

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

Проект фінансується
Європейським Союзом
та Радою Європи



Проект впроваджується
Радою Європи

**ІНТЕГРАЦІЯ УКРАЇНИ В
ЄВРОПЕЙСЬКЕ ІНФОРМАЦІЙНЕ
СУСПІЛЬСТВО:
ВИКЛИКИ ТА ЗАВДАННЯ**

К И Ї В
2 0 1 4

УДК 341
ББК 67.9(4Укр)
І-73

*Рекомендовано до друку Президентською Радою
Української асоціації міжнародного права
Протокол № 17 від 30 вересня 2014 року*

*Рекомендовано до друку вченою радою Інституту міжнародних
відносин Київського національного університету ім. Тараса Шевченка
30 вересня 2014 року, протокол № 2*

Упорядкування і загальна редакція:

Пазюк Андрій Валерійович, керівник лабораторії з управління Інтернетом Української Асоціації міжнародного права, член Експертної ради Комітету Верховної Ради України з питань інформатизації та інформаційних технологій, кандидат юридичних наук

Рецензенти:

доктор юридичних наук, професор, завідувач відділу європейського права та міжнародної інтеграції Інституту законодавства Верховної Ради України
Гріненко Олена Олексіївна

доктор юридичних наук, професор кафедри правознавства Київського національного торговельно-економічного університету

Олійник Олег Вікторович

І-73 Інтеграція України в Європейське інформаційне суспільство: виклики та завдання. — К. : ФОП Клименко 2014. - 212 с.

ISBN 978-966-2717-08-2

У монографії аналізуються загальноєвропейські стандарти розвитку інформаційного суспільства та зобов'язання України щодо проведення правової реформи з метою інтеграції в європейське інформаційне суспільство.

УДК 341
ББК 67.9(4Укр)
© автори, 2014

ISBN 978-966-2717-08-2

Це видання опубліковано в рамках спільної програми Ради Європи та Європейського Союзу «Зміцнення інформаційного суспільства в Україні». Погляди, висловлені в публікації, належать авторам і не обов'язково відображають позицію Ради Європи чи Європейського Союзу.

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

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

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

Контактна інформація

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



ЗМІСТ

Переднє слово	7
---------------------	---

Розділ I. Відповідність законодавства України стандартам Ради Європи в інформаційній сфері

1. Внесок Ради Європи у розвиток міжнародно-правової платформи інформаційного суспільства 11
2. Виконання Україною зобов'язань перед Радою Європи у сфері розвитку інформаційного суспільства 17

Розділ II. Управління Інтернетом, інформаційна екосистема та національні інтереси України

3. Нормативно-правові засади розвитку регуляторного механізму світового інформаційного суспільства: регіональний та глобальний вимір 39
4. Інституційна складова міжнародно-правового регулювання інформаційної сфери 63
5. Розбудова Національного багатостороннього механізму управління розвитком Інтернету в Україні на основі принципів Ради Європи 75

Розділ III. Гармонізація національного законодавства України з європейськими стандартами у сфері інформаційного суспільства: шлях законодавчих реформ

Підрозділ 3.1. Захист персональних даних та доступ до публічної інформації 89

6. Виконання Україною міжнародних зобов'язань із захисту персональних даних 89
7. Досвід зацікавлених сторін у формуванні та реалізації державної політики у сфері електронного доступу до публічної інформації в Україні 99
8. Нарис концепції змін до законодавства України у сфері доступу до публічної інформації 109

Підрозділ 3.2. Забезпечення свободи та плюралізму ЗМІ 121

9. Правове регулювання діяльності засобів масової інформації в рамках права Європейського Союзу	121
10. Основні проблеми правового регулювання дифамації в Європі та в Україні	135
Підрозділ 3.3. Права людини в Інтернеті	143
11. Захист прав людини он-лайн як пріоритетне завдання Ради Європи	143
12. Розвиток правового регулювання суспільних відносин у сфері використання Інтернету в Європейському Союзі	153
13. Здійснення особистих немайнових цивільних прав особи в Інтернеті: судова практика Європейського суду з прав людини	177
Розділ IV. Реформування сфери національної інформаційної безпеки	
14. Організаційно-правове забезпечення національної інформаційної безпеки: шляхи вдосконалення	195
15. Кібервійна як новий засіб і метод ведення війни: виклики міжнародному гуманітарному праву	207
Автори	219

ПЕРЕДНЄ СЛОВО

Україна зробила свій цивілізаційний вибір на користь європейських цінностей та ідеалів — демократії, верховенства права, поваги до прав і свобод людини. Попереду багато завдань, що маємо виконати на шляху реформ. Інтеграція в європейський інформаційний простір — одне з цих завдань. Одночасно, це й виклик на спроможність української нації — усіх громадян нашої держави здолати перешкоди на цьому шляху. Впевнені, об'єднавши зусилля та не покладаючи рук, з цим викликом ми впораємося.

Авторський колектив

РОЗДІЛ I

ВІДПОВІДНІСТЬ ЗАКОНОДАВСТВА УКРАЇНИ СТАНДАРТАМ РАДИ ЄВРОПИ В ІНФОРМАЦІЙНІЙ СФЕРІ

1. Внесок Ради Європи у розвиток міжнародно-правової платформи інформаційного суспільства[©]

Розвиток міжнародно-правового регулювання інформаційної сфери досить активно відбувається на європейському регіональному рівні, в рамках діяльності Ради Європи (РЄ). Діяльність цієї поважної міжнародної організації, членом якої Україна стала після приєднання до Статуту РЄ 9 листопада 1995 року, має на меті досягнення більшої єдності між її членами для захисту та впровадження ідеалів і принципів, які є їх спільною спадщиною, сприяння їх економічному та соціальному прогресу (Пункт 1(а) Статуту РЄ)¹.

Україна бере активну участь у діяльності Ради Європи, а Рада Європи активно впливає на політико-правові реформи в Україні, сприяє розвитку національного законодавства, у тому числі в інформаційній сфері. Враховуючи це, важливим є аналіз внеску Ради Європи у справу розвитку міжнародно-правового регулювання інформаційної сфери на загальноєвропейському рівні, уніфікації національного законодавства на загальноєвропейському рівні та забезпеченню захисту прав і свобод людини в інформаційному суспільстві, що сприяє прогресивному розвитку міжнародного інформаційного права.

Дослідження права Ради Європи в інформаційній сфері (панєвропейського інформаційного права) має важливе значення як з теоретичної точки зору, — для виявлення особливостей та закономірностей розвитку міжнародного інформаційного права на регіональному (європейському) рівні, так і з практичної, — для ефективного виконання нашою державою міжнародно-правових зобов'язань, зокрема тих, що містяться у Плані дій РЄ для України

1. Статут Ради Європи, Лондон, 1949 // Зібрання чинних міжнародних договорів України. — 2006. — № 5. — Книга 2. — С. 435. — Ст. 1270

© *Пазюк Андрій Валерійович*, кандидат юридичних наук, керівник лабораторії з управління Інтернетом Української Асоціації міжнародного права, член Експертної ради Комітету Верховної Ради України з питань інформатизації та інформаційних технологій

на 2011 – 2014 роки², і удосконалення національного законодавства в інформаційній сфері.

Дослідженню теми співробітництва між Україною та Радою Європи у сфері захисту прав людини приділяли увагу українські вчені: М. Анісімова, О. В'юницька, Л. Гіждіван, Б. Мелех, А. Полешко, П. Рабінович. Проте питання паневропейського інформаційного права не були предметом спеціального дослідження в українській науці міжнародного права. Проте, внесок Ради Європи у розвиток міжнародно-правового регулювання інформаційної сфери на паневропейському рівні, визначення особливостей регуляторних інструментів в паневропейському праві та їх ролі в розвитку міжнародного інформаційного права досі залишається розкритим не повною мірою.

Рада Європи фактично випереджала своїми міжнародними договірними інструментами розвиток міжнародного права на універсальному рівні у відповідних сферах, створювала «моделі» міжнародних договорів, які потім втілювалися у загальносвітовому масштабі. Задля досягнення поставленої мети вважаємо за потрібне надати характеристику основних договорів та джерел «м'якого» права Ради Європи в інформаційній сфері

Варто згадати Європейську культурну конвенцію 1954 р., спрямовану на поширення загальноєвропейської культури серед країн шляхом сприяння вивченню громадянами країн-учасниць мов, історії та культури (стаття 2), проведення спільних культурних заходів, що становлять інтерес для Європи (Стаття 3), а також сприяння пересуванню та обміну особами, а також предметами, що мають культурну цінність (стаття 4)³. Відповідні положення, що були апробовані на паневропейському рівні, з'явилися згодом на універсальному рівні – в Рекомендаціях ЮНЕСКО щодо

2. План дій РЄ для України на 2011 – 2014 роки [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_b25

3. Європейська культурна конвенція, Париж, 1954 р. // Зібрання чинних міжнародних договорів України. – 2004. – № 4. – Книга 1. – С. 857. – Ст. 934 / European Cultural Convention // CETS № 018.

міжнародного обміну культурними цінностями (Найробі, 1976 р.), Конвенції ЮНЕСКО про охорону та заохочення розмаїття форм культурного самовираження (Париж, 2005).

У 50-ті роки ХХ ст. відбувається потужний розвиток та поширення звуко- і відеозаписувальної техніки і пристроїв для передачі на далекі відстані звуків і зображень. Реагуючи на потреби ринку аудіо- і відеопродукції, у 1958 році в Парижі підписано *Європейську угоду про обмін програмами телевізійних фільмів*, що має за мету сприяти обміну телевізійними фільмами між європейськими країнами. Сторони угоди домовилися використовувати й демонструвати фільми, виготовлені телерадіомовними організаціями іншої сторони з її дозволу за наявності відповідних положень у контрактах між виробниками фільмів, акторами та іншими особами, що брали участь в їх виробництві⁴.

З метою захисту прав при ретрансляції телевізійних передач у 1960 році Радою Європи ухвалюється текст *Європейської угоди про захист телевізійних передач*⁵. Фактично ці дві угоди підготували появу *Римської конвенції 1961 року*. Додатковими протоколами до цієї Угоди, що були укладені пізніше, обумовлювалася обов'язковим дорученням до *Міжнародної конвенції про охорону прав виконавців, виробників фонограм і організацій ефірного мовлення*, підписаній у Римі 26 жовтня 1961 року.

У 1963 році укладено *Європейську угоду про запобігання радіомовлення зі станцій, що знаходяться за межами національної території*. Угода забороняє організацію на судах, літаках та інших транспортних засобах радіомовлення на територію однієї із держав-учасниць з-поза меж її національної території⁶.

А у 1974 році в Брюсселі приймається міжнародна Конвенція про поширення несучих програми сигналів, що передаються через

4. European Agreement concerning programme exchanges by means of television films, Paris, 1958 / CETS № 027.

5. European Agreement on the Protection of Television Broadcasts, 1960 // CETS № 034.

6. European Agreement for the Prevention of Broadcasts transmitted from Stations outside National Territories, 1965 // CETS № 053.

