з вимогами законодавства.

4.2. Стеження

Заходи стеження, що застосовуються державними органами, повинні відповідати вимогам статті 8 Європейської конвенції, зокрема принципам законності, легітимності та необхідності у демократичному суспільстві, а також бути предметом ефективного, незалежного та неупередженого нагляду.

На сьогодні українське законодавство не містить достатніх гарантій для забезпечення дотримання права на повагу до приватного життя, зокрема приватності електронних комунікацій, в онлайн-середовищі. Відсутність законодавчо визначеного порядку здійснення перехоплення електронних комунікацій, слабкий та формальний контроль за дотриманням прав людини при здійсненні таких заходів, а також поєднання в Службі безпеки України функцій у сфері національної безпеки та розслідування кримінальних правопорушень, створює необмежену дискрецію таких органів та може призводити до безконтрольного втручання в право громадян на приватність.

4.2.2. Вимоги до законодавства у сфері стеження

Відповідно до стандартів Європейської конвенції, заходи стеження повинні здійснюватися відповідно до доступного, чіткого, конкретного та передбачуваного закону. Закон має містити запобіжники щодо дискреції державних органів, для чого зокрема чітко та точно встановлювати:

²²² «Цифрова держава» та персональні дані: дотримання законодавства про захист персональних даних в ініціативах діджиталізації»:

<https://internetfreedom.org.ua/ua/zakhody/158-aba-rol-i-ta-laboratoriia-tsyfrovoi-bezpeky-provely-ekspertne-obhovorennia-tsyfrova-derzhava-ta-personalni-dani-dotrymannia-zakonodavstva-pro-zakhyst-personalnykh-danykh-v-initsiatyvakh-didzhytalizatsii>

- природу порушень, щодо яких можуть застосовуватися заходи стеження;
- компетентні державні органи, які мають повноваження здійснювати заходи стеження, сферу їх дискреції та спосіб її реалізації, базуючись на легітимній цілі відповідного заходу;
- категорії осіб, щодо яких можуть застосовуватися заходи стеження;
- обмеження щодо застосування заходів стеження;
- процедури щодо аналізу, використання та зберігання інформації, отриманої за допомогою заходів стеження;
- запобіжні заходи щодо передавання отриманих даних іншим особам та заходи щодо безпеки передавання даних;
- підстави для знищення або видалення інформації отриманої за результатами стеження;
- державні органи, відповідальні за нагляд за застосуванням заходів стеження ²²³.

Кримінальний процесуальний кодекс України здебільшого охоплює перелічені елементи. Водночас застосування заходів стеження в рамках розвідувальних, контррозвідувальних чи інших заходів, пов'язаних із діяльністю у сфері національної безпеки, не супроводжується достатніми запобіжниками від надмірного втручання у приватність особи.

Закон України «Про розвідку» ²²⁴, ухвалений 17 вересня 2020 року, наділяє розвідувальні органи повноваженнями проводити стосовно особи, місця або речі, які перебувають на території України, окремі розвідувальні заходи, що полягають у знятті інформації з транспортних телекомунікаційних мереж шляхом відбору та фіксації змісту відповідних відомостей або даних, що передаються або отримуються особою, та знятті інформації з електронних інформаційних систем шляхом пошуку, відбору та фіксації відповідних відомостей або даних, що містяться в електронній інформаційній системі або її частині, без відома її власника, володільця або утримувача, а також у локалізації радіоелектронного засобу, шляхом відбору та фіксації відомостей або даних про місцезнаходження та/або використання такого засобу (пристрою) без розкриття змісту повідомлень, що передаються або отримуються особою.

Закон передбачає, що такі розвідувальні заходи проводяться за умов, якщо вони безпосередньо пов'язані зі здійсненням розвідувальної діяльності за межами України або спрямовані на здобування розвідувальної інформації, що має джерело походження за межами України, та виключно на підставі рішення суду. Розвідувальні органи володіють досить широкою дискрецією у визначенні підстав для застосування відповідних заходів. Крім цього, допускається проведення розвідувальних заходів до отримання рішення суду, але не більше ніж 72 години з моменту ідентифікації особи.

²²³ Recommendation CM/Rec(2016)5 on Internet freedom: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016806415d8

²²⁴ Закон України «Про розвідку»: <https://zakon.rada.gov.ua/laws/show/912-20>

Закон встановлює, що строк дії ухвали про застосування відповідних заходів стеження не може перевищувати шести місяців, однак не містить інших вимог, які б регламентували порядок зберігання, використання чи знищення отриманих даних.

Зняття інформації з транспортних телекомунікаційних мереж операторів телекомунікацій, які надають послуги мобільного та/або фіксованого зв'язку, має забезпечуватися «системою технічних засобів, що використовується всіма розвідувальними органами на умовах автономного доступу до інформації у порядку, визначеному законодавством». На сьогодні законом не врегульовано відповідний порядок автономного доступу до інформації. Власне можливість безпосереднього доступу органів безпеки до телекомунікаційних мереж створює серйозні перешкоди для належного й ефективного нагляду за дотриманням прав людини при здійсненні розвідувальних заходів.

Водночас навіть ширшими повноваженнями пропонується наділити Службу безпеки України при здійсненні контррозвідувальних заходів. Відповідний законопроект «Про внесення змін до Закону України “Про Службу безпеки України” щодо удосконалення організаційно-правових засад діяльності Служби безпеки України» № 3196-д²²⁵ передбачає, що під час контррозвідувальної діяльності СБУ може отримувати від операторів та провайдерів телекомунікацій технологічну та іншу інформацію про функціонування мереж, зокрема з обмеженим доступом, на умовах, визначених володільцем цієї інформації та уповноваженим підрозділом Служби безпеки України. Зняття ж інформації з телекомунікаційних мереж, а також пошук, доступ, відбір і фіксація даних, що містяться в електронних інформаційних мережах (системах) або її частинах, доступ до яких обмежується її власником, володільцем, утримувачем або пов'язаний з подоланням системи логічного захисту, можуть здійснюватися виключно за рішенням суду, крім невідкладних випадків, коли звернення може спричинити знищення необхідних в інтересах контррозвідувальної діяльності фактичних даних або зумовити неможливість їх отримання. Тоді керівництво СБУ може самостійно прийняти рішення, яке, однак, протягом 24 годин має бути передане на затвердження до суду. У разі відмови суду – отримана інформація має бути знищена.

При цьому розширення повноважень СБУ щодо стеження не супроводжується належними запобіжниками від зловживань та порушень прав людини. На відміну від регулювання процедур зняття інформації в порядку кримінального провадження, застосування заходів стеження в процесі контррозвідки не передбачає встановлення чітких підстав, категорій та прав суб'єктів щодо яких застосовуються такі заходи. Законопроект суттєво розширює сферу контррозвідувальної діяльності, а однією з цілей стає протидія підривної діяльності, яка тлумачиться досить широко як «вплив на суспільні відносини, що становить чи може становити загрозу державній безпеці та/або підвищує ризики державної безпеки». Відсутність чіткого порядку реалізації повноважень стеження при здійсненні контррозвідки також не враховує посилені гарантії таємниці комунікацій для окремих категорій осіб, таких, як адвокати, журналісти, лікарі тощо.

²²⁵ Картка законопроекту: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243

Порівнюючи з попередньою версією законопроекту, нові положення не передбачають надання безпосереднього доступу органам СБУ до електронних комунікаційних мереж, вказуючи на потребу сприяння провайдерів в організації та проведенні контррозвідувального заходу, Закон України «Про телекомунікації»²²⁶ пропонується доповнити вимогою про те, що «технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації, що встановлюються для здійснення відповідними органами оперативно-розшукових та контррозвідувальних заходів, повинні відповідати стандартам і технічним регламентам, які розробляє уповноважений на це законом державний орган». Отже, технічні умови здійснення доступу до електронних комунікацій у будь-якому разі визначатимуться лише СБУ, і можливість автоматичного віддаленого доступу до перехоплення комунікацій законопроект не виключає.

4.2.3. Авторизація та нагляд у сфері стеження

За загальним правилом заходи стеження мають бути авторизовані судом, що надає відповідний дозвіл на їхнє застосування своєю ухвалою. Судовий нагляд відповідає вимогам щодо незалежності та безсторонності «арбітра». Проте ефективний нагляд у сфері стеження вимагає також наділення відповідних органів контролю достатніми повноваженнями для ефективного нагляду.

Суд, що здійснює нагляд, повинен мати доступ до усієї інформації, необхідної для реалізації його повноважень, незалежно від ступеня секретності, ретельно оцінювати відповідність принципам прав людини заходів стеження, мати повноваження скасувати чи припинити заходи стеження, якщо вони визнаються незаконними, а також вимагати видалення будь-якої інформації, отриманої за результатами таких заходів.

З огляду на перелічені стандарти, судовий нагляд за дотриманням прав людини при застосуванні заходів стеження в Україні потребує посилення.

Варто зауважити, що оцінити, чи справді суди ретельно оцінюють та балансують інтереси національної безпеки чи протидії кримінальним правопорушенням з інтересами поваги до приватності особи, на практиці дуже складно, оскільки відповідні судові ухвали зазвичай не є публічно доступними, про що зазначено в підрозділі 4.2.5.

Недоступна і статистична інформація щодо кількості поданих до судів клопотань про надання дозволів на застосування таких заходів та рівень їх «успішності» — кількість відмов та кількість наданих дозволів.

У будь-якому разі українські суди не мають повноважень за власною ініціативою скасовувати чи припиняти заходи стеження у разі виявлення ознак їх незаконності. Законодавство не регламентує навіть процедури розгляду питання про скасування відповідних заходів. В цілому процедура судового контролю на сьогодні фактично має формальний характер і не гарантує ефективного захисту від надмірного втручання в приватність особи.

²²⁶ Закон України «Про телекомунікації»: <https://zakon.rada.gov.ua/laws/show/1280-15>

Варто також зауважити, що наявна процедура не захищає від зловживання з боку працівників органів безпеки своїм доступом до комунікацій особи. Так у 2020 році щонайменше два обвинувальні вирoki ²²⁷ були ухвалені судами у справах, що стосувалися незаконного продажу даних щодо телефонних з'єднань абонентів, які були отримані шляхом використання спеціальних технічних засобів, призначених для негласного зняття інформації працівниками СБУ в рамках «контррозвідувальної перевірки».

4.2.4. Гарантії безпеки

Стандарти Ради Європи передбачають, що заходи стеження не повинні використовувати методи, що послаблюють системи шифрування чи цілісність комунікаційної інфраструктури, такі, як, наприклад, вбудовані вразливості та так звані «backdoors» в безпеці інформаційно-комунікаційних систем.

Українське законодавство не містить вимог щодо застосування подібних інструментів.

Водночас Закон України «Про телекомунікації» передбачає, що оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових та розвідувальних заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових та розвідувальних заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення.

Закон України «Про розвідку» визначає, що така система технічних засобів має надавати можливість автономного доступу до інформації у порядку, визначеному законодавством.

Закон України «Про електронні комунікації» ²²⁸, що був ухвалений на заміну Закону України «Про телекомунікації» та набуде чинності у 2022 році, також передбачає, що зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг має забезпечуватися єдиною системою технічних засобів, що використовується всіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством. При цьому, постачальник електронних комунікаційних послуг та/або мереж повинен забезпечити можливість під'єднання технічних засобів в точці для такого доступу в електронній комунікаційній мережі, визначеній постачальником електронних комунікаційних мереж та/або послуг.

На сьогодні відсутня встановлена законом процедура використання подібних технічних засобів. Тобто гарантії, необхідні для захисту таємниці комунікацій від свавільного втручання, наразі законом не передбачені.

²²⁷ Див. вирок у справі № 755/2110/20:

<https://reyestr.court.gov.ua/Review/91885873> та у справі № 755/1730/20: <https://reyestr.court.gov.ua/Review/88100538>

²²⁸ Закон України «Про електронні комунікації»: <https://zakon.rada.gov.ua/laws/show/1089-IX>

Саме тому встановлення обладнання з технічними характеристиками, що дозволяють безпосередній доступ представникам правоохоронних органів, створить можливості для безконтрольного втручання в електронні комунікації.

Проект закону про внесення змін до Закону України «Про службу безпеки України» № 3196-д пропонує наділити СБУ загальними повноваженнями впроваджувати устаткування, необхідне для здійснення заходів зі зняття інформації з транспортних телекомунікаційних мереж та здійснювати технічне регулювання засобів негласного отримання інформації та контроль за їхнім обігом. Такий підхід фактично виключає можливість незалежного контролю застосування відповідних технічних засобів та може призвести до засекречування навіть загальної інформації щодо функціональних можливостей встановленого обладнання. Наприклад, чи надаватимуть технічні засоби можливість втручатися у цілісність електронних комунікацій, блокувати чи іншим чином перешкоджати доступу користувачів до окремих вебресурсів тощо.