супутники. Зазначена універсальна конвенція використовує аналогічний підхід до обмеження трансляції сигналів, що й згадана європейська угода.

У 1981 році приймається *Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних*, яка запроваджує міжнародно-правовий режим захисту персональних даних та гарантування їх безперешкодної транскордонної передачі⁷.

Конвенція Ради Європи про транскордонне телебачення 1989 року визначає основні засади такого виду інформаційної діяльності, як телерадіомовлення незалежно від того, як передається сигнал: кабельним телебаченням, наземним передавачем чи супутником (стаття 3)⁸. *Європейська конвенція з питань авторського та суміжних прав у рамках транскордонного супутникового мовлення* 1994 року захищає права та інтереси авторів стосовно їхніх творів, що передаються супутниками⁹. В цілях захисту європейської культурної спадщини у вигляді аудіо- та відеотворів, підвищення їх історичної цінності та художньої форми, шляхом накопичення, збереження та надання широкого доступу до культурної спадщини Рада Європи приймає *Конвенцію про захист європейської культурної спадщини у формі аудіо- та відеотворів* у 2001 році¹⁰.

У 2001 році Радою Європи, крім вищезгаданої конвенції, також приймається ще три конвенції в інформаційній сфері. *Європейська конвенція про правовий захист послуг, що базуються на, або складаються з, умовного доступу* має на меті вивести за рамки закону на територіях держав-учасниць діяльність по наданню несанкціонованого доступу в сфері мовлення та інформаційних

7. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Страсбург, 1981 // CETS № 108. Конвенцію ратифіковано із заявами згідно із Законом України № 2438-VI від 06.07.2010, дата набрання чинності для України: 01.01.2011

8. Європейська конвенція про транскордонне телебачення, Страсбург, 1989 (із змінами 2002 р.) / European Convention on Transfrontier Television // CETS № 132. Конвенцію ратифіковано із заявою та застереженням Законом України № 687-VI (687-17) від 17.12.2008;

9. European Convention relating to questions on copyright law and neighbouring rights in the framework of transfrontier broadcasting by satellite, 1994 // CETS № 153

10. European Convention for the Protection of the Audiovisual Heritage, 2001 // CETS № 183.

послуг¹¹.

Конвенція про інформаційне та правове співробітництво, стосовно «Інформаційних суспільних послуг» передбачає створення юридичної інформаційної системи співробітництва в сфері нових комунікаційних служб шляхом поширення застосування Директиви 98/48/ЄС за межами Європейського Союзу¹². Це дозволить Раді Європи діяти як координаційний центр з розробки законодавства у сфері «інформаційних суспільних послуг» на загальноєвропейському рівні.

У цілях покращення міжнародного співробітництва у боротьбі із злочинами у сфері ІКТ Рада Європи у 2001 році у Будапешті приймає *Конвенцію про кіберзлочинність*¹³. У ній приділяється увага чотирьом видам злочинів, що вчиняються у кіберпросторі з використанням ІКТ, зокрема, правопорушенням щодо конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушенням, пов'язаним з комп'ютерами; правопорушенням, пов'язаним зі змістом; правопорушенням, пов'язаним з порушенням авторських та суміжних прав. Конвенція передбачає надання повноважень, достатніх для ефективної боротьби із зазначеними кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва.

Радою Європи також було вжито заходів щодо посилення гарантій свободи доступу до інформації. Комітет міністрів вперше в 1981 році прийняв Рекомендацію (81) 19 державам-членам Ради Європи стосовно доступу до інформації, що знаходиться у органів публічної влади, яка була актуалізована в 2002 році в Рекомендації

11. European Convention on the legal protection of services based on, or consisting of, conditional access, 2001 // CETS № 178.

12. Convention on Information and Legal Co-operation concerning «Information Society Services», 2001 // CETS № 180

13. Конвенція про кіберзлочинність, Будапешт, 2001, ратифіковано із застереженнями і заявами Законом України № 2824-IV від 07.09.2005 // ВВР. – 2006. – № 5-6. – Ст.71 / Convention on Cybercrime, Budapest, 2001 // CETS № 185.

(2002) 2 про доступ до офіційних документів. *Конвенція Ради Європи про доступ до офіційних документів 2009 року* визначає основний принцип доступу до офіційних документів — гарантувати право кожного на доступ до запитуваних офіційних документів, що є у розпорядженні публічних властей¹⁴.

Останні із зазначених міжнародних договорів значно випереджають розвиток міжнародного права на універсальному рівні, що досягається завдяки узгодженості в підходах та уніфікації законодавства в країнах ЄС.

Окрім договірних норм, право Ради Європи насичене нормативно-правовими положеннями в інформаційній сфері, що містяться у «м'якому» праві — рекомендаціях і деклараціях Комітету Міністрів, резолюціях ПАРЄ. Кількість таких документів на порядок перевищує договірні джерела, завдячуючи більш гнучкому механізму їх ухвалення.

Упродовж минулого півстоліття Рада Європи фактично виступає світовим «локомотивом» міжнародної правотворчості, зокрема у сфері регулювання міжнародно-правових інформаційних відносин на європейському континенті. «М'яке» право відіграє важливу роль у розвитку панєвропейського інформаційного права, завдяки його гнучкості та необтяжливості для держав-членів. Враховуючи зобов'язання України перед Радою Європи, попереду багато роботи для всієї державної «машини», приватного сектора і громадянського суспільства для впровадження високих стандартів у життя. Проте, на виході мають бути здобутки, заради яких Україні варто бути «європейською державою».

2. Виконання Україною зобов'язань перед Радою Європи у сфері розвитку інформаційного суспільства[©]

Розвиток інформаційного суспільства у більшості країн світу визнано одним з найважливіших національних пріоритетів. І Україна не є винятком. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9 січня 2007 року містить положення, яким визначається, що «одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвитку та підвищуючи якість життя»¹⁵. Зважаючи на те, що у розвинутих країнах продовжується перехід до інформаційної сервісно-технологічної економіки, де значна частина ВВП забезпечується діяльністю з виробництва, обробки та поширення інформації та знань, Україні як державі зі значним потенціалом та можливостями в цій царині необхідно продовжувати розбудовувати своє інформаційне суспільство у відповідності до світових тенденцій. Тим паче, що «поширення інформаційних технологій (ІТ) на всі сфери життєдіяльності людини та суспільства стали нормою подальшої еволюції цивілізації»¹⁶.

Своєрідним каталізатором процесу розвитку інформаційного

15. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9 січня 2007 року [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/537-16>

16. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік, с. 5.

суспільства в Україні та забезпечення дотримання прав людини в інформаційній сфері стало членство України в Раді Європи (РЄ), оскільки «вступ країни до Ради Європи традиційно свідчить про її демократичний вибір, послідовність у проведенні реформ, спрямованих на захист прав людини та зміцнення демократичних інститутів», а відповідно саме «членство держави в Раді Європи розглядається впливовими світовими та європейськими фінансовими структурами як показник внутрішньої стабільності та додаткова гарантія захисту власних інвестицій і кредитів у цю державу»¹⁷.

Процедура вступу України до Ради Європи тривала понад три роки та була досить складною. Початок був покладений 14 липня 1992 року, коли Україна офіційно заявила про своє бажання приєднатися до Ради Європи. З цього моменту почалося активне співробітництво між Україною та цією Організацією на двох головних рівнях — урядовому та парламентському. Головною формою співпраці стала активна участь парламентських та урядових представників держави в головних статутних органах, а саме Комітеті міністрів та Парламентській асамблеї. Разом з тим, Організацією було ініційовано процедуру моніторингу національного законодавства на предмет визнання принципів верховенства права, плюралістичної демократії, здатності забезпечення прав та основних свобод людини та громадянина. Вже 26 вересня 1995 року під час вересневої частини своєї сесії 1995 року Парламентська асамблея ухвалила позитивний висновок щодо заявки України на вступ до Ради Європи (Висновок ПА РЄ N 190 (1995)). Однак, визначною подією з точки зору завершення складної і тривалої процедури вступу України до РЄ стало засідання Комітету міністрів Ради Європи, яке відбулося 19 жовтня 1995 року. На підставі винесеного 26 вересня 1995 року ПА РЄ висновку Комітет міністрів РЄ одностайно ухвалив резолюцію про запрошення України стати 37-м членом Організації і приєднатися до її Статуту. Незабаром, 31 жовтня 1995 року Верховна Рада України ухвалила Закон України про приєднання до Статуту Ради Європи.

17. Мармазов В. С., Піляєв І.С. Рада Європи: політико-правовий механізм інтеграції. – К.: Видвничий Дім «Юридична книга», 2000. – С. 311

І вже 9 листопада 1995 року відбулась урочиста церемонія вступу України до Ради Європи, яка офіційно стала 37-м повноправним членом Ради.

Виходячи з пріоритетності розвитку інформаційного суспільства та дотримання прав людини в інформаційній сфері, членство України в РЄ є досить важливою умовою. По-перше, Рада Європи виступає потужною складовою розбудови інформаційного суспільства, а накопичений правовий досвід та існуючі європейські стандарти в цій царині сприяють ефективному проведенню необхідних реформ законодавства держав-членів, до числа яких належить і Україна. По-друге, членство в цій Організації дає можливість Україні більш плідно співпрацювати з іншими державами-членами Ради Європи в межах Комітету міністрів, Парламентської асамблеї Ради Європи (ПАРЄ), Конгресу місцевих і регіональних органів влади Європи та інших органів інституційної системи. По-третє, Україна стала безпосереднім учасником нормотворчого процесу в межах Ради Європи, а тому впливає на формування нових стандартів та принципів в інформаційній сфері.

Під час вступу до Ради Європи Україна, як і всі нові члени РЄ, взяла до виконання, поряд з положеннями Статуту, низку особливих зобов'язань. Проте, слід розрізняти «зобов'язання» та «обов'язки», що впливають з членства України в Раді Європи. Ці поняття є схожими, але не тотожними за своїм змістом.

Що стосується «зобов'язань», то під ними розуміється конкретний, вичерпний перелік питань, котрі Україна під час вступу до Ради Європи погодилася виконати, а в деяких випадках навіть із зазначенням конкретних термінів. Перелік цих зобов'язань наведено у Висновку № 190 Парламентської асамблеї Ради Європи від 1995 року. Вони є надзвичайно важливими і мають бути обов'язково виконані державою, про що йдеться в Статуті та низці документів Ради. Умовно ці зобов'язання можна поділити на чотири основні групи:

- 1) підписання і ратифікація основних міжнародно-правових актів РЄ;
- 2) прийняття у рамках здійснення конституційної та судової реформи низки законів та інших законодавчих актів;
- 3) прийняття низки зобов'язань у галузі правової реформи та внутрішньої політики;
- 4) зобов'язання у сфері зовнішньої політики.

Проте цей перелік не містить пунктів, які б прямо стосувалися інформаційної сфери або ж дотримання в цій сфері прав людини. Це пояснюється тим, що «зобов'язання України перед Радою Європи стосуються саме ключових напрямів конституційної та судово-правової реформи і ключових європейських договорів, членство в яких забезпечує основу для інтеграції держави в європейський правовий простір»¹⁸.

Що стосується «обов'язків», то вони є тим, чого держава повинна неухильно дотримуватися зважаючи на її членство в Раді Європи: положення Статуту Організації та закріплені в ньому такі основоположні засади, як плюралістична демократія, верховенство права та дотримання прав і свобод людини.

Перелік формальних зобов'язань та обов'язків України перед Радою Європи міститься у вищезазначеному Висновку ПАРЄ № 190 від 1995 року та Резолюціях ПАРЄ № 1466 від 2005 року, № 1755 від 2010 року. Втім, найбільш вичерпний перелік обов'язків України в різних сферах було викладено Парламентською асамблеєю у 2005 році в Резолюції № 1466 та Пояснювальному меморандумі до неї, підготовленому співдоповідачами Моніторингового комітету ПАРЄ. Варто відмітити, що робота по завершенню виконання взятих Україною перед Радою Європи зобов'язань здійснюється на підставі Указу Президента України № 24/2011 від 12 січня 2011 року «Про План заходів із виконання обов'язків та зобов'язань України, що випливають з її членства в Раді Європи» та Розпорядження Кабінету

18. Мармазов В. Є., Піляєв І.С. Рада Європи: політико-правовий механізм інтеграції. – К.: Видвничий Дім «Юридична книга», 2000. – С. 319.

Міністрів України № 1002-р від 23 липня 2008 року.

Таким чином, у відповідності до Резолюції ПАРЕ № 1466 та Пояснювального меморандуму, до числа зобов'язань України в інформаційній сфері належить:

- перетворення державних ТРК на канали суспільного мовлення;
- приватизація друкованих ЗМІ, заснованих органами публічної влади;
- гарантування прозорості власності на ЗМІ;
- створення рівних умов для діяльності усіх ЗМІ шляхом перегляду Закону 1997 року «Про державну підтримку ЗМІ та соціальний захист журналістів»;
- ратифікація Європейської конвенції про транскордонне телебачення;
- забезпечення відповідності нової редакції Закону України «Про телебачення і радіомовлення» стандартам Ради Європи і рекомендаціям її експертів (Пункт 12.4)¹⁹;
- вдосконалення законодавства щодо запобігання концентрації медіавласності відповідно до стандартів РЕ;
- вилучення із Закону «Про Національну раду з питань телебачення і радіомовлення» положення щодо можливості висловлення Президентом та Верховною Радою недовіри Національній раді, що веде до відставки її складу;
- ліквідація Держкомтелерадіо під час перегляду Конституції України;
- вилучення з Цивільного кодексу положення (ч. 3 ст. 277) щодо презумпції недостовірності негативної інформації, поширеної про особу²⁰.

Щоб оцінити загальний стан виконання існуючих зобов'язань Україною перед Радою Європи в інформаційній сфері проаналізуємо виконання кожного з них.

19. Резолюція 1466 (2005) ПАРЕ «Про виконання обов'язків та зобов'язань Україною» від 5 жовтня 2005 року [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/994_611

20. Закон України «Про Суспільне телебачення і радіомовлення України» [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/1227-18>

Перетворення державних ТРК на канали суспільного мовлення

Упродовж останнього часу в цьому напрямку спостерігається низка позитивних зрушень, які дають підстави стверджувати, що робота з перетворення державних телерадіокомпаній на канали суспільного мовлення згідно з відповідними стандартами Ради Європи активізується.

Починаючи з 1997 року, коли Верховною Радою було ухвалено Закон України «Про суспільно-правове мовлення в Україні» (який так і не набрав чинності), не відбулися дискусії щодо необхідності запровадження суспільного мовлення. Неодноразово в Парламенті на голосування виносилися відповідні законопроекти щодо суспільного мовлення в Україні, які так і не отримали схвалення. І лише в 2014 році відбулися очікувані зрушення. Так, 17 квітня 2014 року Верховною Радою України було прийнято Закон України «Про Суспільне телебачення і радіомовлення України». Розробкою Закону займалася Громадська гуманітарна рада при Президентові України на підставі затвердженої 30 вересня 2010 року Концепції створення і діяльності Національної громадської телерадіокомпанії України. Закон набув чинності 15 травня 2014 року. Було зроблено важливий крок, оскільки з-поміж європейських країн суспільні мовники були відсутні лише в Україні та Республіці Білорусь.

Прийнятий Закон створює правові основи діяльності Суспільного телебачення і радіомовлення України, а також визначає засади діяльності Національної суспільної телерадіокомпанії України. Текст Закону містить 20 статей, об'єднаних в IV розділі. Перший розділ, «Загальні положення», стосується правових основ діяльності суспільного телебачення та радіомовлення, визначає принципи діяльності та гарантії незалежності Національної суспільної телерадіокомпанії України, а також завдання останньої. Другий розділ, «Органи управління національної суспільної телерадіокомпанії України», містить статті щодо Наглядової ради НСТУ, її складу,

порядку формування, вимог до її членів, а також ряд процедурних моментів функціонування. Третій розділ присвячений «Забезпеченню діяльності Національної суспільної телерадіокомпанії України», в якому йдеться про джерела фінансування, майно, аудит, ліцензії на мовлення, програмну політику, редакційний статут та трансляцію офіційних повідомлень. Четвертий розділ містить кінцеві та перехідні положення, а також положення про внесення змін та доповнень в національне законодавство в зв'язку з прийняттям цього Закону.

Відповідно до положень Закону передбачається, що «для забезпечення поступового та послідовного становлення Суспільного телебачення і радіомовлення України Кабінет Міністрів України на базі Національної телекомпанії України, Національної радіокомпанії України, Державної телерадіокомпанії «Всесвітня служба «Українське телебачення і радіомовлення», Державної телерадіокомпанії «Культура», обласних державних телерадіокомпаній, Державної телерадіокомпанії «Крим», Київської державної телерадіокомпанії, Севастопольської державної телерадіокомпанії, Української студії телевізійних фільмів «Укртелефільм», що реорганізуються, утворює юридичну особу публічного права «Національна суспільна телерадіокомпанія України»²¹. Однак, в практичній площині виникають сумніви з приводу того, чи буде це положення реалізоване повною мірою, бо оскільки останнім часом активно дискутується питання про приналежність до Національної суспільної телерадіокомпанії України обласних державних телерадіокомпаній та УТР, оскільки противники такої приналежності стоять на позиції вилучення обласних державних телерадіокомпаній, разом з УТР, із положень Закону про Суспільне мовлення. Варто зазначити, що в липні та серпні 2014 року у Верховній Раді було зареєстровано два законопроекти, якими пропонується внести зміни до Закону. У першому законопроекті № 4224а «Про внесення змін до ухваленого 17 квітня Закону України «Про Суспільне телебачення і радіомовлення України» (щодо уточнення окремих положень) йдеться про вилучення з Закону УТР.

21. Пояснювальна записка до законопроекту № 4224а [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51602

Законопроектом пропонується не обмежувати суспільне телебачення двома каналами: «Суспільне телебачення здійснює мовлення не менше, ніж на двох загальнонаціональних телеканалах: суспільно-політичному та культурно-освітньому та інших»²². Другий законопроект № 4462а «Про внесення змін до Закону України «Про Суспільне телебачення і радіомовлення України» щодо вилучення з переліку державних мовників, на базі яких буде створюватися Національна суспільна телерадіокомпанія України, обласних державних телерадіокомпаній». У пояснювальній записці до законопроекту говориться, що проект «підготовлений з метою усунення неточностей та прогалин щодо створення Національної суспільної телерадіокомпанії України» і також зазначається, що «прийняття проекту Закону вдосконалює процес створення суспільного телебачення в Україні», а «реалізація законопроекту не вимагатиме додаткових витрат із Державного бюджету України та місцевих бюджетів, не передбачених раніше прийнятими законами». Станом на сьогодні зазначені законопроекти знаходяться на розгляді, а їх доля буде вирішена вже новим скликанням Парламенту.

Наразі Закон про Суспільне мовлення починає поступово втілюватися в практичній площині. Станом на жовтень 2014 року працює робоча група з розробки стратегії створення НСТУ. Цьому сприяє та обставина, що українське медійне середовище та й громадянське також вже давно зачекалося відходу від державного мовлення й переходу до суспільного. Важливо зазначити, що згадуваний Закон України «Про Суспільне телебачення і радіомовлення України» у співвідношенні з існуючими європейськими стандартами є недосконалим, але сама його наявність є свідченням позитивних зрушень в українському інформаційному суспільстві.

22. Проект Закону України про внесення змін до Закону України «Про суспільне телебачення і радіомовлення України» щодо вилучення з переліку державних мовників, на базі яких буде створюватися Національна суспільна телерадіокомпанія України, обласних державних телерадіокомпаній [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51928

Приватизація друкованих ЗМІ, заснованих органами публічної влади

Парламентська Асамблея Ради Європи в своїй Резолюції № 1466 від 5 жовтня 2005 року закликала органи державної влади розпочати роздержавлення друкованих засобів масової інформації, заснованих органами державної влади та місцевого самоврядування. У зв'язку з цим Указом Президента України від 20 січня 2006 року № 39 «Про План заходів із виконання обов'язків та зобов'язань України, що випливають з її членства в Раді Європи» передбачалася підготовка у відповідності до стандартів Ради Європи та подання в установленому порядку Кабінету Міністрів України законопроекту про обмеження впливу органів державної влади та органів місцевого самоврядування на друковані засоби масової інформації.

Зазначений проект Закону України «Про реформування державних і комунальних засобів масової інформації» був розроблений і внесений Кабінетом Міністрів України до Верховної Ради України за № 4003 ще 5 липня 2007 року. Однак, у 2007 році цей законопроект був знятий з розгляду через дострокове припинення повноважень Верховної Ради України.

Проте, робота над законопроектом на цьому не завершилася. Так, Кабінет Міністрів України на основі положень Закону України «Про мораторій на відчуження від редакцій державних та комунальних засобів масової інформації приміщень та майна» № 883-VI від 15 січня 2009 року та Постановою Верховної Ради України «Про Рекомендації парламентських слухань «Про стан свободи слова у регіональних засобах масової інформації» № 2253-VI від 13 травня 2010 року повинен був внести на розгляд Верховної Ради України законопроект про реформування державних та комунальних засобів масової інформації. Цей припис був реалізований Урядом, і вже 1 листопада 2010 року відповідний законопроект було зареєстровано у Верховній Раді за № 7313. Сам проект був розроблений Міністерством юстиції України за участі громадських організацій, зокрема Інституту

Медіа Права. А вже 12 жовтня 2010 року Кабінет Міністрів України на своєму засіданні розглянув і схвалив зазначений документ. Проте, він так і не був проголосований у Верховній Раді України.