4.2.5. Доступ до інформації

Українське законодавство не гарантує належного рівня прозорості застосування заходів стеження. Закон України «Про доступ до публічної інформації» встановлює загальний обов'язок усіх суб'єктів владних повноважень оприлюднювати та надавати публічну інформацію у відповідь на запити та дозволяє обмежувати доступ до відомостей лише при дотриманні сукупності таких вимог («трискладовий тест»):

- 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;
- 2) розголошення інформації може завдати істотної шкоди цим інтересам;
- 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні ²²⁹.

Попри це, доступ до інформації про діяльність правоохоронних органів та органів безпеки залишається дуже обмеженим. Публічні звіти, що оприлюднюються такими державними органами, не містять навіть статистичної інформації щодо застосування заходів стеження.

Закон України «Про розвідку» вводить новий вид таємної інформації – «розвідувальну таємницю», що охоплює відомості та дані, отримані або створені розвідувальними органами України, розголошення яких «може завдати шкоди функціонуванню розвідки» і доступ до яких обмежено відповідно до цього закону в інтересах національної безпеки України.

²²⁹ Закон України «Про доступ до публічної інформації»: <https://zakon.rada.gov.ua/laws/show/2939-17>

У статті 46 цього закону передбачено, що інформація, яка належить до розвідувальної таємниці, не підлягає оприлюдненню та наданню на запити відповідно до Закону України «Про доступ до публічної інформації», а також на інші звернення та запити, крім випадків, прямо визначених законом. Для забезпечення доступу громадян до інформації про діяльність розвідувальних органів окремі відомості або дані, що належать до розвідувальної таємниці, можуть передаватися або оприлюднюватися за рішенням керівника розвідувального органу.

Закон «Про розвідку» фактично дозволив обмежувати доступ до інформації про діяльність розвідувального органу на розсуд його керівника, незалежно від дотримання вимог «трискладового тесту», що суперечить Конституції України та Конвенції. З цього приводу правозахисні організації навіть зверталися до Президента України з вимогою ветоувати ухвалений законопроект ²³⁰.

Подібний підхід пропонується у проекті Закону України «Про Службу безпеки України» № 3196-д. Голова СБУ чи уповноважені керівники отримують право відмовляти в наданні публічної інформації про діяльність СБУ, якщо вони «обґрунтовано» вважатимуть, що таке розкриття створить загрози «власній безпеці та безпеці оперативно-службової діяльності», незалежно від реальності шкоди та існування переважного суспільного інтересу в оприлюдненні.

Окремо слід звернути увагу на можливість особи отримати інформацію про застосування щодо неї заходів стеження.

Відповідно до Закону України «Про доступ до судових рішень» ²³¹ загальний доступ до ухвал, дозвіл на проведення негласної слідчої (розшукової) дії, про відмову в задоволенні клопотання про проведення негласної слідчої (розшукової) дії забезпечується через один рік після внесення таких ухвал до Єдиного державного реєстру судових рішень. Проте, інформація у реєстрі є знеособленою та не дає можливості ідентифікувати особу, щодо якої вживалися відповідні заходи. Крім цього, закон також передбачає, що у визначених законом випадках судові рішення про надання дозволу на проведення розвідувального заходу або про відмову в наданні такого дозволу, винесене в закритому судовому засіданні, не оприлюднюється і не публікується.

Закон «Про розвідку» передбачає, що розвідувальний орган має надавати інформацію щодо обмеження прав, свобод і законних інтересів особи виключно після завершення розвідувальних заходів, з якими було пов'язане таке обмеження, та за умови, що надання цієї інформації не створюватиме загрозу національній безпеці України.

Законопроект про внесення змін до Закону України «Про Службу безпеки України» № 3196-д передбачає, що ухвала про надання дозволу на проведення контррозвідувального заходу або про відмову в наданні такого дозволу до Єдиного державного реєстру судових рішень не вноситься, а відповідні матеріали мають зберігатися з дотриманням вимог законодавства про охорону державної таємниці.

²³⁰ Інститут масової інформації. Громадянське суспільство просить Зеленського ветоувати закон про розвідку: <https://imi.org.ua/news/gromadyanske-suspilstvo-prosyty-zelenskogo-vetuvaty-zakon-pro-rozvidku-i35254>

²³¹ Закон України «Про доступ до судових рішень»: <https://zakon.rada.gov.ua/laws/show/3262-15>

Хоча така вимога може бути виправданою на час проведення контррозвідальних заходів, після їх завершення, статус документів має бути переглянутий, а доступ до інформації відкритий відповідно до норм Закону України «Про доступ до публічної інформації».

Законопроект також містить колізії, пропонуючи безальтернативно обмежити право особи отримувати інформацію про передання її персональних даних за запитами органів, що здійснюють оперативно-розшукову або контррозвідальну діяльність та боротьбу з тероризмом, передбачаючи при цьому зміни до Закону «Про доступ до публічної інформації», за якими таке обмеження має діяти до прийняття рішення за результатами зазначеної діяльності або заходів.

Докладний порядок повідомлення особи про застосування щодо неї негласних слідчих дій передбачено лише Кримінальним процесуальним кодексом, який встановлює, що особи, конституційні права яких були тимчасово обмежені під час проведення негласних слідчих (розшукових) дій, а також підозрюваний, його захисник мають бути письмово повідомлені прокурором або за його дорученням слідчим про таке обмеження. Конкретний час повідомлення визначається з урахуванням наявності чи відсутності загроз для досягнення мети досудового розслідування, суспільної безпеки, життя або здоров'я осіб, які причетні до проведення негласних слідчих (розшукових) дій. Відповідне повідомлення про факт і результати негласної слідчої (розшукової) дії повинне бути здійснене протягом дванадцяти місяців з дня припинення таких дій, але не пізніше звернення до суду з обвинувальним актом (стаття 253 КПК України)²³².

²³² Кримінальний процесуальний кодекс України: <https://zakon.rada.gov.ua/laws/show/4651-17>

РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 4:

4.1. Захист персональних даних

**ВЕРХОВНІЙ РАДІ УКРАЇНИ,
КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ, КОМІТЕТУ
ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ,
УПОВНОВАЖЕНОМУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ:**

— узгодити національне законодавство із вимогами оновленої Конвенції та Загального регламенту ЄС із захисту даних та забезпечити створення незалежного наглядового органу у сфері захисту персональних даних з достатніми ресурсами для ефективного здійснення його повноважень.

**ПРЕЗИДЕНТУ УКРАЇНИ, КАБІНЕТУ МІНІСТРІВ УКРАЇНИ
ТА ВЕРХОВНІЙ РАДІ УКРАЇНИ:**

— підписати та ратифікувати Протокол змін до Конвенції про захист осіб у зв'язку з автоматизованим обробленням персональних даних (CETS No.223), що посилює вимоги до захисту персональних даних країнами Ради Європи та був відкритий до підписання 10 жовтня 2018 року.

**ВЕРХОВНІЙ РАДІ УКРАЇНИ, КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ
З ЦИФРОВОЇ ТРАНСФОРМАЦІЇ, КАБІНЕТУ МІНІСТРІВ УКРАЇНИ:**

— вдосконалити регулювання та функціонування державних реєстрів та баз даних, впровадивши належні нормативні, технічні та організаційні заходи задля гарантування безпечності даних та прозорих правил щодо порядку доступу до такої інформації.

**КАБІНЕТУ МІНІСТРІВ УКРАЇНИ,
МІНІСТЕРСТВУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ:**

— вжити заходів для узгодження оброблення персональних даних громадян, у зв'язку з протидією поширенню Covid-19, з національним законодавством та міжнародними стандартами, зокрема:

– обмежити доступ органів влади, залучених у протиепідемічні заходи, виключно до тих категорій персональних даних, які є мінімально необхідними для виконання їхніх повноважень, визначених законодавством. Це дозволить погодити наявну систему зі статтею 6 Закону України «Про захист персональних даних»: склад та зміст персональних даних мають бути відповідними, адекватними та не надмірними стосовно визначеної мети їх оброблення;

— забезпечити прозорість оброблення персональних даних у рамках взаємодії між МОЗ, Мінцифри та МВС. Зокрема, зобов'язати Мінцифри оприлюднити протоколи, що регламентують перелік відомостей, які передаються у межах інформаційного обміну з МВС та порядок такої інформаційної взаємодії на час введення карантину. Крім цього, забезпечити підготовлення та оприлюднення узагальнених звітів щодо інформації, отриманої від МОЗ та яким чином ці дані були використані, а також щодо кількості та підстав запитів від МВС на отримання інформації та результати їх опрацювання;

— оприлюднити інформацію щодо результатів використання додатку «Дій вдома» («Вдома») за весь час застосування карантинних обмежень;

— забезпечити відкритість у підготовленні актів, що регулюватимуть порядок знеособлення та знищення зібраної персональної інформації після завершення карантинних заходів та ін.

КАБІНЕТУ МІНІСТРІВ УКРАЇНИ:

— вжити заходів для узгодження своїх актів та актів центральних органів виконавчої влади із вимогами чинного законодавства у сфері захисту персональних даних, зокрема, в частині дотримання принципів оброблення персональних даних при наповненні, використанні та верифікації даних з державних реєстрів, а також доступу до інформації з таких реєстрів у процесі надання адміністративних послуг онлайн.

МІНІСТЕРСТВУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ:

— забезпечити прозорість та підзвітність на усіх етапах впровадження цифрових ініціатив, що дозволить оцінити дотримання принципів надійності, конфіденційності, безпеки даних, а також пропорційності обсягу даних меті їх оброблення при використанні інструментів цифрової ідентифікації особи.

МІНІСТЕРСТВУ ВНУТРІШНІХ СПРАВ УКРАЇНИ, ОФІСУ ГЕНЕРАЛЬНОГО ПРОКУРОРА, СЛУЖБІ БЕЗПЕКИ УКРАЇНИ:

— розробити та узгодити методичні рекомендації щодо розслідування справ, пов'язаних із незаконним поширенням персональних даних у мережі «Інтернет» та регулярно інформувати громадськість про вжиті заходи.

4.2. Стеження

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 (з участю правозахисників), з метою забезпечити відповідність пропонованих обмежень міжнародним стандартам законності, легітимності, пропорційності, виправданості та обґрунтованості обмежень.

ВЕРХОВНІЙ РАДІ УКРАЇНИ:

— розробити та ухвалити закон, що регулюватиме вимоги до перехоплення електронних комунікацій особи та відповідатиме вимогам передбачуваності, прозорості, пропорційності та обґрунтованості таких заходів, міститиме гарантії щодо обмеження дискреційних повноважень органів влади через встановлення категорій осіб, які можуть підлягати моніторингу, процедури проведення дій, граничної тривалості заходів, порядку аналізу, використання та зберігання отриманих даних, умов передачі даних іншим суб'єктам або їх знищення, вимог щодо безпечності технічних заходів для стеження та ін.

ВЕРХОВНІЙ РАДІ УКРАЇНИ, КОМІТЕТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ НАЦІОНАЛЬНОЇ БЕЗПЕКИ, ОБОРОНИ ТА РОЗВІДКИ:

— доопрацювати проєкт закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України № 3196-д та узгодити вимоги щодо доступу до персональних даних та здійснення заходів стеження з вимогами Конвенції про захист прав людини та основоположних свобод і практикою Європейського суду з прав людини.

МІНІСТЕРСТВУ ВНУТРІШНІХ СПРАВ УКРАЇНИ, ОФІСУ ГЕНЕРАЛЬНОГО ПРОКУРОРА, СЛУЖБІ БЕЗПЕКИ УКРАЇНИ:

— забезпечити щоквартальне оприлюднення статистичної інформації щодо кількості та видів заходів стеження, що були застосовані до громадян України за відповідний період;

— дотримуватися вимог Закону України «Про доступ до публічної інформації» при обмеженні доступу до відомостей, що стосується їхньої діяльності.

РОЗДІЛ 5. Дотримання прав людини в діяльності інтернет-посередників

5.1. Загальні вимоги

5.1.1. Державна політика у сфері діяльності інтернет-посередників

Питання регулювання діяльності інтернет-посередників досить гостро постало в Україні з початком агресії зі сторони Російської Федерації у 2014 році, після того, як соціальні мережі стали ще однією ареною боротьби. Сфера діяльності таких інтернет-посередників залишалася неврегульованою: містилися положення лише про діяльність провайдерів телекомунікацій (зокрема й інтернету) в Законі України «Про телекомунікації», але вони стосувалися винятково технічних аспектів їхньої діяльності, пов'язаних з ліцензуванням²³³; регулювання інших категорій інтернет-посередників не було передбачене. Частково це можна пов'язати з тим, що жоден зі значних світових посередників — зокрема соціальних медіа та платформ спільного доступу до відео — не має українського походження. Це означає, що будь-яке застосування механізмів регулювання зі сторони держави стикатиметься з питаннями наявності юрисдикції над такими посередниками та юрисдикційних конфліктів, попри тенденцію останніх років щодо застосування національного права до іноземних посередників, зокрема в Німеччині після прийняття NetzDG²³⁴. Додатковим фактором також слугує і загальна тенденція неврегульованості інтернету в Україні, що має як позитивні, так і негативні риси²³⁵.