Ще один відповідний законопроект був підготовлений і 21 березня 2013 року зареєстрований у Верховній Раді України. Проте, Постановою Верховної Ради № 438-УІІ його було відправлено на доопрацювання з наступним внесенням на повторне перше читання. У зв'язку з цим виникла необхідність внесення на розгляд Верховної Ради України доопрацьованого проекту Закону України «Про реформування державних і комунальних друкованих засобів масової інформації».

Новий доопрацьований законопроект «Про реформування державних і комунальних друкованих засобів масової інформації» в серпні 2014 року було винесено на громадське обговорення Державним комітетом телебачення і радіомовлення. Метою Закону є обмеження впливу органів державної влади та органів місцевого самоврядування на діяльність друкованих ЗМІ. Разом з тим, «реалізація Закону має звести до мінімуму використання медіа з метою маніпулювання суспільною свідомістю і особистою думкою громадян та забезпечить соціальні гарантії журналістам реформованих засобів масової інформації. На думку експертів, цей закон сприятиме створенню економічно незалежних друкованих медіа та належних умов їх діяльності, що у свою чергу покращить інформаційне забезпечення громадян України»²³.

Окремі положення законопроекту перегукується з чинними законами «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про державну підтримку засобів масової інформації та соціальний захист журналістів».

26 23. Винесено на обговорення доопрацьований законопроект про реформування державних та комунальних друкованих ЗМІ [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/uk/publish/article?art_id=247388005&cat_id=244277212

Таким чином, дотепер не прийнято жодного із запропонованих проектів Закону України про приватизацію друкованих ЗМІ, заснованих органами публічної влади, хоч робота в цьому напрямку ведеться упродовж останніх дев'яти років. Попри всі недоліки та хиби існуючих законопроектів ухвалення одного з них має концептуально змінити підхід до друкованих ЗМІ, забезпечити доступ ЗМІ до інформації та сприятиме дотриманню принципів свободи слова.

Гарантування прозорості власності на ЗМІ

Проблеми, пов'язані з прозорістю власності на ЗМІ, в українському суспільстві, належать до активно обговорюваних. Після того, як Парламентська Асамблея у своїй Резолюції № 1466 від 2005 року закликала органи влади України з метою покращення рівня функціонування плюралістичної демократії «гарантувати прозорість власності на засоби масової інформації», проблема знайшла своє висвітлення в Указі Президента «Про План заходів із виконання обов'язків та зобов'язань України, що випливають з її членства в Раді Європи» від 20 січня 2006 року. В Указі також містилося завдання для Міністерства юстиції України та Національної Ради України з питань телебачення і радіомовлення підготувати та подати в установленому порядку Кабінету Міністрів України з подальшим внесенням на розгляд Верховної Ради України законопроект «Про внесення змін до деяких законів України щодо гарантування прозорості відносин власності щодо засобів масової інформації». До числа вітчизняних законів, які у відповідності до законопроекту потребують змін, було віднесено наступні: «Про телебачення і радіомовлення», «Про друковані засоби масової інформації (пресу) в Україні», «Про інформаційні агенства», «Про Національну раду України з питань телебачення і радіомовлення» та «Про державну реєстрацію юридичних осіб та фізичних осіб - підприємців».

У Верховній Раді України цей законопроект був зареєстрований 16 листопада 2006 року за номером № 2555, а трохи згодом, 23

січня 2007 року, був переєстрований за номером № 0890, проте, був відхилений Парламентом і внаслідок цього знятий з розгляду.

Відмітимо, що з часу надання доручення підготувати законопроект про забезпечення прозорості відносин власності стосовно засобів масової інформації Верховною Радою України було прийнято Закон України від 12 січня 2006 р. № 3317-IV «Про внесення змін до Закону України «Про телебачення і радіомовлення», яким Закон України «Про телебачення і радіомовлення» викладено у новій редакції, а також внесено ряд змін до Закону України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців». Таким чином, змінами до зазначених законів України вже було частково врегульовано питання прозорості відносин власності щодо засобів масової інформації, але відповідних змін потребують також інші закони України, які регулюють діяльність засобів масової інформації.

Ще однією спробою покращення національного законодавства щодо прозорості власності на ЗМІ став законопроект «Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації, а також реалізації принципів державної політики в сфері телебачення і радіомовлення», який 23 січня 2013 року був зареєстрований у Верховній Раді за номером № 2074, а згодом, з урахуванням внесених правок, був схвалений ВРУ і набрав чинності 4 липня 2013 року. Згідно із Законом, відповідні зміни вносилися до законів «Про друковані засоби масової інформації (пресу) в Україні», «Про інформаційні агенства», «Про Національну раду України з питань телебачення і радіомовлення» та «Про телебачення і радіомовлення»²⁴. Законом вносилися такі зміни:

- запровадження обов'язкового зазначення в заяві про державну реєстрацію друкованого ЗМІ даних про юридичну або фізичну особу, яка здійснює контроль за засновником (співзасновниками), власником (співвласниками) друкованого ЗМІ, а також юридичну особу, за якою засновник, власник (співвласник) здійснює

28 24. Закон України «Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації»[Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/409-18>

- відповідний контроль. При цьому під здійсненням контролю визнається безпосереднє або через пов'язаних осіб володіння частками (паями, акціями), що забезпечує досягнення 50 і більше відсотків голосів у вищому органі юридичної особи, яка є засновником (співзасновником) друкованого ЗМІ (Пункт 1.1.);
- запроваджує як одну із підстав відмови в державній реєстрації друкованого ЗМІ порушення засновником (співзасновниками) вимог статті 10 Закону України «Про друковані засоби масової інформації (пресу) в Україні» (щодо недопущення монополізації друкованих ЗМІ) (Пункт 1.3.4);
 - передбачає обов'язкове зазначення в кожному випуску друкованого ЗМІ прізвища та ініціалів особи, відповідальної за випуск відповідного номера видання, поряд з наступними вихідними даними: назва видання, інформація про засновника (співзасновників), прізвище та ініціали редактора, порядковий номер випуску і дата його виходу в світ, індекс видання, розповсюджене за передплатою, тираж, ціна або помітка «Безкоштовно», адреса редакції, видавця, друкарні, серія, номер та дата видачі свідоцтва про державну реєстрацію, видавець (Пункт 1.4.4);
 - передбачає запровадження обов'язкового розміщення інформації про засновника (співзасновників) та власника (співвласників) інформаційних агентств у кожному випуску продукції таких агентств (Пункт 2.1)
 - «Пов'язана особа - юридична або фізична особа, яка здійснює контроль за засновником (співзасновниками), власником (співвласниками) друкованого засобу масової інформації, а також юридична особа, за якою засновник, власник (співвласник) здійснює відповідний контроль. У разі, якщо одним із співзасновників (співвласників) друкованого засобу масової інформації є фізична особа, пов'язаними з нею особами вважаються також члени її сім'ї (чоловік, дружина, діти та батьки, мачуха та вітчим, рідні брати, сестри та їхні діти, чоловіки (дружини), спільно з якими вона здійснює контроль за друкованим засобом масової інформації» (Пункт 1.2.);

- «Контроль за засновником (співзасновником), власником (співвласником) телерадіоорганізації - безпосереднє або через пов'язаних осіб володіння частками (паями, акціями), що забезпечує досягнення 50 і більше відсотків голосів у вищому органі юридичної особи, яка є засновником (співзасновником), власником (співвласником) телерадіоорганізації» (Пункт 4.1.);
- «Забороняються створення та діяльність телерадіоорганізації, засновником (співзасновниками), власником (співвласниками) якої є нерезидент (нерезиденти), що зареєстрований в одній з офшорних зон, перелік яких визначений Кабінетом Міністрів України» (Пункт 4.2);
- у заяві про видачу (продовження) ліцензії на мовлення, яка подається до Національної ради з питань телебачення і радіомовлення, запроваджується обов'язкове зазначення відомостей про пов'язаних осіб та акціонерів, які на момент подання відповідної заяви володіють пакетами акцій більш як по 5 відсотків (Пункт 4.6);
- покласти на Національну раду України з питань телебачення і радіомовлення обов'язок надавати детальне обґрунтування всім своїм рішенням щодо видачі, відмови у видачі та відмови у продовженні ліцензій (Пункт 4.6); та деякі інші.

Тож, з ухваленням Закону «Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації» було зроблено значний вклад в поліпшення прозорості стосунків власників та медіа, так само як і фінансово-господарської діяльності ЗМІ. Проте, задля вирішення проблеми гарантування прозорості власності на ЗМІ потрібно ще на законодавчому рівні обмежити або заборонити участь офшорних компаній у структурі власності телеорганізацій, оскільки теперішня ситуація певною мірою створює правову невизначенність, яка є суттєвою перепорою для інвестування.

Створення рівних умов для діяльності усіх ЗМІ шляхом перегляду Закону «Про державну підтримку ЗМІ та соціальний захист журналістів» 1997 року

Нагадаємо, що «Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» N 540/97-ВР від 23 вересня 1997 року (далі – Закон) визначає правові, економічні, організаційні засади державної підтримки засобів масової інформації та соціального захисту журналістів»²⁵. Задля виконання своїх обов'язків, котрі випливають із членства України в Раді Європи, та створення рівних умов для діяльності усіх ЗМІ, до Закону України «Про державну підтримку ЗМІ та соціальний захист журналістів» від 1997 року було внесено чимало змін та доповнень.

Так, Законом України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про загальнообов'язкове державне пенсійне страхування» від 17 листопада 2005 року вносилися зміни до частини четвертої статті 16 Закону та було сформульовано, що «у разі поранення, контузії, каліцтва, одержаних під час виконання службових обов'язків у місцях надзвичайних подій, журналіст або прирівняний до нього працівник має право на призначення дострокової пенсії за віком відповідно до Закону України «Про загальнообов'язкове державне пенсійне страхування», але не раніше ніж за 5 років до досягнення пенсійного віку (для чоловіків - 60 років, для жінок - 55 років), за наявності страхового стажу не менше 25 років - для чоловіків і не менше 20 років - для жінок»²⁶. Таким чином, було зменшено віковий

25. Коментар проекту Закону України «Про внесення змін до Закону України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (щодо уточнення поняття «працівники засобів масової інформації, прирівняні до журналістів» та усунення протиріч між окремими законодавчими актами України)» від 7 листопада 2013 року за N 3577 [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/1_doc2.nsf/link1/JG2RD001.html

26. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про загальнообов'язкове державне пенсійне страхування» від 17 листопада 2005 року [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/1_doc2.nsf/link1/T053108.html

ценз для отримання пенсій журналістами або прирівняними до них працівниками.

В 2007 році після прийняття Закону України «Про внесення змін до деяких законів України щодо соціального захисту інвалідів» від 3 травня 2007 року були внесені зміни в пункт 1 частини 2, частину першу статті 3 Закону, за якими державна адресна підтримка надається не лише виключно засобам масової інформації для дітей та юнацтва, але поширюється й на ЗМІ для інвалідів.

Ряд змін до Закону було внесено також з прийняттям Закону України «Про внесення змін до Бюджетного кодексу України та деяких інших законодавчих актів України» від 23 грудня 2010 року. У відповідності до них звільнення від податку на додану вартість та пільгове оподаткування редакцій (юридичних осіб) ЗМІ здійснюються у відповідності до Податкового кодексу України.

Незначні зміни були внесені з ухваленням законів «Про внесення змін до деяких законодавчих актів України щодо діяльності Міністерства фінансів України, Міністерства економічного розвитку і торгівлі України, інших центральних органів виконавчої влади, діяльність яких спрямовується та координується через відповідних міністрів» від 16 жовтня 2012 року та «Про внесення змін до деяких законодавчих актів України щодо приведення законодавства у відповідність з Кримінальним процесуальним кодексом України» від 16 травня 2013 року.

Зазначені зміни сприяли покращенню умов діяльності усіх ЗМІ, проте не є достатніми аби стверджувати, що зобов'язання в цьому напрямку Україна виконала в повному обсязі. Важливо відмітити, що створення більш рівних умов для діяльності всіх засобів масової інформації допоможе зберегти плюралізм думок у ЗМІ, уможливить існування преси, яка виражає погляди різних верств населення, а також дозволить громадянам повніше реалізовувати право на вільний доступ до інформації.

Ратифікація Європейської конвенції про транскордонне телебачення

Будучи повноправним членом Ради Європи, Україна підписала Європейську конвенцію про транскордонне телебачення 14 червня 1996 року і цим виразила свою згоду на обов'язковість для себе її положень. Проте, знадобилося майже дванадцять років, щоб ратифікувати саму Конвенцію, і це незважаючи на неодноразові заклики національних медіа-експертів і рекомендації Парламентської Асамблеї Ради Європи.

21 січня 2009 року набрав чинності Закон України «Про ратифікацію Європейської конвенції про транскордонне телебачення» від 17 грудня 2008 року. Відповідно до цього Закону, Україна ратифікує Європейську Конвенцію зі змінами, внесеними Протоколом про внесення змін до Європейської конвенції про транскордонне телебачення від 9 вересня 1998 року, з такими заявами та застереженнями. Перше застереження до статті 19 Конвенції про те, «що органом, на який покладаються повноваження» з надання інформації щодо телемовників, про внутрішнє законодавство та практику з питань, що охоплюються Конвенцією, та який співпрацює, коли це необхідно, з органами інших країн-учасниць, «є Національна Рада України з питань телебачення і радіомовлення». Друге застереження висловлювалось до статті 32 Конвенції та полягало в тому, що «Україна залишає за собою право обмежувати на своїй території трансляцію програм, що містять рекламу алкогольних напоїв, у частині, що не відповідає національному законодавству»²⁷.

Це стало наступним кроком на шляху регуляторної реформи сфери телебачення та надання програмних послуг, виходячи із загальноєвропейських стандартів. Разом з тим, це посприяло більшій інтеграції національних правил регулювання діяльності у сфері телерадіомовлення з відповідними загальноєвропейськими.

Нагадаємо, що основний лейтмотив Конвенції викладений у статті

27. Закон України «Про ратифікацію Європейської конвенції про транскордонне телебачення» [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/687-17>

4 (свобода прийому та ретрансляції), у відповідності до положень якої сторони забезпечують свободу самовираження й інформації згідно зі статтею 10 Конвенції про захист прав людини і основоположних свобод, гарантують свободу прийому й не обмежують ретрансляцію на своїх територіях програмних послуг, які відповідають умовам Конвенції.

Забезпечення відповідності нової редакції Закону України «Про телебачення і радіомовлення» стандартам Ради Європи і рекомендаціям її експертів

Нагадаємо, що Закон України «Про телебачення і радіомовлення» ухвалений Верховною Радою України та введений в дію після його опублікування 22 лютого 1994 року. У відповідності до Конституції та Закону України «Про інформацію», цей Закон регулює відносини, що виникають у сфері телевізійного та радіомовлення на території України, визначає правові, економічні, соціальні, організаційні умови їх функціонування, спрямовані на реалізацію свободи слова, прав громадян на отримання повної, достовірної та оперативної інформації, на відкрите і вільне обговорення суспільних питань.

За висновками експертів Ради Європи Закон України «Про телебачення і радіомовлення» є досить суперечливим у своїх положеннях і потребує ретельного перегляду і внесення змін.

Перший ґрунтовний аналіз Закону (в редакції від 2006 року) було здійснено експертами Ради Європи Ів Саломон та д-ром Карол у січні 2007 року на запит української влади. В аналізі та коментарях, підготовлених експертами, чітко зазначаються недоліки Закону та містяться вказівки та рекомендації стосовно вдосконалення положень Закону. Деякі з них були враховані в наступних редакціях Закону.

Ще один експертний аналіз Закону (але вже в редакції від 2011 року) був здійснений Ів Саломон та Бернд Мьовес у грудні 2011 року. У своєму аналізі автори надали численні пропозиції стосовно внесення змін у Закон з метою приведення його у відповідність з

європейськими стандартами. У цій редакції Закону їх рекомендації були враховані лише частково. Значні заобсягом зміни в цій редакції мають технічний характер — наприклад, заміна певних термінів, перенесення положень (правила спонсорства) до інших законів, пов'язаних з медіа, перерозподіл обов'язків між органами. В цілому, Закону від 2006 року не змінився в соїй основі попри настійливі рекомендації експертів Ради Європи у 2007 році²⁸.

Низка змін до Закону була внесена відповідними законами протягом 2012 та 2013 років, проте вони не виправляють усіх зазначених в експертизах недосконалостей та неточностей положень зазначеного Закону.

Вдосконалення законодавства щодо запобігання концентрації медіавласності відповідно до стандартів РЄ

Питання запобігання концентрації медіавласності нерозривно пов'язане з питанням гарантування прозорості структури власності на українські ЗМІ.

Зазначимо, що «основою політики Ради Європи щодо забезпечення прозорості власності на ЗМІ та запобігання надмірній концентрації в медійній сфері є два документи — вже згадувана Європейська конвенція про захист прав людини та основних свобод (стаття 10) і Європейська конвенція про транскордонне телебачення. Так, стаття 10-біс Європейської конвенції про транскордонне телебачення вимагає від сторін-учасниць Конвенції «всіма можливими засобами виключити можливість порушення плюралізму засобів масової інформації стосовно програмних послуг, що транслюються або ретранслюються мовником, фізичною або юридичною особою, що підпадає під юрисдикцію даного Учасника Конвенції». Стаття 6 цієї ж Конвенції передбачає, що інформація про телерадіомовника має надаватись компетентним органам учасників Конвенції, що

28. Аналіз та коментарі до Закону України «Про телебачення і радіомовлення» [Електронний ресурс]. – Режим доступу: http://www.telekritika.ua/doc/images/news/70044/Modified%20Final%20Analysis%20and%20Comments%20on%20Ukr.Br-g%20Law_01.03.2012.pdf

забезпечують трансляцію, на їх вимогу і як мінімум має включати прізвище, найменування, місце проживання/місцезнаходження, статус мовника, структуру, цілі і порядок фінансування програм, які транслюватимуться мовником або які він має намір транслювати. На базі положень цих документів Радою Європи було напрацьовано ряд рекомендацій щодо забезпечення прозорості ЗМІ та обмеження концентрації в медійній сфері»²⁹.

Виходячи з аналізу законодавства на предмет відносин власності у сфері ЗМІ в Україні, можна зробити висновок, що такі відносини є непрозорими, оскільки отримати інформацію про власників-бенефіціаріїв ЗМІ практично неможливо. Зазвичай такими власниками-бенефіціаріями є фізичні особи, які насправді володіють або ж контролюють медійні компанії. Цьому слугують два головні фактори. Перший — Закон не зобов'язує медійні компанії оприлюднити відомості про кінцевих власників, а також і осіб, котрі впливають на їх редакційну політику. Другий — це приналежність ЗМІ компаніям, зареєстрованим в офшорних зонах, законодавство яких стоїть на сторожі конфіденційності відомостей про фактичних власників.

Національне законодавство про засоби масової інформації, а саме Закон «Про телебачення і радіомовлення» і Закон «Про друковані ЗМІ» не вимагають розкриття відомостей про бенефіціарних власників медійних компаній. Разом з тим, згідно з Законом «Про мовлення», організації ефірного мовлення можуть перебувати у власності фізичної або юридичної особи. Натомість закон не містить вимоги про розкриття осіб, які володіють юридичними особами. У відповідності до положень Закону «Про друковані ЗМІ», обов'язковою є реєстрація засновників періодичних видань, як фізичних, так і юридичних осіб, проте така процедура реєстрації не передбачається для бенефіціарних власників компанії, що видають друковані ЗМІ. Тому виникає прогалина, за якої фізичні особи можуть володіти компаніями в сфері

36 29. Запобігання концентрації ЗМІ та забезпечення прозорості відносин власності щодо ЗМІ: досвід країн Європи та пропозиції для України [Електронний ресурс]. – Режим доступу: <http://www.media.parlament.org.ua/uploads/files/f717.pdf>

друкованих ЗМІ без розкриття своєї особи. Це означає, що отримати інформацію можна лише про засновників компаній у сфері ЗМІ, але не про власників таких медіа компаній.

Ще однією складною проблемою є те, що українським законодавством не встановлено обмеження щодо частки іноземних компаній у власності на ЗМІ. І, як наслідок, деякі українські ЗМІ перебувають у власності офшорних компаній самих українців.

За Законом «Про телебачення і радіомовлення» іноземні юридичні чи то фізичні особи не можуть бути засновниками телерадіомовних компаній. Проте в Законі такі терміни як «власник» та «засновник» телекомпанії часто використовуються як взаємозамінні. Заборона іноземцям на володіння друкованими ЗМІ не міститься і в положеннях Закону «Про пресу».

Таким чином, вищезазначене дає підстави стверджувати, що встановлення структури власності в медійних компаніях в Україні є вкрай складною процедурою. В свою чергу, це є свідченням недосконалості українського законодавства в цій царині й зовсім не відповідає стандартам Ради Європи.

Вилучення із Закону України «Про Національну раду з питань телебачення і радіомовлення» положення щодо можливості висловлення Президентом та Верховною Радою недовіри Національній раді, що веде до відставки її складу

З моменту прийняття у 1997 році Закон «Про Національну Раду з питань телебачення і радіомовлення» був розкритикований за практично необмежені можливості Президента та Верховної Ради України звільняти будь-коли призначених ними членів.