Єдина норма, яка стосувалася змісту інформації, що передавалася мережами посередників, містилася у статті 39 Закону «Про телекомунікації» і передбачала обов'язок провайдерів телекомунікацій на підставі рішення суду обмежувати доступ своїх абонентів до ресурсів, через які здійснюється розповсюдження дитячої порнографії. Як вже зазначалося вище, таке технічне регулювання з 1 січня 2022 року буде замінено з набуттям чинності Закону України «Про електронні комунікації».

В цілому можна стверджувати, що Україна покладає на посередників мінімальний обсяг зобов'язань щодо дотримання ними у власній діяльності прав людини та щодо втручання таких посередників під впливом держави у їхню діяльність. Найзначніше протистояння у сфері, дотичній до прав людини та пов'язаній з технічним регулюванням, відбувається щодо обов'язку провайдерів за власні кошти встановити технічні засоби, за допомогою яких правоохоронні органи матимуть можливість здійснювати оперативно-розшукові та розвідувальні заходи.

²³³ Закон України «Про телекомунікації»: <https://zakon.rada.gov.ua/laws/show/1280-15>

²³⁴ Network Enforcement Act (Netzdurchsetzungsgesetz, NetzDG): <https://germanlawarchive.iuscomp.org/?p=1245>

²³⁵ Права людини онлайн: Порядок денний для України / Віта Володовська, Максим Дворовий — Київ: ГО «Лабораторія цифрової безпеки», 2019. — 56 с.: https://dslua.org/wp-content/uploads/2019/12/DRA_FINAL_UKR.pdf

Законопроекти, метою яких є модифікація відповідної норми в Законі України «Про телекомунікації», постійно з'являються на порядку денному парламенту. Останнім з них є проєкт закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів (№ 4004) ²³⁶. Відповідний обов'язок самостійно та власним коштом встановлювати обладнання для моніторингу та фільтрування контенту суперечить вимогам Директиви про електронну комерцію ²³⁷. Іншим аспектом регулювання діяльності посередників, згаданим вище, є вимоги до обмеження доступу до контенту в мережі та блокування сайтів.

Приклад гібридного регулювання діяльності інтернет-посередників, які не підпадають під категорію аудіовізуальних медіапослуг та платформ спільного доступу до відео, пропонує проєкт закону «Про медіа» ²³⁸. Національна рада України з питань телебачення і радіомовлення за ним може отримати право укладати з, за термінологією проєкту, платформами спільного доступу до інформації, меморандуми, якими може бути передбачено забезпечення вимог та обмежень щодо інформації, що поширюється на платформах спільного доступу до інформації та доступна на території України, механізми співрегулювання, співпраця у сфері протидії поширення дезінформації та забезпечення прозорості фінансування передвиборчої агітації на платформах, дотримання інших вимог виборчого законодавства України з боку користувачів.

Цей законопроект також врегульовує таку категорію посередників як платформи спільного доступу до відео, відповідно до вимог Директиви ЄС про аудіовізуальні медіапослуги, а також аудіовізуальні медіапослуги на замовлення (прикладом такого сервісу є «Нетфлікс»), регулювання яких буде більше прирівняне до аудіовізуальних медіа ²³⁹. Він передбачає такі обов'язки платформ, що перебувають під юрисдикцією України та підлягають реєстрації в Україні — і вони в цілому відповідають положенням Директиви:

- 1) розмістити умови користування сервісом платформи спільного доступу до відео на такій платформі та ознайомити користувачів платформи з такими умовами;
- 2) передбачити в умовах користування сервісом платформи спільного доступу до відео заборону на поширення користувацької інформації, яка порушує вимоги Закону, а також вимоги законодавства про авторське право та суміжні права;

²³⁶ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

²³⁷ *C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*. Judgment of the Court (Third Chamber) of 24 November 2011: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN>

²³⁸ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

²³⁹ *Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)*: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02010L0013-20181218&from=EN>

3) забезпечити перевіряння віку користувача перед отриманням ним доступу до інформації, що може зашкодити фізичному, моральному або ментальному розвитку дітей, забезпечити можливість встановлення систем батьківського контролю з метою захисту дітей від такої інформації;

4) надати користувачам дієвий механізм направлення звернень щодо інформації або матеріалів, що поширені на платформі спільного доступу до відео, забезпечити працездатність такого механізму, а також безперебійну роботу ефективного механізму реагування на звернення, повідомлення користувача про розгляд його звернень та механізм оскарження дій провайдера платформи спільного доступу до відео;

5) передбачити в умовах користування сервісом платформи спільного доступу до відео порядок реалізації права на відповідь або спростування недостовірної інформації та забезпечувати інформування користувачів про факт і зміст спростування або відповіді в описовій інформації до відповідного користувацького відео, а також шляхом повідомлення користувачів перед отриманням доступу до відповідної програми.

Варто згадати про ще одну законодавчу ініціативу — проєкт закону про внесення змін до Податкового кодексу України щодо скасування оподаткування доходів, отриманих нерезидентами у вигляді виплати за виробництво та/або розповсюдження реклами та удосконалення порядку оподаткування податком на додану вартість операцій з постачання нерезидентами електронних послуг фізичним особам (№ 4184) ²⁴⁰. За його положеннями, надавачі електронних послуг сплачуватимуть ПДВ у розмірі 20 % від оплатних послуг, наданих на митній території України. Податок буде непрямим, тобто його вартість включатиметься до ціни наданих послуг. Ті надавачі електронних послуг, які надаватимуть їх у сумі, що перевищуватиме 1 мільйон гривень, муситимуть зареєструватися як платники ПДВ.

5.1.2. Зобов'язання інтернет-посередників щодо дотримання прав людини

Через описані вище проблеми юрисдикційного характеру Україна не може вимагати від найбільших світових посередників, таких, як «Ютуб», «Фейсбук», «Твіттер», та інших дотримуватися прав людини у своїй діяльності та не має можливості змусити їх забезпечити дотримання відповідних прав. Саме тому ця сфера перебуває в ексклюзивному регулюванні самих платформ. Вимоги дотримання ними прав людини у своїй діяльності неодноразово зауважувалися різноманітними міжнародними організаціями, зокрема Радою Європи ²⁴¹ та спеціальними доповідачами з питань свободи вираження поглядів ООН, ОБСЄ та інших організацій ²⁴².

²⁴⁰ Картка законопроєкту: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70112

²⁴¹ Рекомендація Комітету Міністрів CM/Rec(2018)2 державам-членам про ролі та обов'язки Інтернет-посередників: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808c6192

²⁴² OSCE Representative on Freedom of the Media. Joint Declaration on Challenges to Freedom of Expression in the Next Decade: <https://www.osce.org/files/f/documents/9/c/425282.pdf>

Зокрема, останні у 2019 році у своїй Спільній декларації «Виклики для свободи вираження поглядів у наступному десятиріччі» наголосили на необхідності імплементації компаніями Керівних принципів ООН щодо бізнесу та прав людини²⁴³ з подальшим наглядом держави за такою імплементацією.

Цей документ передбачає, що держава має в законодавстві врегулювати обов'язок підприємств поважати у своїй діяльності права людини й надати керівні роз'яснення з цього приводу. У районах, вражених конфліктами, що є актуальним для України, 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 через їхню діяльність. 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.

Як згадувалося вище, проєкт закону «Про медіа» створює законодавчі підстави вимагати дотримання прав людини від однієї з категорій посередників — платформ спільного доступу до відео (прикладом якої є «Ютуб») ²⁴⁴. У разі, якщо така платформа зареєструється в Україні, вона мусить забезпечити створення низки механізмів реагування на контент та порушення прав людини таким контентом. Якщо такі механізми не будуть створені, відповідним платформам загрожуватиме штраф у розмірі від 10 до 50 мінімальних заробітних плат на день вчинення порушення.

5.2. Прозорість та підзвітність

5.2.1. Зобов'язання держави

Як вже зазначалося вище, в Україні станом на кінець 2020 року відсутні законодавчі закріплені механізми звернення правоохоронних та інших державних органів до посередників щодо видалення контенту. З огляду на це, немає законодавчих вимог і щодо публікації інформації про такі звернення. Тому очікувати на прозорість відповідних заходів, у разі їх здійснення, не варто. Заходи щодо блокування сайтів, які є протиправними, втілюються достатньо прозоро та з відповідною публікацією на сайті НКРЗІ та в Єдиному державному реєстрі судових рішень, про що згадувалося вище.

В окремих випадках органи влади справді публікують інформацію про власне звернення до посередників. Так, Служба безпеки України 9 жовтня 2020 року повідомила про власне звернення до «Google LLC» та «Apple Inc» щодо поширення на їхніх сервісах «Play Market» і «App Store» мобільних додатків заблокованих в Україні сайтів ²⁴⁵. Також під час низки публічних дискусій лунала інформація про наявність у «Фейсбук» контактів з правоохоронними органами.

²⁴⁵ Служба безпеки України ініціювала блокування заборонених російських додатків на електронних майданчиках Google та Apple: <https://www.facebook.com/SecurSerUkraine/posts/2833103260252994/>

Попри перші спроби врегулювати діяльність посередників в Україні проектом закону «Про медіа» законодавець вирішив не включати до нього зобов'язань з прозорості. Тому навіть у разі прийняття проекту найближчим часом, публікація інформації про обмеження прав людини, яке здійснюють посередники, буде їх добровільною практикою, а не оприлюднення такої інформації не призводитиме до жодних санкцій.

5.2.2. Зобов'язання інтернет-посередників

Прозорість інтернет-посередників можна розглядати в кількох аспектах. По-перше, вони мають публікувати свої правила використання та політики щодо регулювання контенту. По-друге, вони мають надавати суттєву інформацію про використання алгоритмів та автоматизованих методів оброблення даних у процесі їх діяльності. По-третє, вони мають публікувати звіти з прозорості, що охоплюють інформацію про взаємодію з державними органами щодо надання інформації про користувачів, видалення контенту, а також впровадження власних політик щодо обмежень поширення певних категорій інформації ²⁴⁶.

Стосовно першого аспекту, то найбільші посередники, такі як «Фейсбук» ²⁴⁷, «Інстаграм» як окремий сервіс від «Фейсбук» ²⁴⁸, «Гугл» ²⁴⁹ та «Ютуб» як окремий сервіс від «Гугл» ²⁵⁰, мають переклади умов використання українською мовою. У «Фейсбук» перекладені також і низка політик, зокрема стандарти спільноти, що регулюють контент ²⁵¹. Так само вони перекладені й у «Інстаграм» ²⁵². У «Твіттер» умови та положення є лише англійською або російською мовами; доступний переклад правил «Твіттера» українською ²⁵³. Майже всі політики перекладені в сервісів «Гугл». «ТікТок» же, на противагу, не має перекладу користувацького договору та жодних політик українською ²⁵⁴.

Прозорість алгоритмів посередників є наріжним каменем для розуміння того, яким чином відповідні сайти та компанії впливають на нашу свідомість та здатні відображати це в нашій стрічці.

²⁴⁶ Рекомендація Комітету Міністрів CM/Rec(2018)2 державам-членам про ролі та обов'язки Інтернет-посередників: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808c6192

²⁴⁷ Умови використання Facebook: <https://www.facebook.com/legal/terms>

²⁴⁸ Умови використання Instagram: <https://help.instagram.com/581066165581870>

²⁴⁹ Загальні положення та умови Google: <https://policies.google.com/terms?hl=uk>

²⁵⁰ Правила та безпека Youtube: <https://www.youtube.com/intl/uk/about/policies/#community-guidelines>

²⁵¹ Стандарти спільноти Facebook: <https://www.facebook.com/communitystandards/>

²⁵² Правила спільноти Instagram: [https://www.facebook.com/help/instagram/477434105621119/?helpref=hc_fnav&bc\[0\]=%D0%94%D0%BE%D0%B2%D1%96%D0%B4%D0%BA%D0%B0%20Instagram&bc\[1\]=%D0%A6%D0%B5%D0%BD%D1%82%D1%80%20%D0%BA%D0%BE%D0%BD%D1%84%D1%96%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%81%D1%82%D1%96%20%D1%82%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8](https://www.facebook.com/help/instagram/477434105621119/?helpref=hc_fnav&bc[0]=%D0%94%D0%BE%D0%B2%D1%96%D0%B4%D0%BA%D0%B0%20Instagram&bc[1]=%D0%A6%D0%B5%D0%BD%D1%82%D1%80%20%D0%BA%D0%BE%D0%BD%D1%84%D1%96%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%81%D1%82%D1%96%20%D1%82%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8)

²⁵³ Правила Twitter: <https://help.twitter.com/uk/rules-and-policies/twitter-rules>

²⁵⁴ Пользовательское соглашение Tiktok: <https://www.tiktok.com/legal/terms-of-use?lang=ru-RU>

Найчастіше такі алгоритми захищаються як об'єкти авторського права, а тому посередники неохоче розкривають власні таємниці. Прозорим є пошуковий алгоритм «Гугл», в якому компанія надала перелік факторів, що впливають на видачу матеріалів у пошуку²⁵⁵. Чітку інформацію про формування власного фіду надає мережа «Твіттер»²⁵⁶. У 2020 році мережа «ТікТок» у своєму офіційному блозі також описала частину інформації про те, на підставі чого формується стрічка перегляду відео²⁵⁷. Щодо «Ютуб», то існує стаття працівників «Гугл», у якій вони пояснюють використання нейромереж для ранжування контенту в мережі²⁵⁸. Втім, за даними дослідників, з того часу алгоритми мережі змінилися²⁵⁹.