Згодом ці та інші недосконалості Закону були враховані в новій редакції закону, підготовлений Комітетом з питань свободи слова, яка була прийнята Верховною Радою України 3 березня 2005 року. Проте, це не дає підстави стверджувати, що нова редакція вирішує всі спірні та недосконалі положення Закону.

У відповідності до нової редакції, суттєвого реформування зазнали положення, які стосувалися призначення та звільнення членів Національної ради, особливо в частині підстав та процедури дострокового припинення їх повноважень. Важливим здобутком стало скорочення переліку підстав для дострокового припинення повноважень та заміна процедури такого припинення. Відтак, статтю 8 передбачається вісім підстав для дострокового припинення повноважень та ще одна в статті 16. У всіх зазначених випадках рішення приймає сама Національна Рада або ж суд. А це, в свою чергу, є свідченням наближеності положень Закону до європейських стандартів.

Вкрай суперечливим та таким, що не відповідає європейським підходам, був абзац, доданий до статті 16 Закону, наступного змісту: «За результатами розгляду звіту Національної ради Верховна Рада України та/чи Президент України можуть висловити недовіру Національній раді, що має наслідком відставку її членів у повному складі». Певною мірою це ставить членів Національної ради в залежність від Президента чи то Верховної Ради. Більше того, таке формулювання певною мірою розширювало право Президента та Верховної Ради порівняно з первинним текстом Закону, оскільки тепер з'являлася можливість звільнення всього складу Національної ради, а не лише призначених ними членів Ради.

Незважаючи на постійні рекомендації ПАРЕ виключити із Закону положення про можливість висловлення Президентом та Верховною Радою недовіри Національній раді, що веде до відставки її складу, рішучих кроків з цього приводу так і не було зроблено. Свідченням цьому слугує положення Закону України «Про внесення змін до Закону України «Про Національну раду України з питань телебачення і радіомовлення» щодо дострокового припинення повноважень членів Національної ради України з питань телебачення і радіомовлення» від 17 квітня 2014 року, в якому міститься наступне формулювання частини п'ятої статті 16:

«5. За результатами розгляду звіту Національної ради Верховна Рада України як суб'єкт призначення може прийняти рішення про незадовільну оцінку діяльності члена (членів) Національної ради з частини складу Національної ради, призначеної нею, що має наслідком дострокове припинення повноважень члена (членів) Національної ради з цієї частини складу Національної ради.

У разі незадовільної оцінки діяльності члена (членів) Національної ради за результатами розгляду звіту Президент України як суб'єкт призначення може достроково припинити повноваження члена (членів) Національної ради з частини складу Національної ради, призначеної ним»³⁰.

Таке формулювання дає підстави стверджувати, що попри внесення змін до Закону в частині висловлення недовіри Президентом та Верховною Радою України, сутність самого положення залишається незмінною, а саме положення чинним.

Ліквідація Державного комітету телебачення і радіомовлення України під час перегляду Конституції України

Варто зазначити, що це зобов'язання України поки що залишається не виконаним. На сьогодні Державний комітет телебачення і радіомовлення України функціонує на основі Положення про Державний комітет телебачення і радіомовлення України, затвердженого Постановою Кабінету міністрів України від 13 серпня 2014 року.

Вилучення з Цивільного кодексу України положення (ч. 3 ст. 277) щодо презумпції недостовірності негативної інформації, поширеної про особу

Частина 3 ст. 277 ЦК України встановлює презумпцію

30. Закон України «Про внесення змін до Закону України «Про Національну раду України з питань телебачення і радіомовлення» щодо дострокового припинення повноважень членів Національної ради України з питань телебачення і радіомовлення» від 17 квітня 2014 року [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1222-18>

недостовірності негативної інформації: «негативна інформація, поширена про особу, вважається недостовірною, якщо особа, яка її поширила, не доведе протилежного». Тобто, будь-яка негативна інформація про особу буде вважатися судом недостовірною, якщо поширювач інформації не доведе, що ця негативна інформація відповідає дійсності. Це положення й досі залишається чинним, тому ми можемо говорити, що ще одне зобов'язання поки залишається не виконаним Україною.

Здійснивши детальний аналіз існуючих зобов'язань України перед Радою Європи в сфері розвитку інформаційного суспільства, варто відмітити, що з переліку наявних зобов'язань належним чином виконано лише один пункт — ратифіковано Європейську конвенцію про транскордонне телебачення. Разом з тим, простежується ціла низка позитивних зрушень стосовно інших пунктів, зокрема щодо перетворення державних ТРК на канали суспільного мовлення, приватизації друкованих ЗМІ, заснованих органами публічної влади, та певною мірою гарантування прозорості власності на ЗМІ, хоча вважати ці пункти виконаними, на нашу думку, не можна. Це стосується і пунктів, які містяться в Пояснювальному меморандумі до Резолюції ПАРЄ № 1466, котрі також не отримали практичного виконання та закріплення на законодавчому рівні. Але варто наголосити, що виконання зобов'язань є постійним процесом, який неможливо вичерпати прийняттям декількох законів.

РОЗДІЛ II

УПРАВЛІННЯ ІНТЕРНЕТОМ, ІНФОРМАЦІЙНА ЕКОСИСТЕМА ТА НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ

3. **Нормативно-правові засади розвитку світового інформаційного суспільства: регіональний та глобальний вимір[©]**

Зазвичай суспільства та соціальні системи класифікують залежно від форми соціальної організації, що лежить в їх основі. Як правило, такі класифікації мають дихотомічний характер. Ще Конфуцій поділяв суспільства на ті, що мають велику схожість, та ті, у яких є зовсім мало спільного. Наразі найбільш поширеною класифікацією є поділ суспільств на інформаційно багаті та інформаційно бідні. Перехід до інформаційного суспільства був викликаний переосмисленням цінності ресурсів та переміщенням акцентів. У наш час інформація визнається найбільш цінним ресурсом, контроль над яким власне і визначає впливовість суб'єктів на міжнародній арені.

Слід проводити чітке розмежування між поняттями інформаційне суспільство та інформаційна ера. Перше з них стосується соціальної системи, в той час як друге використовується для позначення періоду існування людської цивілізації. Таким чином, цілком можливою є ситуація, коли група людей, що живе в інформаційну еру, знаходиться поза межами інформаційного суспільства.

Крім того, настання інформаційної ери не означає відмову від аграрного та індустріального типів суспільства, що можуть цілком органічно існувати в рамках нової суспільної формації, продовжуючи задовольняти базові потреби людей. Відверто кажучи, інформаційне суспільство буде нежиттєздатним, якщо припиниться постачання сировини, виробництво продуктів харчування та техніки. Отже, мову слід вести не про абсолютне заміщення інформаційним суспільством тих суспільних формацій, що існували раніше, а швидше про

© *Кирилюк Ольга Василівна, аспірантка кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка*

перерозподіл повноважень та налагодження взаємодії³¹.

Історична спадщина людства повинна використовуватися максимально ефективно та повно в нових умовах інформаційної ери з тим, щоб приносити якомога більшу користь.

Двома ключовими характеристиками сучасного історичного періоду є глобалізація та інформаційно-комунікаційні технології (надалі – «ІКТ»). ІКТ виступають як головної рушійної сили глобалізованих суспільств, в основі яких лежать знання та інформація³². Вплив ІКТ на людство був настільки значним, що навіть привів до формування нового типу суспільного устрою.

Формування інформаційного суспільства є одночасно викликом сучасній системі міжнародних відносин та безцінною можливістю для вирівнювання рівня розвитку країн та народів, між якими впродовж тривалого часу зберігалася та поглиблювалася прірва. Слід чітко усвідомити, що ІКТ самі по собі не є гарантією економічного зростання, подолання бідності та встановлення абсолютної рівності можливостей між усіма країнами. Без створення відповідних інституційних механізмів та розробки ефективної політики технологічний розрив між розвиненими країнами та країнами, що розвиваються, буде лише поглиблюватися, загострюватиметься соціальна нерівність та посилюватимуться деструктивні тенденції розвитку сільських регіонів. Для того, щоб створити інформаційне суспільство, недостатньо встановити комп'ютери та прокласти оптичні кабелі. Повинна бути розроблена низка регіональних та міжнародних угод, проведена реформа національних інформаційних політик та створена мережа інституцій, відповідальних за ефективний і справедливий розподіл благ всередині інформаційного суспільства.

ІКТ мають серйозний потенціал для посилення регіональних та глобальних інтеграційних процесів, оскільки вони можуть значно

31. Flor A. Developing Societies in the Information Age: A Critical Perspective / Alexander G. Flor. – Quezon City: The University of the Philippines Open University, 2009. – P. 13 – 14.

32. Herselman M. Challenges Posed by Information and Communication Technologies (ICT) for South African Higher Education Institutions [Електронний ресурс] / M. Herselman, H. Hay – Режим доступу: <http://proceedings.informingscience.org/IS2003Proceedings/docs/119Herse.pdf>.

скоротити транзакційні витрати, пов'язані із веденням внутрішньої регіональної торгівлі, підвищити прозорість регуляторних процедур та механізмів всередині держав, підтримати розвиток електронної торгівлі, прискорити обмін інформацією та здійснення електронних транзакцій, а також консолідувати наукову та технологічну співпрацю між державами відповідного регіону.

Втім, слід утримуватися від абсолютизації ролі ІКТ в регіональних та глобальних інтеграційних процесах. Значення, яке ІКТ відіграють в інтенсифікації співробітництва та розбудові інформаційного суспільства, цілком залежить від політичної волі та фінансової підтримки, які в свою чергу, визначають рівень конвергенції правових норм і стандартів, інфраструктурну інтеграцію, що забезпечує кращу взаємодію та об'єднання дослідницьких ресурсів, а також створює належні умови для розвитку людського потенціалу.

Цифрова революція сприяла поступовому зближенню очікувань різних верств суспільства та секторів економіки на глобальному рівні. Таке рідко трапляється в історії, щоб прагнення різних соціальних, політичних та фінансових груп співпадали у їх баченні подальшого розвитку людства, що ґрунтується на використанні переваг інформаційної ери. Ще раз наголосимо на тому, що ІКТ самі по собі не можуть вирішити проблеми, пов'язаних із забезпеченням зростання, рівності, демократії та справедливості. Вони відкривають перед міжнародним співтовариством величезні можливості, які можуть бути ефективно використані лише за умови, якщо народи, держави, регіони та світ в цілому продемонструють свою здатність розробити відповідні стратегії та створити інституції, головною метою яких буде забезпечення сталого розвитку, створення інформаційного суспільства рівних можливостей, у якому права людини визнаються найвищою соціальною цінністю.

Розбудова інформаційного суспільства неминуче призведе до посилення інформаційно-комунікаційної складової функціонування міжнародного співтовариства та життєдіяльності кожної окремо

взятої людини. В недалекому майбутньому можна буде спостерігати своєрідне роздвоєння середовища існування людини та держави. Відтак, все більшого значення набуватиме кіберпростір, який наразі містить в собі чимало поки що невіршених викликів праву на приватність та недоторканість особистого життя. Ще однією важливою характеристикою кіберпростору є взаємозумовленість та нерозривність технічної, інституційної та власне інформаційної складових.