Позитивом є те, що всі згадані вище платформи регулярно (двічі на рік) та належно публікують звіти про прозорість. На момент проведення аналізу в рамках цього дослідження були опубліковані звіти лише за перші 6 місяців 2020 року. За їхніми даними можна побачити, що до мережі «ТікТок» Україна запитів у цей період не надсилала²⁶⁰, тоді як до мережі «Твіттер» була висунута одна правова вимога щодо видалення контенту (без уточнення того, від приватної особи чи від держави), що не була задоволена²⁶¹. Запитів від державних органів щодо отримання інформації у звітному періоді «Твіттер» не отримував²⁶².

«Фейсбук» отримав 52 запити від України на отримання інформації про 163 користувачів, з яких у 58 % випадків надав якусь частину інформації. Також було отримано 9 запитів на збереження інформації²⁶³. «Фейсбук» видалив один пост внаслідок приватного сповіщення про дифамацію з України²⁶⁴.

«Гугл» отримав 29 запитів на розкриття інформації про 46 облікових записів. Протягом першого півріччя 2020 року «Гугл» також отримав 2 запити на збереження інформації. У їхньому звіті про прозорість окремо вказано також і те, що в цей період 1 запит був отриманий через офіційні дипломатичні канали — зокрема через механізми міжнародної правової допомоги²⁶⁵.

²⁵⁵ Google. Як працюють алгоритми пошуку: <https://www.google.com/search/howsearchworks/algorithms/>

²⁵⁶ About your Twitter timeline: <https://help.twitter.com/en/using-twitter/twitter-timeline>

²⁵⁷ How TikTok recommends videos #ForYou: <https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you>

²⁵⁸ Paul Covington. Jay Adams. Emre Sargin. Deep Neural Networks for YouTube Recommendations: <https://static.googleusercontent.com/media/research.google.com/uk/pubs/archive/45530.pdf>

²⁵⁹ Paige Cooper. How Does the YouTube Algorithm Work? A Guide to Getting More Views. Hootsuite. 18 August 2020: <https://blog.hootsuite.com/how-the-youtube-algorithm-works/>

²⁶⁰ TikTok Transparency Report 2020 H1: <https://www.tiktok.com/safety/resources/transparency-report-2020-1?lang=en>

²⁶¹ Twitter Transparency — Removal Requests, January-June 2020: <https://transparency.twitter.com/en/reports/removal-requests.html#2020-jan-jun>

²⁶² Twitter Transparency — Information Requests, January-June 2020: <https://transparency.twitter.com/en/reports/information-requests.html#2020-jan-jun>

²⁶³ Facebook Transparency — Requests Ukraine: <https://transparency.facebook.com/government-data-requests/country/UA>

²⁶⁴ Facebook Transparency — Content Restrictions Ukraine: <https://transparency.facebook.com/content-restrictions/country/UA>

²⁶⁵ Google. Глобальні запити щодо особистих даних користувачів. Україна: https://transparencyreport.google.com/user-data/overview?user_data_produced=authority:UA;series=compliance&lu=dlr_request&user_requests_report_period=series:requests,accounts;authority:UA;time:Y2020H1&legal_process_breakdown=expanded:0&dlr_requests=authority:UA;time

Окремо «Гугл» веде звіт щодо звернення державних органів щодо видалення контенту. За їхніми даними, в зазначений період 45 запитів щодо 242 елементів було отримано від України. З цих елементів 230 стосувалися наклепу і лише 5 – питань національної безпеки, а до 222 з них обмеження застосовувалися за рішенням суду. Видалено з юридичних причин лише 55 елементів – 22,7 % від загального числа оскаржених. «Гугл» навіть подає один з прикладів таких запитів, який компанія не задовольнила: «Ми отримали від колишнього головного прокурора Києва запит на основі ухвали суду на видалення статті, у якій ідеться про те, що він із колегою вимагали гроші від бізнесменів в обмін на закриття кримінальних справ» ²⁶⁶.

«Гугл» окремо публікує щоквартальні звіти щодо видалення контенту, який не відповідає правилам спільноти «Ютуб» ²⁶⁷. За їх допомогою можна виявити скільки відео було видалено в українському сегменті та з яких причин, хоча більшість відео зникає внаслідок процедури автоматичного виявлення. Подібний щоквартальний звіт, без деталізації за країнами, однак з поясненнями щоквартальних трендів, публікує «Фейсбук» ²⁶⁸, а піврічний – «Твіттер» ²⁶⁹. Дані про впровадження власних політик щодо контенту висвітлює і «ТікТок» ²⁷⁰.

У контексті прозорості окремо варто наголосити і на прозорості політичної реклами. У 2020 році в Україні відбувалися місцеві вибори, на яких частина посередників була залучена у виборчих кампаніях кандидатів. «Фейсбук» за допомогою власної бібліотеки реклами ²⁷¹ дозволяє відстежувати відповідні витрати. За даними «Опори», протягом кампанії до місцевих виборів на платформі було опубліковано понад 90 тисяч рекламних оголошень політичного змісту ²⁷². Відповідна політика прозорості «Гугл» поки що не поширюється на Україну ²⁷³, тоді як «Твіттер» заборонив розповсюдження політичної реклами в себе на платформі у 2019 році ²⁷⁴.

²⁶⁶ Google. Запити на видалення контенту від державних установ. Україна:

https://transparencyreport.google.com/government-removals/by-country/UA?hl=uk&country_item_amount=group_by:requestors;period:Y2020H1;authority:UA&lu=country_item_amount&country_request_amount=group_by:totals;period:Y2020H1;authority:UA&country_request_explore=period:Y2020H1;authority:UA

²⁶⁷ Youtube. Контроль відповідності правилам спільноти YouTube:

https://transparencyreport.google.com/youtube-policy/removals?videos_by_country=period:Y2020Q4;region:&lu=content_by_flag&content_by_flag=period:Y2020Q4;exclude_automated:human_only

²⁶⁸ Facebook Community Standards Enforcement Report: <https://transparency.facebook.com/community-standards-enforcement>

²⁶⁹ Twitter Transparency – Rules Enforcement, January – June 2020:

<https://transparency.twitter.com/en/reports/rules-enforcement.html#2020-jan-jun>

²⁷⁰ TikTok Transparency Report 2020 H1: <https://www.tiktok.com/safety/resources/transparency-report-2020-1?lang=en>

²⁷¹ Facebook Ad Library:

https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=UA

²⁷² Опора. Особливості політичної реклами у соціальній мережі Facebook на місцевих виборах 2020 (5 вересня – 20 жовтня): <https://danivvyboriv.net/archives/1779>

²⁷³ Політична реклама в Google: <https://transparencyreport.google.com/political-ads/home>

²⁷⁴ Twitter. Political content policy: <https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html>

5.3. Захист свободи вираження поглядів

5.3.1. Зобов'язання держави

Проблематика блокування контенту в Україні вже підіймалася у розділах 2.2.1 та 2.2.2 цього звіту. Можна стверджувати, що наявні в українському законодавстві механізми блокування вебсайтів та обмеження доступу до контенту в цілому відповідають трискладовому тесту обмеження прав людини. Декілька механізмів, які застосовуються на практиці, зокрема використання Закону України «Про санкції» та арешту майнових прав інтелектуальної власності, які виникають у користувачів мережі «Інтернет» при використанні вебсайтів, не має підстав у законодавстві та порушує вимоги до передбачуваності таких обмежень законом. Також українське законодавство не містить чітких визначень щодо того, які категорії контенту є забороненими для поширення у мережі.

З прийняттям Закону України «Про електронну комерцію» у 2015 році та подальших змін до нього у 2017 році більше врегулювалось і питання імунітету посередників²⁷⁵. Положення цього закону були покликані імплементувати положення Директиви ЄС про електронну комерцію²⁷⁶. Серед іншого, саме її положеннями закріплюється, що постачальники послуг хостингу (до яких відносяться, зокрема, соціальні мережі) звільняються від відповідальності за розміщений ними контент у разі, якщо вони не мають відомостей про протиправну діяльність та контент або про обставини, з яких впливає очевидний протиправний характер такої діяльності («actual knowledge») або ж, отримавши відомості про таку діяльність та контент, діють достатньо оперативно для видалення або обмеження доступу до нього («expeditious removal»). Ці положення відображені в частині четвертій статті 9 Закону «Про електронну комерцію»²⁷⁷. Окрім того, прийнятий Закон України «Про електронні комунікації» прямо посилається на ці положення у контексті згадок про відповідальність провайдерів електронних комунікаційних послуг за зміст переданої інформації²⁷⁸. Втім, судова практика застосування цієї норми протягом 2020 року в Єдиному державному реєстрі судових рішень відсутня, що може свідчити про загальне належне застосування цієї норми і відсутність судових суперечок щодо того, що може вважатися належним повідомленням про протиправний характер інформації та які дії є достатньо швидкими для обмеження доступу до інформації.

²⁷⁵ Закон України «Про електронну комерцію»: <https://zakon.rada.gov.ua/laws/show/675-19>

²⁷⁶ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'): <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>

²⁷⁷ Закон України «Про електронну комерцію»: <https://zakon.rada.gov.ua/laws/show/675-19>

²⁷⁸ Закон України «Про електронні комунікації»: <https://zakon.rada.gov.ua/laws/show/1089-IX>

Законодавство України не передбачає заборони встановлювати для посередників загальний обов'язок контролю за контентом, до якого вони надають доступ. Таке зобов'язання передбачене статтею 15 згаданої вище Директиви ЄС про електронну комерцію і слугує додатковою гарантією захисту платформ²⁷⁹.

Чинне законодавство лише в загальних рисах розмежовує різні категорії посередників та різний ступінь їхньої відповідальності у статті 9 Закону України «Про електронну комерцію», якою передбачене розрізнення між «постачальником послуг проміжного характеру в інформаційній сфері, що надає послуги проміжного (тимчасового) зберігання інформації, наданої одержувачем послуги, з єдиною метою — покращити подальшу передачу інформації іншим одержувачам послуги на їхню вимогу» («кешинг» за термінологією статті 13 Директиви) та «постачальником послуг проміжного характеру в інформаційній сфері, що надає послуги постійного зберігання інформації на запит одержувача послуг хостингу» («хостинг» за термінологією статті 14 Директиви)²⁸⁰. Діяльність «mere conduit» регулюється Законом України «Про телекомунікації» та Законом України «Про електронні комунікації», що замінить його з 2022 року. Як вже зазначалося вище, проєкт закону «Про медіа» встановлює додаткове розрізнення та різноманітні способи регулювання для таких категорій посередників як платформи спільного доступу до відео, платформи спільного доступу до інформації та аудіовізуальні медіапослуги на замовлення²⁸¹.

5.3.2. Зобов'язання інтернет-посередників

Інтернет-платформи мають власні розгалужені політики щодо обмеження доступу до протиправного контенту. Вони опубліковані на платформах, є частиною умов використання сервісів тих чи інших посередників, а їх виконання забезпечується сукупністю людських та автоматизованих ресурсів, роботу яких має забезпечити посередник. Постає питання того, наскільки відповідні політики та їх впровадження відповідають вимогам у сфері захисту прав людини, Керівним принципам ООН з прав людини та бізнесу та Міжнародним пактам про захист прав людини відповідно.

У 2018 році міжнародна організація «Article 19» проаналізувала внутрішні політики найбільших посередників («Фейсбук», «Ютуб», «Твітер» та «Гугл») щодо їх відповідності стандартам захисту прав людини та свободи вираження поглядів²⁸². На думку її експертів, категорії контенту, позначені як заборонені у внутрішніх політиках, є надто широкими у всіх сферах, від мови ворожнечі й терористичного контенту до контенту, що порушує приватність, та фейкових новин. Незрозумілими для експертів були механізми використання алгоритмів та штучного інтелекту для протидії шкідливому контенту.

²⁷⁹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'): <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>

²⁸⁰ Закон України «Про електронну комерцію»: <https://zakon.rada.gov.ua/laws/show/675-19>

²⁸¹ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

²⁸² Article 19. Side-stepping rights: Regulating speech by contract. Policy brief: <https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB-v2.pdf>

Також експерти «Article 19» наголосили і на тому, що санкції за порушення політик користувачами часто залишаються нечіткими. Саме тому незрозуміло, який захід реагування і в якому випадку буде застосований до того чи іншого порушення, вчиненого користувачем. «Article 19» все ж дійшла висновку про те, що в широкому сенсі стандарти, які застосовуються «Фейсбук», «Ютуб» та «Твіттер», відповідають міжнародним стандартам у сфері захисту посередників.

«Ютуб» має велику кількість політик регулювання типів контенту від безпеки дітей до інформації щодо Covid-19²⁸³. Станом на 2020 рік вони мали і найчіткішу систему санкцій: за перше порушення автор каналу отримував попередження, за друге — страйк. При страйку автор каналу на один тиждень позбавляється низки прав на платформі, зокрема — права завантажувати нові відео. Другий страйк виноситься авторові каналу в тому разі, якщо він допускає порушення ще раз протягом 90 днів після отримання першого; тоді заборона на завантаження контенту триватиме два тижні. При трьох страйках канал підлягає видаленню. Кожен страйк з каналу знімається через 90 днів з дня його накладення²⁸⁴.

Стандарти спільноти «Фейсбук» досить детально пояснюють різноманітні категорії забороненого контенту і намагаються розтлумачити користувачам, що не варто розміщувати. Проте санкції за порушення вимог щодо контенту є невизначеними. Так, «Фейсбук» зазначає, що наслідки за порушення стандартів спільноти варіюватимуться залежно від природи порушення: когось можуть попередити за перше порушення, комусь обмежити право публікувати дописи, а іншим — деактивувати профіль²⁸⁵. Такими самими невизначеними є і заходи, які застосовуватиме до користувачів при порушеннях «Інстаграм»²⁸⁶.

«Твіттер» описує низку факторів, на які зважатиме при застосуванні санкцій до порушника правил. Цими факторами є те, на кого спрямований контент або поведінка, чи була подана скарга особою, яку зачіпає контент, або ж третьою особою, якою є історія особи, що порушила правила, яким є порушення та те, наскільки контент може слугувати темою легітимного суспільного інтересу. Також порядок застосування санкцій є нечітким: «Твіттер» може спочатку вказати користувачеві на протиправність його посту і попросити видалити цей пост перед створенням подальшого контенту. Наступні порушення можуть спричинити тимчасове призупинення можливості розміщувати твіти або ж верифікацію власності акаунта. Видалення акаунта є винятковим заходом²⁸⁷.

²⁸³ Youtube Community Guidelines:

<https://www.youtube.com/howyoutubeworks/policies/community-guidelines/#community-guidelines>

²⁸⁴ Youtube Community Guidelines strike basics: <https://support.google.com/youtube/answer/2802032>

²⁸⁵ Facebook Community Standards: <https://www.facebook.com/communitystandards/>

²⁸⁶ Instagram Community Guidelines: <https://www.facebook.com/help/instagram/477434105621119/>

²⁸⁷ Twitter. Our approach to policy development and enforcement philosophy: <https://help.twitter.com/en/rules-and-policies/enforcement-philosophy>

Стандарти спільноти в «ТікТок» загалом є менш детальними щодо дефініцій протиправного контенту. Так само нечіткими є і положення застосування санкцій. Вказується, що акаунт може бути призупинено або забанено — зокрема через повторні та грубі порушення, такі, як заклики до ворожнечі чи жорстокого екстремізму ²⁸⁸.

В українському контексті загалом можна згадати масове блокування українських користувачів у «Фейсбук» 2015 ²⁸⁹ та 2018 років ²⁹⁰, за різноманітні вислови, переважно пов'язані з агресією Російської Федерації проти України. Тоді «Фейсбук» пояснював це порушенням стандартів спільноти, однак не наводив детальної аргументації щодо випадків блокування. Подібної практики в Україні у 2020 році не відбувалося — однак можна згадати випадок видалення мережі акаунтів, помічених у скоординованій неавтентичній поведінці під час виборів 2019 року та пов'язаних з рекламною агенцією «Postmen». Усього було видалено 65 акаунтів та 32 сторінки у «Фейсбук» та 5 акаунтів у «Інстаграм»; які витратили на рекламу майже 2 мільйони доларів ²⁹¹.

5.4. Захист конфіденційності та захист даних

5.4.1. Зобов'язання держави

Попри те, що ключові інтернет-посередники прямо не підпадають під юрисдикцію України, держава має вживати усіх належних заходів задля гарантування прав на захист персональних даних громадян при використанні соціальних мереж чи інших платформ.

Насамперед такі заходи мають охоплювати встановлення чітких законодавчих рамок щодо принципів оброблення персональних даних (законності, справедливості та прозорості, обмеження мети, мінімізації даних, точності, обмежень за часом зберігання і захисту даних, зокрема цілісності й конфіденційності) і гарантій дотримання прав суб'єктів даних в Україні у повній відповідності до Конвенції 108 з урахуванням останніх змін ²⁹².

Крім цього, національне законодавство повинне належно врегулювати підстави та порядок звернення державних органів до інтернет-посередників щодо надання доступу до інформації про користувачів.

²⁸⁸ Tiktok Community Guidelines: <https://www.tiktok.com/community-guidelines>

²⁸⁹ Олександр Савицький. Ганна Бєднова. Чому у Facebook блокують відомих українців? Deutsche Welle. 23 березня 2015: <https://www.dw.com/uk/чому-у-facebook-блокують-відомих-українців/a-18468517>

²⁹⁰ Український тиждень. Юрій Лапаєв. Бан в одні ворота. За що українців блокують у Facebook. 21 квітня 2018 року: <https://tyzhden.ua/Society/212651>

²⁹¹ Nathaniel Gleicher. Removing Coordinated Inauthentic Behavior: <https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/>

²⁹² Див. Розділ 4.1.

Будь-яка вимога чи запит органів державної влади на адресу інтернет-посередників щодо надання доступу, збору чи перехоплення персональних даних їхніх користувачів, зокрема для цілей кримінального судочинства або будь-яких інших заходів, що суперечать праву на недоторканність приватного життя, мають бути передбачені законом, здійснюватися для досягнення законної мети та бути пропорційними та обґрунтованими.

На сьогодні національне регулювання заходів стеження (доступу до комунікацій особи чи іншої інформації про користувачів) встановлює порядок отримання інформації від операторів телекомунікацій, тоді як вимоги та порядок звернення до міжнародних інтернет-посередників фактично не визначені.

5.4.2. Зобов'язання інтернет-посередників

Інтернет-посередники зобов'язані виконувати вимоги щодо законного оброблення персональних даних користувачів, зокрема отримувати поінформовану згоду користувачів на використання їхніх персональних даних, що охоплює інформування про цілі та обсяги оброблення даних, права користувачів тощо. Інтернет-посередники повинні надавати користувачам право на відкликання згоди та на видалення їхніх персональних даних. Виконання зазначених вимог великою мірою залежить від забезпечення посередниками вимог прозорості, про які йшлося вище. Міжнародні інтернет-посередники такі, як «Фейсбук», «Ґґл» та «Твіттер», в цілому виконують вимоги щодо належного оброблення та захисту персональних даних в Україні, зокрема з огляду на поширення на них регулювання ЄС у сфері захисту даних. Проте здійснення відстеження та профайлінгу користувачів не є повністю прозорим.

У 2020 році українські державні органи неодноразово зверталися до найпопулярніших інтернет-платформ із запитом щодо отримання інформації про користувачів.

Так, за перше півріччя 2020 року «Фейсбук» отримав 52 запити від України на отримання інформації про 163 користувачів, з яких у 58 % випадків надав якусь частину даних. З цих запитів 9 базувалися на правових вимогах, решта були екстреними (тобто стосувалися справ, пов'язаних із потенційною загрозою для дитини або небезпекою смерті чи серйозного фізичного ушкодження будь-якої особи)²⁹³. «Ґґл» отримав 29 запитів на розкриття інформації про 46 облікових записів. З них 21 запит стосувався екстрених ситуацій, а 8 спиралося на інші правові вимоги. У 38 % випадків було надано деякі дані, причому жодного разу за правовою вимогою²⁹⁴.

Дані звітів про прозорість свідчать про те, що за загальним правилом, посередники не розкривають персональні дані у відповідь на будь-який запит, а проводять оцінювання щодо його відповідності законодавству, можуть відмовити в наданні даних чи вимагати уточнення занадто широких вимог.

²⁹³ Facebook Transparency – Requests Ukraine: <https://transparency.facebook.com/government-data-requests/country/UA>

²⁹⁴ Google. Глобальні запити щодо особистих даних користувачів. Україна: https://transparencyreport.google.com/user-data/overview?user_data_produced=authority:UA;series=compliance&lu=dlr_request&user_requests_report_period=series:requests,accounts;authority:UA;time:Y2020H1&legal_process_breakdown=expanded:0&dlr_requests=authority:UA;time

Разом з тим звіти не містять достатньої інформації (наприклад, узагальнені дані про підстави запитів, їх обґрунтування, причини відмови в наданні інформації тощо) для проведення оцінювання забезпечення принципів законності та необхідності в демократичному суспільстві при розгляді таких запитів.

5.5. Доступ до ефективних засобів правового захисту

5.5.1. Зобов'язання держави

Без права на доступ до ефективних засобів правового захисту зобов'язання держави з захисту прав людини в інтернеті є неповним, адже користувачі не отримуватимуть змоги оскаржити протиправні дії посередників. У трикутнику регулювання «держава-користувач-посередник» саме державні механізми розв'язання спорів мають ставити крапку, якщо врегулювання відносин між користувачем та посередником завершилося нічим.

В українському контексті варто нагадати, що право на справедливий судовий розгляд гарантоване Конституцією України²⁹⁵ та подальшими рішеннями Конституційного Суду України: суд не може відмовити у правосудді, якщо громадянин України, іноземець, особа без громадянства вважають, що їх права і свободи порушені або порушуються, створено або створюються перешкоди для їх реалізації або мають місце інші ущемлення прав та свобод²⁹⁶. Теоретично це має означати, що будь-який спір, який виникатиме з дій посередників щодо користувачів на території України має бути розглянутий українськими судами. Оскільки цей позов стосуватиметься захисту прав споживачів, то за вимогами Цивільного процесуального кодексу вони можуть пред'являтися і за зареєстрованим місцем проживання споживачів²⁹⁷ — тож потенційно позови проти технологічних гігантів щодо, наприклад, неправомірності видалення контенту можуть розглядатися судами загальної юрисдикції. Втім, існують серйозні проблеми з загальною легітимністю судового розв'язання спорів: судам в Україні загалом не довіряє або скоріше не довіряє 78 % відсотків населення держави²⁹⁸.

Проект закону «Про медіа» пропонує для такої категорії посередників, як платформа спільного доступу до відео, закріпити зобов'язання створити дієвий механізм направлення звернень щодо інформації або матеріалів, що поширені на платформі, забезпечити працездатність такого механізму, а також безперебійне реагування на звернення, повідомлення користувача про розгляд його звернень та оскарження дій провайдера такої платформи²⁹⁹.

²⁹⁵ Конституція України: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

²⁹⁶ Рішення Конституційного Суду України № 9-зп від 25 грудня 1997 року у справі за конституційним зверненням громадян Проценко Раїси Миколаївни, Ярошенко Поліни Петрівни та інших громадян щодо офіційного тлумачення статей 55, 64, 124 Конституції України (справа за зверненнями жителів міста Жовті Води): <https://zakon.rada.gov.ua/laws/show/v009p710-97>

²⁹⁷ Цивільний процесуальний кодекс України: <https://zakon.rada.gov.ua/laws/show/1618-15>

²⁹⁸ Центр Разумкова. Звіт за результатами дослідження «Ставлення громадян України до судової системи». 2020: <https://rm.coe.int/zvitsud2020/1680a0c2d7>

²⁹⁹ Картка законопроекту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

У разі прийняття цього законопроекту, платформи, що перебуватимуть під юрисдикцією України, повинні створити відповідний механізм під загрозою застосування санкцій.

Україна досить активно рухається у напрямку використання інструментів медіаграмотності для популяризації заходів з захисту прав людини в інтернеті. Протягом 2020 року Міністерство цифрової трансформації України записало низку освітніх серіалів, які стосуються цифрових прав³⁰⁰, аби користувачі могли дізнатися про те, як захищати власні персональні дані, про безпеку дітей в інтернеті, зокрема і в соціальних мережах, тощо.