Інформаційне суспільство передбачає унікальне поєднання демократичних інституцій, ефективних планів розвитку та політичних курсів, сприятливого для інновацій середовища, а також активного та структурованого громадянського суспільства.

Сьогодні світ переживає небачений раніше ріст багатокультурних суспільств. Процеси глобалізації та швидке поширення інформаційних технологій докорінно змінили парадигму людського спілкування. Налагодження міжкультурного діалогу і співпраці на засадах рівності та справедливості є ключовим завданням на шляху до побудови інформаційного суспільства. Об'єднання та згуртування в рамках інформаційного суспільства різноманітних гравців на міжнародній арені навколо єдиних загальнолюдських цінностей, що визнаються усім цивілізованим світом, дозволить вийти на якісно новий рівень розбудови міжнародних відносин у цифрову еру.

Інформаційне суспільство має величезний потенціал для налагодження міжкультурної комунікації та перетворення різновекторних, подекуди хаотичних зв'язків між сучасними суб'єктами міжнародних відносин на впорядкований мережевий механізм, що функціонує за чіткими законами. Подолання цифрового розриву дозволить суб'єктам, що наразі перебувають поза рамками глобального суспільства, стати повноправними членами глобального інформаційного суспільства³³.

Концепція глобалізації в контексті інформаційного суспільства

46 33. Measuring the Information Society [Електронний ресурс] // ITU. – 2013. – Режим доступу до ресурсу: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf.

передбачає відкритість кожного суб'єкта міжнародних відносин до зовнішньої взаємодії та поглиблення взаємовигідної співпраці, а також високий ступінь конвергенції самих соціальних систем. Стимуляторами сучасних інтеграційних процесів на глобальному ринку в більшості своїй виступають саме ІКТ.

Глобалізація матиме своїм наслідком суттєве переформатування суб'єктного складу інформаційного суспільства та зміщення важелів впливу. Так, держави продовжуватимуть залишатися основними акторами на міжнародній арені, однак до процесу нормотворення на рівних підставах будуть долучені представники громадянського суспільства, приватного сектору та міжнародних організацій. Останні в силу своєї транскордонної природи будуть відігравати ключову роль у глобалізованому, інклюзивному інформаційному суспільстві.

На противагу процесам глобалізації у світі виникла тенденція до регіоналізації міжнародних відносин. На нашу думку, розбудова глобального інформаційного суспільства неможлива без одночасного формування його національних та регіональних структур. Фактично, міжнародне співтовариство переживає транзитивний період, що передбачає зміщення акценту з індивіда як найвищої соціальної цінності на глобальну спільноту, у якій гарантуються рівні можливості для кожного.

Ініціативи, що імплементуються на національному рівні, повинні охоплювати якомога більше коло суб'єктів. Національні стратегії розвитку інформаційного суспільства повинні інтегрувати не лише регуляторну та технічну складову публічного сектору, але, що головне, долучити до процесу прийняття рішень та повноцінного партнерства приватний сектор, громадянське суспільство, регіональні та міжнародні організації. Важливо забезпечити такі умови формування національного інформаційного суспільства, які б не залежали від політичної волі та послідовно і ретельно виконувалися, незалежно від переформатування вищих керівних органів держави. Співробітництво з іноземними урядами, багатосторонніми кредитними організаціями,

торговими організаціями та іншими міжурядовими організаціями повинне розглядатися як стратегічний засіб для створення внутрішньодержавного інформаційного суспільства. Публічно-приватне партнерство та участь громадянського суспільства не повинні розглядатися виключно як розподіл функціональних обов'язків, коли від приватного сектора очікують фінансування, від громадянського суспільства — взяття на себе відповідальності, а держава при цьому виступає лише суб'єктом, що акумулює необхідні засоби та ресурси. У довгостроковій перспективі такий розподіл повноважень виявить свою абсолютну нежиттєздатність. З метою вироблення дієвої концепції інформаційного суспільства необхідно виробити та послідовно втілювати в життя спільне бачення можливих шляхів розвитку. Інтереси та потреби громадянського суспільства повинні бути орієнтиром при прийнятті рішень. Зосередженість приватного сектора на отриманні прибутку (принаймні в довгостроковій перспективі) повинна поважатися та враховуватися, в той час як держава і громадянське суспільство мають гарантувати, щоб жоден член чи група суспільства не виявилися поза загальним процесом розподілу благ.

Подібні національні стратегії розвитку інформаційного суспільства не потребують значної фінансової підтримки. Їх першочергове завдання полягає в об'єднанні зусиль, налагодженні взаємозв'язків, співпраці та координації між різними членами національного інформаційного суспільства, а також у забезпеченні участі кожного з них у прийнятті рішень.

Національні ініціативи повинні в першу чергу бути спрямовані на уникнення випадків дублювання прикладених зусиль та їх неузгодженості між собою. На жаль, наразі запровадження ІКТ в організаційну структуру різних секторів (е-врядування, е-медицина, е-навчання тощо) не інтегроване у традиційний процес їх реформування та відбувається паралельно із останнім. Робота у комп'ютерних лабораторіях часто не включена у традиційний навчальний розклад та функціонує на добровільних засадах поза

навчальним процесом. Таке розпорошення ресурсів є наслідком того, що будь-яке обговорення реформ зводиться до питань технологій та комп'ютеризації, натомість поза увагою залишаються адміністративна ефективність, транспарентність, управлінські та педагогічні підходи.

Процес формування інформаційного суспільства на національному рівні передбачає постановку чітких цілей з урахуванням інтересів та потреб усіх можливих суб'єктів, а також визначення строків та ресурсів, необхідних для їх досягнення. ІКТ мають потенціал для задоволення досить широкого кола потреб. Втім, дуже важливим з самого початку є вироблення національних ініціатив, які б зосереджувалися лише на деяких з них, щоб уникнути плутанини та втрати чітких орієнтирів, що зрештою призводить до демотивації населення, згасання політичної та фінансової підтримки таких програм розвитку.

Національні стратегії формування інформаційного суспільства повинні неминуче враховувати міжнародний аспект. Транснаціональний характер Інтернету вимагає, щоб будь-які ініціативи з розбудови суспільства нового типу не обмежувалися державними кордонами. Надзвичайно важливо, щоб національні політики узгоджувалися з відповідними регіональними та глобальними тенденціями розвитку. Крім того, держави, що розвиваються повинні мати можливість брати безпосередню участь у розробці відповідних ініціатив та отриманні переваг від їх реалізації. Інформаційне суспільство повинно стати суспільством рівних можливостей, де кожен його член буде відчувати свою важливість та причетність до прийняття усіх рішень, які зачіпають навіть найменш значущі його інтереси.

Починати формування інформаційного суспільства необхідно саме з національного та регіонального рівнів, оскільки технічні зміни та стратегії розвитку тісно взаємопов'язані з конкретними фізичними, історичними, соціальними та інституційними умовами. У спадок від індустріального суспільства різним народам, державам та регіонам залишилися різні умови, що закладуть основу для стартових позицій на шляху до формування глобального інформаційного суспільства.

Для того, щоб забезпечити повноцінне та абсолютне використання усіх наявних ресурсів, необхідно долучити до розбудови суспільства нового типу усіх його потенційних членів, яким до того ж такі ресурси належать³⁴.

Первинною метою розробки регіонального вектора співробітництва є інтенсифікація взаємодії між тими суб'єктами міжнародних відносин, що мають спільні або подібні вихідні дані (територіальне розташування, історичний розвиток, економічні та технічні умови тощо), що, по-перше, полегшує налагодження діалогу між ними, а по-друге, інтегруючи їх, дозволяє останнім виступати єдиною внутрішньо організованою силою при відстоюванні своїх інтересів на глобальному рівні, що значно посилює їх шанси бути почутими, особливо коли мова йде про держави, що розвиваються.

Міжнародні організації повинні активно працювати над розробкою стандартів, що будуть покладені в основу функціонування глобального інформаційного суспільства, а також виступати як форум для інтенсифікації співробітництва між державами, приватним сектором та громадянським суспільством. Прийняття будь-якої узгодженої стратегії повинно супроводжуватися розробкою відповідної нормативно-правової бази та чітким окресленням обсягу прав і відповідальності усіх суб'єктів міжнародних відносин, чий інтереси така стратегія може зачіпати.

Глобальне інформаційне суспільство є надзвичайно комплексним явищем, а тому потребує особливо ретельного підходу до розробки нормативно-правового забезпечення його функціонування. Так, врегулювання потребує технічна інфраструктура (телекомунікації, технічне та програмне забезпечення), взаємодія суб'єктів міжнародних відносин у кіберпросторі та забезпечення прав людини у цифровому середовищі. Наразі регулювання окреслених вище питань є відмінним у різних державах, що може бути пояснено неоднаковим рівнем їх технологічного розвитку та економічного зростання. Розбудова

34. Hilbert M. Building an Information Society: A Perspective from Latin America and the Caribbean / M. Hilbert, J. Katz. – Santiago, Chile, 2003. – P. 221 – 224.

інклюзивного глобального інформаційного суспільства потребує уніфікації нормативно-правового регулювання в усіх секторах та запровадження єдиних стандартів співробітництва, що гарантували б рівність можливостей та враховували інтереси усіх суб'єктів. Імовірно, одним із найскладніших завдань буде віднайти баланс між сталим розвитком та здоровою конкуренцією.

Вироблення універсального механізму нормативно-правового забезпечення розвитку інформаційного суспільства передбачає запровадження глобального правового режиму у визначених сферах взаємодії суб'єктів міжнародних відносин. Водночас процеси регіоналізації та вироблення відповідного масиву міжнародно-правових норм на рівні регіональних об'єднань можуть відбуватися паралельно із процесом глобалізації. Подекуди регіональні ініціативи можуть бути більш економічно виправданими та оперативнішими завдяки спільності середовища та спорідненості умов, у яких розвиваються та функціонують суб'єкти міжнародних відносин кожного окремого регіону. Зважаючи на те, що інформаційне суспільство нівелює значення кордонів у їх традиційному розумінні, все ще зберігається чимало підстав саме для регіональної інтеграції. Так, держави продовжують об'єднуватися у союзи за ознакою рівня їх технологічного розвитку і лише згодом виступають єдиним фронтом у процесі відстоювання своїх прав та інтересів у переговорах з розвинутими державами. Останні задля збереження своєї гегемонії не надто прагнуть до подолання цифрового розриву, що є одним з найбільших викликів інформаційному суспільству. Адже лише вирівнявши рівень розвитку всіх країн світу, можна буде створити суспільство загального добробуту. Якщо цього не буде зроблено, інформаційне суспільство стане ще однією суспільною формацією, яка вкотре закріпить вже історично традиційний принцип панування розвинених країн над тими, що розвиваються. Зміни, таким чином, будуть зведені лише до інструментарію, за допомогою якого таке панування буде підтримуватися.