5.5.2. Зобов'язання інтернет-посередників

Здебільшого посередники створили на власних платформах різноманітні механізми розв'язання спорів та повідомлень про протиправність контенту. За допомогою цих механізмів користувач може повідомити про поширення, наприклад, мови ворожнечі чи терористичного контенту, а сам інтернет-посередник – відреагувати на порушення. У той самий час, як зазначила організація «Article 19», відповідним механізмам «Фейсбук», «Ютуб», «Твітер» та «Гугл» бракує гарантій справедливого розгляду: зокрема, вони часто не пояснюють причини видалення контенту користувачам, не надають можливості пояснити власну позицію щодо оскаржуваного контенту користувачу, що його розмістив, а також не створили механізмів апеляції рішення, прийнятого посередником³⁰¹ (за винятком «Твітер», де можна подати апеляцію на призупинення акаунта).³⁰² Так само посередники не зазначають часових строків прийняття рішення щодо оскаржуваного контенту, а тому в окремих випадках прийняття рішень щодо сторінок, про які було повідомлено, триває роками.

Інтернет-посередники додатково захищають себе і юрисдикційними положеннями у власних правилах користування сервісами. Лише «Фейсбук» передбачає, що споживачі можуть позиватися до компанії щодо тлумачення правил користування сервісами за місцем проживання.³⁰³ Користувачі «Твітер» матимуть йти за захистом своїх прав до Сан-Франциско у США³⁰⁴, а користувачі «ТікТок» – звертатися до арбітражного суду в Сингапурі³⁰⁵. «Гугл» та «Ютуб» передбачають розгляд справ у Каліфорнії, крім випадків, коли чинне місцеве законодавство перешкоджає розв'язанню цих спорів у суді штату Каліфорнія³⁰⁶.

³⁰⁰ Дія. Цифрова освіта. Освітні серіали: <https://osvita.diiia.gov.ua/courses>

³⁰¹ Article 19. Side-stepping rights: Regulating speech by contract. Policy brief: <https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB-v2.pdf>

³⁰² Twitter Help Center. Appeal an account suspension or locked account: <https://help.twitter.com/forms/general>

³⁰³ Умови надання послуг Facebook: <https://www.facebook.com/terms.php>

³⁰⁴ Twitter Terms of Service: <https://twitter.com/en/tos#update>

³⁰⁵ TikTok Terms of Service: <https://www.tiktok.com/legal/terms-of-use?lang=en#terms-row>

³⁰⁶ Загальні положення та умови Google: <https://policies.google.com/terms?hl=uk>

Станом на 2020 рік механізм апеляцій щодо страйків також з'явився в «Ютуб»³⁰⁷ та у «ТікТок», що під час проведення дослідження у 2018 році ще не набув широкої популярності.³⁰⁸ Проте чи не найбільшим здобутком у сфері дотримання права на доступ до ефективних засобів правового захисту у 2020 році серед інтернет-посередників став запуск «Фейсбук» Oversight Board.³⁰⁹ Цей експертний орган уповноважений переглядати рішення модераторів та алгоритмів «Фейсбук» та «Інстаграм» щодо обмеження доступу до контенту, залучаючи авторів контенту, незалежних експертів та збираючи коментарі третіх сторін. Рішення прийматиметься більшістю від експертів, що є членами органу. У рішеннях міститиметься мотивація та рекомендації щодо модифікації в майбутньому політик «Фейсбук» щодо контенту.³¹⁰ Публікація перших рішень очікується на початку 2021 року та відбуватиметься на сайті органу.

³⁰⁷ Youtube. Appeal Community Guidelines Actions: <https://support.google.com/youtube/answer/185111?hl=en>

³⁰⁸ TikTok. Account Safety: <https://support.tiktok.com/en/safety-hc/account-and-user-safety/account-safety>

³⁰⁹ The Oversight Board is now accepting cases. October 2020: <https://www.oversightboard.com/news/833880990682078-the-oversight-board-is-now-accepting-cases/>

³¹⁰ Oversight Board Charter: <https://www.oversightboard.com/governance/>

РЕКОМЕНДАЦІЇ ДО РОЗДІЛУ 5:

5.1. Загальні вимоги

СУБ'ЄКТАМ ЗАКОНОДАВЧОЇ ІНІЦІАТИВИ

— при розробленні законодавчих ініціатив, спрямованих на регулювання інтернет-посередників, зважати на їх різноманітність та потребу застосувати різні заходи регулювання, а також належним чином використовувати правила встановлення юрисдикції над інтернет-посередниками.

СУБ'ЄКТАМ ЗАКОНОДАВЧОЇ ІНІЦІАТИВИ

— передбачити в чинному законодавстві обов'язок приватних компаній поважати права людини та створювати внутрішні політики на підставі міжнародних стандартів у цій сфері.

5.2. Прозорість та підзвітність

СУБ'ЄКТАМ ЗАКОНОДАВЧОЇ ІНІЦІАТИВИ

— передбачити в законодавстві обов'язок публікувати статистику звернень правоохоронних органів до найбільших інтернет-посередників з вимогами видалення контенту, сторінки чи ресурсу, або ж з запитами на доступ до персональних даних.

ПРАВООХОРОННИМ ОРГАНАМ

(НАЦІОНАЛЬНІЙ ПОЛІЦІЇ, СЛУЖБІ БЕЗПЕКИ УКРАЇНИ)

— публікувати статистику звернень до найбільших інтернет-посередників з вимогами видалити той чи інший контент, сторінку або ресурс.

ІНТЕРНЕТ-ПОСЕРЕДНИКАМ

— розкрити більше інформації про власні алгоритми та їх застосування щодо контенту.

5.3. Захист свободи вираження поглядів

ІНТЕРНЕТ-ПОСЕРЕДНИКАМ

— передбачити більше чіткості щодо механізму застосування санкцій за порушення стандартів спільноти для того, аби користувачі мали змогу регулювати власну поведінку.

5.4. Захист конфіденційності та захист даних

ПРАВООХОРОННИМ ОРГАНАМ

(НАЦІОНАЛЬНІЙ ПОЛІЦІЇ, СЛУЖБІ БЕЗПЕКИ УКРАЇНИ)

— публікувати статистику звернень до найбільших інтернет-посередників з вимогами надати доступ до інформації про користувачів.

ІНТЕРНЕТ-ПОСЕРЕДНИКАМ

— оприлюднювати узагальнену інформацію про розгляд звернень державних органів щодо доступу до інформації про користувачів, що, крім статистичних даних, міститиме відомості про підстави для відмови в задоволенні таких запитів, види порушень, у зв'язку з якими подавалися відповідні запити на доступ, які саме державні органи тощо.

5.5. Доступ до ефективних засобів правового захисту

СУБ'ЄКТАМ ЗАКОНОДАВЧОЇ ІНІЦІАТИВИ

— передбачити механізми ефективного захисту прав споживачів послуг, що надаються інтернет-посередниками, зокрема шляхом зобов'язання таких посередників встановити ефективні механізми захисту на платформах.

ІНТЕРНЕТ-ПОСЕРЕДНИКАМ

— закріпити механізми оскарження рішень щодо контенту на власних платформах.

ІНТЕРНЕТ-СВОБОДА В УКРАЇНІ 2020

*ДОТРИМАННЯ ПРАВ ЛЮДИНИ
ТА ОСНОВОПОЛОЖНИХ СВОБОД В ІНТЕРНЕТІ*

НАЦІОНАЛЬНИЙ ЩОРІЧНИЙ ЗВІТ

МЕТОДОЛОГІЯ

Предметом аналізу Національного щорічного звіту «Інтернет-свобода в Україні 2020: дотримання прав людини та основоположних свобод в інтернеті» є відповідність національного законодавства, регуляторних ініціатив, судової та адміністративної практики, а також діяльності приватних суб'єктів, зокрема інтернет-посередників, міжнародним стандартам у сфері прав людини (Додаток 1) відповідно до індикаторів, наведених у Додатку 2.

Метою аналізу є оцінювання стану впровадження міжнародних стандартів у сфері прав людини в національному законодавстві та практиці, а також підготовки та просування рекомендацій щодо вдосконалення захисту прав людини в онлайн-середовищі.

ДОДАТОК 1

Перелік міжнародних договорів та рекомендацій у сфері інтернет-свободи

- ▶ Міжнародний пакт про громадянські й політичні права
- ▶ Конвенція про захист прав людини та основоположних свобод (European Convention on Human Rights, далі – Європейська конвенція)
- ▶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, далі – Конвенція 108)
- ▶ Convention on Cybercrime (ETS No. 185, “the Budapest Convention”)
- ▶ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, “the Lanzarote Convention”)
- ▶ Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries
- ▶ Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business
- ▶ Recommendation CM/Rec(2016)5 on Internet freedom
- ▶ Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality
- ▶ Recommendation CM/Rec(2015)6 on the free, transboundary flow of information on the Internet
- ▶ Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users
- ▶ Recommendation CM/Rec(2013)1 on gender equality and media
- ▶ Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines
- ▶ Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services

- ▶ Recommendation CM/Rec(2011)7 on a new notion of media
- ▶ Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling
- ▶ Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet
- ▶ Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data
- ▶ Guidelines for the cooperation between law enforcement and internet service providers against cybercrime
- ▶ United Nations Guiding Principles on Business and Human Rights

ДОДАТОК 2

ІНДИКАТОРИ ОЦІНКИ

1. *Сприятливість середовища для інтернет-свободи*

1.1. Законодавча основа. Захист прав та свобод гарантовано законом, що відповідає міжнародним договорам (зокрема Європейській конвенції). Будь-яке втручання держави в реалізацію відповідає вимогам Конвенції.

1.2. Розроблення регулювання. Закони та інші регуляторні акти у сфері інтернету на етапі підготовки оцінюються на предмет можливого впливу на права та основоположні свободи людини. Закони та інші акти розробляються з дотриманням принципів інклюзивності та прозорості, із залученням усіх зацікавлених груп, зокрема представників приватного сектору, громадянського суспільства, академічної та технічної спільнот.

1.3. Регуляторний орган. Будь-який державний орган, до компетенції якого належать питання, пов'язані з урядуванням інтернету, здійснює свою діяльність незалежно від політичного та комерційного впливу, прозоро та з дотриманням цілей захисту та просування інтернет-свободи.

1.4. Ефективні засоби захисту. Держава має гарантувати доступ осіб до судових та адміністративних процедур неупередженого розгляду скарг щодо порушення прав людини, відповідно до вимог статті 6 Європейської конвенції. Держава має забезпечувати ефективні засоби юридичного захисту згідно зі статтею 13 Європейської конвенції. Це охоплює дієві позасудові механізми, адміністративні чи інші засоби захисту, наприклад інституції захисту прав людини (Омбудсман); відсутність юридичних, процедурних, фінансових чи інших бар'єрів для доступу

1.5. Захист від кіберзлочинності. Держава вживає заходів щодо захисту осіб від кіберзлочинності (кримінальна юстиція чи ін.). Якщо такі заходи створюють ризики для втручання у право на повагу до приватного життя, свободу вираження поглядів чи свободу зібрань та об'єднань, мають бути впроваджені належні умови та гарантії від зловживань, заходи протидії кіберзлочинності повинні відповідати вимогам статей 8, 10 та 11 Європейської конвенції.

1.6. Цифрова грамотність. Держава створює та впроваджує програми для посилення здатності громадян приймати обґрунтовані рішення та поважати права та свободи інших в онлайн-середовищі. Сприяє доступу до навчального, культурного, наукового та іншого суспільно корисного контенту.

2. Свобода вираження поглядів

2.1. Доступ до інтернету

2.1.1. Загальний рівень доступу до інтернету. Інтернет доступний без перешкод та за прийнятну плату для всіх осіб без дискримінації.

2.1.2. Спеціальні заходи забезпечення доступу до інтернету. Держава завдяки приватним компаніям сприяє в доступі до інтернету через спеціальні точки в місцях надання публічних послуг та навчальних закладах, а також вживає розумних заходів для забезпечення доступу до інтернету вразливим групам населення (малозабезпеченим, людям з інвалідністю), у віддалених та сільських районах.

2.1.3. Правомірність обмеження доступу до інтернету. Відсутні загальні, національні відключення інтернету, за винятком особливих ситуацій, коли обмеження доступу до інтернету відповідає Європейській конвенції. Згідно із законодавством та адміністративною і судовою практиками, обмеження доступу особи до інтернету, за загальним правилом, визнається надмірним обмеженням свободи вираження поглядів. Будь-яке обмеження, зокрема в пенітенціарних установах, має відповідати вимогам Європейської конвенції щодо законності, легітимності та необхідності в демократичному суспільстві.

Заходи щодо обмеження доступу до інтернету мають застосовуватися під наглядом суду або незалежного адміністративного органу, за умови, що цей захід є найменш обтяжливим для досягнення відповідної легітимної цілі. Необхідність продовження такого заходу має постійно переглядатися судом чи іншим незалежним органом. Особа, чиє право обмежене, має право на оскарження такого рішення в суді, відповідно до вимог статті 6 Європейської конвенції.

2.2. Свобода думки, право отримувати та поширювати інформацію

2.2.1. Блокування інтернет-ресурсів. Будь-які заходи держави щодо блокування чи іншого обмеження доступу до всієї інтернет-платформи (соціальні медіа, соціальні мережі, блоги чи будь-який інший вебсайт), інформаційно-комунікаційних технологій (ІКТ) (миттєвий обмін повідомленнями або інші застосунки) або будь-який запит з боку державних органів на здійснення таких дій відповідає статті 10 Конвенції щодо законності, легітимності і пропорційності обмежень (необхідності в демократичному суспільстві).

2.2.2. Блокування, фільтрування та видалення онлайн-контенту. Будь-які заходи, що вживаються державними органами для блокування, фільтрування, видалення онлайн-контенту або будь-який запит з боку державних органів здійснювати такі дії супроводжується дотриманням умов статті 10 Конвенції щодо законності, легітимності і пропорційності обмежень (необхідності в демократичному суспільстві).

2.2.3. Право на оскарження. Інтернет-користувачі або інші зацікавлені сторони можуть звертатися до суду відповідно до статті 6 Європейської конвенції стосовно будь-яких заходів, прийнятих з метою обмежити їхню здатність отримувати і поширювати контент або інформацію онлайн.

2.2.4. Прозорість обмежень. Держава своєчасно і належним чином інформує громадськість про застосовані обмеження, наприклад, позначає вебсайт, що був заблокований або з якого були видалені дані, повідомляє детальну інформацію про правову основу, необхідність та обґрунтування таких обмежень, сповіщає про відповідне судове рішення та право на оскарження.

2.3. Свобода онлайн-медіа

2.3.1. Свобода діяльності. Медіа не зобов'язані отримувати спеціальний дозвіл чи ліцензію для здійснення своєї діяльності онлайн чи ведення блогів (крім реєстрації підприємницької діяльності, якщо необхідно).

2.3.2. Гарантії журналістської діяльності. Захист таємниці журналістських джерел поширюється на журналістів та інших медіаучасників, що ведуть свою діяльність онлайн, за законом та на практиці.

2.3.3. Редакційна незалежність. Незалежність редакційної політики медіа гарантується у законодавстві та на практиці. Медіа не стають об'єктом тиску щодо розміщення або видалення певної інформації чи вимог дотримуватися певного напрямку редакційної політики. Журналісти та інші медіаучасники не є суб'єктами для погроз або переслідувань з боку держави. Вони не застосовують самоцензуру через страх покарання, залякування або нападу.

2.3.4. Захист від погроз і тиску. Сайтам медіа та нових медіаучасників не загрожують кібератаки чи інші дії, що порушують їхнє функціонування. Погрози і злочини проти журналістів та медіаучасників оперативно та ефективно розслідуються. Відсутня атмосфера безкарності.

2.4. Законність, легітимність та необхідність обмежень у демократичному суспільстві

2.4.1. Загальні принципи обмежень. Держава не накладає надмірних обмежень на свободу вираження поглядів в інтернеті у своєму законодавстві. Будь-яке обмеження права на свободу вираження поглядів в інтернеті відповідно до вимог статті 10 Європейської конвенції:

- передбачене законом, який є доступним, ясним, недвозначним і досить точним, щоб дати особі можливість регулювати свою поведінку. Закон забезпечує жорсткий контроль за сферою застосування обмежень і ефективний судовий контроль для запобігання зловживанням владою.

Закон вказує з достатньою ясністю сферу розсуду, органи державної влади щодо запровадження обмежень і порядок здійснення цього розсуду;

- має легітимну мету, як вичерпно перераховано в статті 10 Європейської конвенції;
- є необхідним у демократичному суспільстві та пропорційним відповідній легітимній меті. Існує гостра суспільна потреба в обмеженні, яке здійснюється на підставі рішення суду або за рішенням незалежного адміністративного органу, що підлягає нагляду в судовому порядку. Рішення повинно бути цілеспрямованим і конкретним. Крім того, воно має ґрунтуватися на оцінці ефективності обмеження і ризиків надмірного блокування. Ця оцінка повинна визначити, чи може обмеження привести до надмірної заборони доступу до інтернет-контенту або до певних типів контенту і чи є це найбільш демократичним засобом для досягнення поставленої легітимної мети.

2.4.2. Свобода вираження поглядів та захист національної безпеки, територіальної цілісності, громадської безпеки, запобігання розголошенню конфіденційної інформації. Закони щодо мови ворожнечі або охорони громадського порядку, національної безпеки чи про державну таємницю і захист даних не застосовуються у спосіб, який стримує публічні дискусії з питань суспільного інтересу. Такі закони накладають обмеження на свободу вираження поглядів тільки у відповідь на нагальні суспільні потреби, повинні якомога вужче та передбачати співмірні санкції.

2.4.3. Свобода вираження поглядів та охорона здоров'я чи моралі. Закони щодо захисту моралі чи неповнолітніх не застосовуються у спосіб, який обмежує публічні дискусії з питань суспільного інтересу. Такі закони накладають обмеження на свободу вираження поглядів тільки у відповідь на нагальні суспільні потреби, повинні визначатися якомога вужче та передбачати співмірні санкції.

2.4.4. Свобода вираження поглядів та захист репутації чи прав інших осіб. Закони про дифамацію є специфічними і вузько визначеними для сфери їхнього застосування. Вони не перешкоджають публічним дебатам або критиці державних органів і не накладають надмірних штрафів, непропорційних збитків чи судових витрат. Серйозні санкції, такі як позбавлення волі, застосовуються тільки тоді, коли основні права інших людей були серйозно порушені, наприклад, у випадках підбурювання до насильства або ненависті.

2.4.5. Свобода вираження поглядів та підтримання авторитету і безсторонності суду. Закони про захист суду від зовнішніх впливів та тисків не містять загрози публічним дебатам щодо гучних судових справ та не використовуються для того, аби притягнути до відповідальності критиків суду. Відповідні закони накладають співмірні санкції, які застосовуються лише за наявності нагальної суспільної потреби.

3. Свобода мирних зібрань та об'єднань

3.1. Свобода використовувати інтернет-платформи. Кожна людина має право вільно використовувати інтернет-платформи, зокрема соціальні медіа, для комунікації з іншими, створення об'єднань, визначення їхніх цілей, заснування професійних

спілок, організації мирних зібрань, а також здійснювати інші активності, що не суперечать законам відповідно до міжнародних стандартів. Асоціації вільні використовувати інтернет для реалізації права на свободу вираження поглядів та участі в дебатах з політичних та суспільних питань.

3.2. Обмеження свободи зібрань та об'єднань в інтернеті. Будь-які обмеження реалізації цього права в інтернеті, зокрема заходи, пов'язані з блокуванням використання інтернет-платформ у контексті реалізації права на свободу зібрань, відповідають статті 11 Європейської конвенції:

- передбачені законом, який є доступним, ясним, недвозначним і досить точним, щоб дати особі можливість регулювати свою поведінку;
- мають легітимну мету, як вичерпно перераховано в статті 11 Європейської конвенції;
- необхідні в демократичному суспільстві та пропорційні меті, задля якої застосовуються. Існує гостра суспільна потреба в обмеженні. Встановлено справедливий баланс між реалізацією свободи зібрань або об'єднань та інтересами суспільства в цілому. Застосовується захід, що є найменш обтяжливим, якщо він дозволяє досягнути визначеної мети. Обмеження вузько тлумачиться і застосовується, а також не посягає на сутність права на свободу зборів і асоціацій.

4. Право на повагу до приватного і сімейного життя

4.1. Захист персональних даних

4.1.1. Законодавча основа. Закон гарантує захист персональних даних відповідно до вимог Європейської конвенції та Конвенції 108 (Конвенції 108+).

4.1.2. Принципи оброблення персональних даних. Персональні дані обробляються відповідно до закону (за однозначною згодою особи або з інших законних підстав) з легітимною метою та в обсязі, що не перевищує необхідний для досягнення такої мети, з дотриманням точності та безпеки даних. Зазначені умови застосовуються також до «профайлінгу» (техніки автоматичного оброблення персональних даних, що передбачає збір та використання інформації про особу з метою ідентифікації, аналізу та передбачення її вподобань, поведінки та поглядів).

4.1.3. Права осіб у зв'язку з обробленням їхніх даних. Рішення, що суттєво впливають на особу, не повинні ґрунтуватися виключно на результатах автоматизованого оброблення даних, без взяття до уваги думки особи. Кожній особі гарантується право та ефективні можливості: отримувати за запитом інформацію про оброблення персональних даних, заперечувати проти оброблення даних, вимагати виправлення чи видалення даних, давати згоду, заперечувати чи відкликати згоду щодо оброблення персональних даних чи профайлінгу. Існують ефективні механізми захисту в разі порушення прав особи. Обов'язки суб'єктів владних повноважень та приватних суб'єктів щодо оброблення персональних даних визначені законом.

Водночас законодавство у сфері персональних даних містить належні гарантії щодо доступу до публічної інформації та свободи вираження поглядів.

4.1.4. Наглядовий орган. Наглядовий орган, що діє повністю незалежно та безсторонньо, забезпечує дотримання законодавства у сфері захисту персональних даних.

4.1.5. Обмеження. Будь-які обмеження права на повагу до приватного і сімейного життя повинні відповідати Європейській конвенції, зокрема бути передбачені законом, переслідувати легітимну ціль та бути необхідними в демократичному суспільстві. Держава не встановлює заборон, ні законом, ні на практиці, щодо анонімності, псевдонімізації, таємниці приватних комунікацій чи застосування технологій шифрування. Обмеження анонімності та таємниці комунікацій допускається лише згідно з вимогами статті 8 Європейської конвенції.

4.2. Стеження

4.2.1. Загальні вимоги. Заходи стеження, що застосовуються державними органами (наприклад, службою безпеки), повинні відповідати вимогам статті 8 Європейської конвенції та бути предметом ефективного, незалежного та неупередженого нагляду. Заходи стеження мають відповідати принципам законності, легітимності та необхідності в демократичному суспільстві.

4.2.2. Вимоги до законодавства у сфері стеження. Заходи стеження повинні здійснюватися відповідно до доступного, чіткого, конкретного та передбачуваного закону. Закон має містити запобіжники щодо дискреції державних органів, для чого зокрема чітко та точно встановлювати:

- природу порушень, щодо яких можуть застосовуватися заходи стеження;
- компетентні державні органи, які мають повноваження здійснювати заходи стеження, сферу їхньої дискреції та спосіб її реалізації, базуючись на легітимній цілі відповідного заходу;
- категорії осіб, щодо яких можуть застосовуватися заходи стеження;
- обмеження щодо застосування заходів стеження;
- процедури щодо аналізу, використання та зберігання інформації, отриманої за допомогою заходів стеження;
- запобіжні заходи щодо передачі отриманих даних іншим особам та заходи щодо безпеки передачі даних;
- підстави для знищення або видалення інформації, отриманої в результаті стеження;

4.2.3. Авторизація та нагляд у сфері стеження. Заходи стеження мають бути авторизовані самостійним та безстороннім арбітром, що встановлений законом, або іншим державним органом, незалежним від державних органів, які здійснюють такі заходи, та виконавців. Заходи стеження підлягають ефективному судовому нагляду чи контролю з боку іншого державного органу, що гарантує найвищі стандарти неупередженості та незалежності від органів, які реалізують стеження.

Суд або інший орган, що здійснює нагляд, має доступ до усієї інформації, необхідної для реалізації його повноважень, незалежно від ступеня секретності. При цьому, під час реалізації своїх наглядових повноважень, наглядовий орган повинен використовувати секретну інформацію та персональні дані виключно для цілей, визначених законом, та захищати їх від нецільового використання чи розкриття.

Наглядові органи ретельно оцінюють відповідність принципам прав людини заходів стеження, охоплюючи й ті, що здійснюються у співпраці з іноземними органами. Судові органи чи інші органи нагляду мають повноваження скасувати чи припинити заходи стеження, якщо вони визнаються незаконними, а також вимагати видалення будь-якої інформації, отриманої за результатами таких заходів.

4.2.4. Гарантії безпеки. Заходи стеження не повинні містити заходи, що послаблюють системи шифрування чи цілісність комунікаційної інфраструктури (такі, як вбудовані вразливості та «backdoors» в безпеці інформаційно-комунікаційних систем).

4.2.5. Доступ до інформації. Державні органи, що здійснюють заходи стеження, та органи нагляду не звільняються від зобов'язань, передбачених законодавством, про доступ до інформації. Рішення про відмову в наданні інформації має прийматися окремо щодо кожного запиту, бути належним чином обґрунтованим, підлягати нагляду з боку відповідних державних органів з питань доступу до інформації чи захисту персональних даних. Наглядові органи оприлюднюють інформаційні періодичні звіти.

5. Дотримання прав людини в діяльності інтернет-посередників

5.1. Загальні вимоги

5.1.1. Державна політика у сфері діяльності інтернет-посередників. Закони, положення та правила, що застосовуються до інтернет-посередників незалежно від їхньої мети або сфери застосування, охоплюючи комерційну та некомерційну діяльність, повинні ефективно захищати права людини та основні свободи, закріплені в Європейській конвенції.

При розробленні та впровадженні законодавства, що стосується інтернет-посередників, відповідно до своїх зобов'язань за міжнародними договорами, Держава вживає належні кроки для захисту прав людини від зловживань з боку приватних суб'єктів, зокрема забезпечує імплементацію Рекомендації CM/Rec(2018)2 Комітету Міністрів державам-членам про ролі та обов'язки інтернет-посередників, Рекомендації CM/Rec(2016)3 Комітету Міністрів державам-членам з питань прав людини та бізнесу та «Керівних принципів, що стосуються бізнесу і прав людини: імплементація Рамкової програми ООН “Захист, повага і засоби правового захисту”». Такі заходи мають охоплювати також прозорий та інклюзивний процес ухвалення законодавства чи інших відповідних регуляторних актів, а також оцінювання їхнього потенційного впливу на права людини.

Держава забезпечує, що законодавство, регулювання та політика, пов'язані з інтернет-посередниками, інтерпретуються та виконуються без дискримінації.

Будь-яке втручання в діяльність інтернет-посередників, що може призвести до обмеження прав людини, має відповідати принципам законності, легітимності та необхідності в демократичному суспільстві.

5.1.2. Зобов'язання інтернет-посередників щодо дотримання прав людини.

Інтернет-посередники повинні в усіх своїх діях поважати міжнародно визнані основні права та свободи людини, своїх користувачів та інших сторін, які постраждали від їхньої діяльності. Ця відповідальність існує незалежно від здатності або готовності держав виконувати власні зобов'язання щодо прав людини, не неї не впливає розмір, сектор, операційний контекст, структура власності чи природа інтернет-посередника. Водночас масштаби та складність засобів, за допомогою яких посередники виконують свої обов'язки, можуть бути різними і мають враховувати ступінь впливу на права людини, що можуть мати їх послуги.

Інтернет-посередники повинні проводити регулярне відкрите та інклюзивне оцінювання належного виконання ними своїх обов'язків щодо впровадження відповідальності за дотриманням основних прав та свобод людини (наслідки впливу їхніх політик, продуктів та послуг на користувачів та ефективність реагування на результати такого оцінювання).

Інтернет-посередники повинні намагатися постачати свою продукцію та послуги без будь-якої дискримінації, а також вживати обґрунтовані та пропорційні заходи для подолання наявної нерівності.

5.2. Прозорість та підзвітність

5.2.1. Зобов'язання Держави. Держави повинні публічно та на регулярній основі надавати вичерпну інформацію про кількість, характер та правову основу контентних обмежень або розголошення персональних даних, які вони застосували протягом певного періоду через запити, адресовані посередникам, охоплюючи ті, що базуються на міжнародних договорах про взаємну правову допомогу та кроки, вжиті в результаті цих запитів.

Для цілей прозорості держави повинні вимагати, щоб посередники легко розкривали чітку (просту та машинозчитувану), доступну та важливу інформацію про втручання у здійснення прав і свобод у цифровому середовищі на підставі судових або адміністративних розпоряджень, запитів приватних заявників або виконання власних політик обмеження контенту.

5.2.2. Зобов'язання інтернет-посередників. Інтернет-посередники повинні гарантувати, що всі умови угод про надання послуг та політики, які визначають права користувачів, та всі інші стандарти та практики для модерації контенту та оброблення і розкриття даних користувачів, а також зміни до таких регулювань, є загальнодоступними, викладеними чіткою, зрозумілою мовою (якою володіють відповідні користувачі) та в доступних форматах.

Інтернет-посередники повинні чітко та прозоро надавати суттєву публічну інформацію про роботу автоматизованих методів оброблення даних у процесі їхньої діяльності.

Інтернет-посередники зобов'язані регулярно публікувати звіти про прозорість, які надають чіткі (прості та зручні для машинного опрацювання), легкодоступні та значущі відомості про всі обмеження вільного та відкритого потоку інформації та ідей, а також про всі запити щодо такого обмеження, запити на доступ до даних на основі рішень суду, міжнародних договорів про взаємну правову допомогу, запитів приватних заявників або виконання власних політик обмеження контенту.

5.3. Захист свободи вираження поглядів

5.3.1. Зобов'язання Держави. Будь-який запит, вимога чи інші дії державних органів, адресовані інтернет-посередникам для обмеження доступу (охоплюючи блокування або видалення вмісту), або будь-які інші заходи, які можуть призвести до обмеження права на свободу вираження поглядів, встановлюються законом, мають одну із законних цілей, передбачених статтею 10 Конвенції, є необхідними в демократичному суспільстві та пропорційними очікуваній меті.

Державам слід визначити належний рівень захисту, а також обов'язки та зобов'язання відповідно до ролі, яку посередники відіграють у процесі виробництва та розповсюдження контенту. Органи державної влади не повинні прямо чи опосередковано нав'язувати посередникам загальний обов'язок контролю за контентом, до якого вони надають доступ, передають або зберігають автоматизованими чи іншими засобами.

Держави повинні забезпечити закріплення у законодавстві та на практиці, що посередники не несуть відповідальності за сторонній контент, до якого вони надають доступ, передають або зберігають. Інтернет-посередники можуть бути співвідповідальними за контент, який вони зберігають, якщо не діятимуть оперативно, аби обмежити доступ до контенту чи послуг, як тільки-но усвідомлять їхній незаконний характер, зокрема через процедури на основі сповіщення. При цьому вимоги до реагування на повідомлення повинні забезпечувати гарантії від надмірних обмежень.

5.3.2. Зобов'язання інтернет-посередників. Інтернет-посередники повинні поважати права користувачів отримувати, випускати та поширювати інформацію, думки та ідеї. Будь-яке втручання посередників у вільний і відкритий потік інформації та ідей, автоматизованими засобами чи ні, має базуватися на чіткій і прозорій політиці та обмежуватися конкретними законними цілями.

Будь-які заходи, спрямовані на обмеження доступу (зокрема блокування або видалення контенту) в результаті державного наказу чи запиту, мають бути здійснені найменш обмежувальними засобами. Обмежуючи доступ до контенту згідно з власною політикою обмеження контенту, посередники повинні це робити прозоро і без дискримінації. Будь-яке обмеження контенту має бути за обсягом та тривалістю виключно таким, як необхідно для того, щоб уникнути супутнього обмеження або видалення законного контенту. Будь-яке обмеження контенту має супроводжуватись інформуванням громадськості про те, який контент був обмежений і на якій правовій основі.

Через недосконалу здатність автоматизованих засобів оцінювати контекст посередники повинні ретельно слідкувати за впливом автоматизованого управління контентом у галузі прав людини та забезпечувати людський контроль там, де це потрібно.

5.4. Захист конфіденційності та захист даних

5.4.1. Зобов'язання Держави. Заходи стеження, вжиті державами у співпраці з інтернет-посередниками чи без, мають бути цілеспрямованими, чітко визначеними, підлягати ефективному зовнішньому нагляду та відповідати статті 8 Європейської конвенції, а також положенням Конвенції 108.

Будь-яка вимога чи запит органів державної влади на адресу інтернет-посередників щодо надання доступу, збору чи перехоплення персональних даних користувачів, зокрема для цілей кримінального судочинства або будь-яких інших заходів, що суперечать праву на недоторканність приватного життя, мають бути передбачені законом, здійснюватися для досягнення законної мети, передбаченої статтею 8 Європейської конвенції та статтею 9 Конвенції 108, і використовуватися пропорційно лише тоді, коли це необхідно в демократичному суспільстві. Захист права на приватність та захист даних поширюється на пристрої, що використовуються для доступу до інтернету або збережених даних.

Державні органи повинні забезпечити, щоб їхні законодавчі рамки, відповідні політики і практики посередників відстоювали принципи захисту даних (законності, справедливості та прозорості, обмеження мети, мінімізації даних, точності, лімітів за часом зберігання і захисту даних, зокрема цілісності й конфіденційності) і гарантували права суб'єкта даних у повній відповідності до Конвенції 108.

5.4.2. Зобов'язання інтернет-посередників. Посередники не повинні розкривати персональні дані третій особі, якщо це не передбачено законом або не вимагається судовим органом чи іншим незалежним адміністративним органом, рішення якого підлягають судовому перегляду, що визначив – розкриття відповідає застосовним у демократичному суспільстві законам та стандартам і пропорційне легітимній меті.

Інтернет-посередники повинні обмежувати оброблення персональних даних у контексті чітко визначеної мети, про яку активно повідомляється всім користувачам. Оброблення персональних даних має базуватися на вільній, конкретній, обґрунтованій та однозначній згоді користувача щодо певної мети чи іншої законної основи, встановленої законом, як це передбачено в Конвенції 108. Додаткові гарантії, такі, як явна згода, анонімність або шифрування, мусять застосовуватися для автоматичного оброблення спеціальних категорій даних.

Принципи “privacy by default” and “privacy by design” мають використовуватися на всіх етапах, аби запобігти чи мінімізувати ризик втручання в основні права та свободи користувачів.

Користувачі мають право на доступ до своїх персональних даних, а також на виправлення, видалення чи обмеження доступу до них.

Посередники повинні чітко інформувати користувачів про умови, за яких вони можуть користуватися правом на видалення персональних даних, заперечувати проти оброблення даних та відкликати згоду.

Будь-яке відстеження та профілювання користувачів посередниками має бути повністю прозорим. Інтернет-посередники не повинні використовувати методи профілювання та цифрового відстеження, які порушують здійснення користувачами прав людини, охоплюючи право на свободу вираження поглядів та право на приватність.

5.5. Доступ до ефективних засобів правового захисту

5.5.1. Зобов'язання Держави. Держави повинні гарантувати доступні та ефективні судові та позасудові процедури, які забезпечують неупереджений розгляд скарг про порушення прав людини, передбачених Європейською конвенцією, в цифровому середовищі.

Держава імплементує політики та заходи щодо заохочення приватних суб'єктів поважати права людини в їхній діяльності, зокрема встановлювати ефективні механізми подання та розгляду скарг. Такі механізми відповідають вимогам статті 13 Європейської конвенції та критеріям:

- Легітимності (викликають довіру, забезпечують справедливий процес розгляду);
- Доступності (зацікавлені особи обізнані про такі інструменти та можуть їх використовувати без бар'єрів);
- Передбачуваності (забезпечують чітку і зрозумілу процедуру з орієнтовними тимчасовими рамками для кожного етапу, ясність процесу і результатів, а також засобів здійснення моніторингу імплементації);
- Справедливості (забезпечення розумного доступу до джерел інформації, консультацій та експертних знань, необхідних для участі в процесі розгляду скарг);
- Прозорості (інформування сторін про хід розгляду скарги).

Держави повинні підтримувати виважені вікові та гендерні підходи, заохочуючи засоби масової інформації та поширюючи інформаційну грамотність, щоб забезпечити ефективне інформування всіх користувачів про їхні права та свободи, зокрема щодо їхнього права на ефективні засоби захисту державними органами та інтернет-посередниками.

5.5.2. Зобов'язання інтернет-посередників. Інтернет-посередники повинні зробити доступними ефективні онлайн- та офлайн-засоби правового захисту та системи вирішення спорів, які забезпечують оперативне та пряме відшкодування у випадках виникнення скарг від користувача, контент-провайдера чи пов'язаних сторін.

Механізми скарг повинні бути доступними, рівними, сумісними із правами, прозорими та прийнятними. Вони також повинні охоплювати автоматичні гарантії, щоб уникнути конфліктів інтересів, коли компанія безпосередньо керує механізмом, наприклад, залучаючи наглядові структури.

Скарги слід розглядати без необґрунтованих затримок, а відповідні механізми не мають негативно впливати на можливості для скаржників звертатися за допомогою до незалежних національних, зокрема судових, механізмів перегляду.

Посередники повинні забезпечити, щоб усі користувачі та інші сторони, на які вплинули їх дії, мали повний і легкий доступ до інформації чіткою та зрозумілою мовою про застосовні механізми скарг, різні етапи процедури, орієнтовні терміни та очікувані результати.

Посередники не повинні включати в свої умови надання послуг відмову від прав або перешкод для ефективного доступу до засобів правового захисту, таких, як обов'язкова юрисдикція за межами країни, в якій проживає користувач, або арбітражні положення, що не підлягають відмові.

Посередники повинні проводити діалог з асоціаціями споживачів, правозахисниками та іншими організаціями, що представляють інтереси користувачів та інших сторін, а також з органами з питань захисту даних та іншими незалежними адміністративними або регуляторними органами, щоб забезпечити розроблення, впровадження, оцінювання механізмів скарг і вдосконалювати їх шляхом залучення. Вони також повинні регулярно аналізувати частоту, закономірності та причини отриманих скарг, щоб засвоїти цей досвід та поліпшити свою політику, процедури та практику.



Контакти:

Ярополк Бриних

yaropolk.brynykh@abaroli.org

+38-063-241-20-87