В основі регіональної інтеграції не завжди можна відшукати «благі»

мотиви. Так, держави, що не володіють достатніми засобами, щоб бути почутими на глобальному рівні, цілком можуть задовольнити своє самолюбство через регіональне лідерство³⁵. Регіональні гегемони, як правило, задовольняють базові потреби та ключові вимоги інших держав, що входять до складу відповідного регіонального об'єднання, з єдиною метою — отримання в їх особі підтримки власних ініціатив, що позиціонуються як такі, що несуть загальне благо, та нарощування за їх рахунок власного багатства та впливовості. В свою чергу, глобальні ініціативи більше орієнтовані на досягнення абсолютних цілей.

Надзвичайно складно виробити ефективні та справедливі механізми нормативно-правового регулювання розвитку глобального інформаційного суспільства. Слід чітко усвідомлювати, що універсальні документи, які розробляються ООН, є дієвими настільки, наскільки вони імплементовані у національне законодавство. Це свідчить про необхідність пошуку нових, більш практичних регуляторних засобів, які б максимально враховували транскордонну природу Інтернету. Для регулювання останнього більш виправданим та придатним є саме глобалізований підхід, що повинен сприяти уніфікації нормативно-правового регулювання та подоланню його фрагментації. Національна монополія на регулювання Інтернету стримує розвиток ІКТ всередині країни та гальмує її інтегрування в глобальне інформаційне суспільство.

Інтернет та інформаційне суспільство є глобальними феноменами, а отже й відповідне нормативно-правове регулювання повинно базуватися не лише на національному законодавстві та регіональних домовленостях, але й поступово виходити на глобальний рівень, де буде забезпечена багатостороння участь усіх зацікавлених сторін. Для того, щоб нормативно-правове забезпечення розвитку інформаційного суспільства було ефективним, останнє має бути глобальним за своєю природою.

Глобалізація зумовлює необхідність перегляду зафіксованих

та жорстких меж між національною та міжнародною сферами регулювання, тим самим змінюючи наше уявлення про належність тієї чи іншої групи міжнародних відносин до відповідної сфери регулювання³⁶. Наразі можемо спостерігати більш гнучкий підхід до нормативно-правового регулювання, який передбачає відхід від ідеї, згідно з якою право повинне походити з єдиного владного джерела, яким є суверен³⁷. Процес глобалізації регуляторного механізму можна певним чином охарактеризувати як націоналізацію міжнародного права у тому розумінні, що виробляються єдині для всіх суб'єктів стандарти, дотримання та виконання яких презюмується вже внаслідок їх прийняття і не потребує подальшої національно-правової імплементації. Оскільки у глобальному інформаційному суспільстві немає кордонів як таких, то не повинно бути і будь-яких обмежень для нормативно-правового регулювання через якісь причини. Тенденція до збереження розмежування національного та міжнародного права досить швидко втрачатиме свою актуальність у глобалізованому кіберпросторі. Пріоритетними формами регулювання повинні стати універсальні стандарти та саморегулювання.

Наразі можна виділити чотири основні конкуруючі регуляторні механізми у кіберпросторі:

- 1) національно-правове регулювання сфери телекомунікацій;
- 2) саморегулювання на рівні окремих компаній чи корпорацій або їх об'єднань;
- 3) двосторонні (міжрегіональні) угоди між ЄС та його країнами-членами із США або між окремими компаніями;
- 4) багатосторонні переговорні платформи, наприклад ОЕСР, ICANN, СОР, ООН.

В умовах глобального інформаційного суспільства національне

36. Jayasuriya K. Globalization, Law, and the Transformation of Sovereignty: The Emergence of Global Regulatory Governance / Kanishka Jayasuriya // Indiana Journal of Global Legal Studies. – 1999. – № 6.

37. McCormick P. Private sector influence in the International Telecommunication Union / Patricia K. McCormick // The journal of policy, regulation and strategy for telecommunications, information, and media. – 2007. – № 9. – Pp. 70–80.

законодавство виявиться абсолютно неефективним та недієвим регулятором. Інтернет є глобальною мережею завдяки своїй природі й не може бути обмежений будь-якими національними кордонами. Безперечно, доступ надається за локальною прив'язкою, втім, контент однозначно є транскордонним. Це свідчить про неприпустимість фрагментації нормативно-правового регулювання Інтернету, який з самого початку створювався як вільний простір, що знаходиться поза рамками державного регулювання. Втім, така правова невизначеність досить швидко призвела до того, що технічно розвинені країни почали розвиватися шаленими темпами, стримуючи при цьому розвиток країн третього світу з метою закріплення свого домінуючого становища, уникнення конкуренції та резервування за собою права диктувати правила поведінки у цифровому середовищі.

Наразі відсутня зацікавленість суб'єктів міжнародних відносин в універсальному міжнародно-правовому регулюванні питань розвитку Інтернету. Саме тому переважна більшість документів, що регулюють відносини в глобальній мережі, належать до м'якого права. Нормативно-правове регулювання Інтернету намагаються побудувати за принципом домінування сильніших акторів над слабшими. Втім, зрештою слабші приходять до розуміння свого дискримінаційного становища та порушують питання про перегляд існуючих регуляторних рамок.

Концепція Інтернету виходить з принципу рівності усіх зацікавлених сторін. Втім, досі не вироблено збалансованої моделі взаємодії цих сторін, яка б чітко визначала обсяг прав та межі відповідальності кожної з них. Ключовим гравцям на міжнародній арені значно легше домовитися з інфраструктурних та технічних аспектів, аніж знайти спільну мову у питаннях управління Інтернетом, захисту прав людини та інтелектуальної власності, дозволеного та забороненого контенту.

54 Гарантування та захист прав людини повинні визнаватися ключовою цінністю в мережі Інтернет. Однак, негативним моментом є те, що в контексті прав людини акцент завжди робиться виключно

на питаннях доступу. Поза увагою залишається необізнаність та не усвідомлення кінцевими користувачами механізму управління Інтернетом. Допоки у користувачів є можливість використання відкритого та доступного Інтернету, мало хто з них задумується над тим, яким чином гарантується та забезпечується такий доступ.

Індивіди як кінцеві користувачі не проявляють зацікавленості та не беруть участі у тих процесах, які, на їх думку, не мають до них прямого стосунку. Щоб відбувся переворот у свідомості людей, потрібен потужний поштовх. Перш за все, слід проводити послідовну та продуману роз'яснювальну роботу серед кінцевих користувачів з тим, щоб вони чітко усвідомили, що Інтернет не зводиться до соціальних та пошукових мереж. Відповідно і проблеми, пов'язані з виробленням універсальних регуляторних механізмів, є надзвичайно серйозними. Враховуючи стрімкі темпи розвитку інформаційно-комунікаційних технологій, ніхто не може передбачити, коли питання управління Інтернетом дійсно дійде до критичної точки. Зрозуміло лише одне: не можна зволікати зі створенням відповідного універсального нормативного забезпечення.

Неспроможність ключових гравців домовитися про принципи та механізми універсального управління Інтернетом закладають небезпечні основи для фрагментації Інтернету, що суперечить самій природі глобальної мережі. Відсутність глобального багатостороннього регулювання спричинила появу такого феномена, як саморегулювання, в основу якого завжди покладається задоволення певного корпоративного інтересу та просування компаніями власних цілей на масштабних переговорних платформах. Нерозуміння важливості вироблення єдиних правил поведінки для всіх суб'єктів, що так чи інакше взаємодіють у рамках інформаційного суспільства, рано чи пізно призведе до того, що внаслідок зростання долі саморегулювання відбудеться проста заміна американських цінностей (США впродовж тривалого часу лишалися гегемоном в інформаційній сфері) на цінності транснаціональних корпорацій, роль яких стрімко зростає.

Міжнародні організації, у свою чергу, також породжують додаткові перешкоди на шляху до створення універсального регуляторного механізму, що пояснюється їх традиційним міжсекторальним суперництвом. На регіональному рівні конкуруючі погляди на інформаційне суспільство мають ЄС та Рада Європи. ЄС керується в першу чергу принципом економічної доцільності, що закріплений Римським договором та подальшими змінами до нього. Натомість, Рада Європи орієнтована перш за все на виконання положень Європейської конвенції з прав людини, зокрема, забезпечення права на приватність та свободи слова. На багатосторонньому рівні можна виділити три конкуруючі позиції в рамках ООН, що відстоюються відповідно ЮНЕСКО (розвиток культури та захист культурної спадщини), ЮНКТАД (економічна ефективність та справедливість) та МСЕ (технологічний розвиток та співпраця)³⁸. Таким чином, в інформаційному суспільстві глобальне регулювання виникає у відповідь на вже існуючі практичні проблеми. Тобто, причинно-наслідковий зв'язок простежується у напрямку породження глобалізацією як об'єктивним процесом нових технологічних та контентних викликів, реакцією на які і повинен бути «живий» глобальний регуляторний механізм.

Розвиток ІКТ є настільки стрімким, що глобальний регуляторний механізм повинен встигати оперативно та перманентно відображати відповідні зміни на нормативному рівні. Саме тому вважаємо, що такий механізм повинен виконувати роль живого організму, який реагує на будь-які серйозні подразники зовнішнього світу. Для характеристики екосистеми, що створюється в рамках глобального інформаційного суспільства, доречно провести аналогію з імунною системою організму людини. Для підтримання стабільного функціонування останньої потрібно докладати певні зусилля для профілактики захворювань та запобігання збоям у функціонуванні будь-якого з органів. Те саме стосується і глобального інформаційного суспільства: для успішного, взаємовигідного співробітництва усіх зацікавлених суб'єктів потрібно,

перш за все, виробити єдині стандарти взаємодії, щоб в подальшому уникнути ймовірних зловживань. Суб'єкти міжнародних відносин настільки тісно взаємопов'язані в умовах інформаційного суспільства, що будь-які перекоси на користь будь-кого з них неминуче негативно відобразяться на всіх інших. Натомість, якщо приділяти належну увагу кожному суб'єкту та компоненту інформаційного суспільства, в кінцевому підсумку підвищиться функціональність та ефективність усього «інформаційного організму».

Найбільша складність, пов'язана з формуванням глобального інформаційного суспільства, полягає у виробленні єдиних правових стандартів взаємодії усіх зацікавлених суб'єктів міжнародних відносин та пошуку найбільш ефективних регуляторних механізмів. У глобальному вимірі правова основа функціонування інформаційного суспільства повинна бути достатньо стійкою, щоб гарантувати стабільність кіберпростору. В той же час, вона повинна знаходитися у режимі постійного реагування на технологічний прогрес та відображати відповідні зміни на нормативному рівні. Крім того, потрібно забезпечити максимальну технологічну нейтральність глобального правового регулювання та уникати надмірної деталізації нормативних положень. Нормативно-правове забезпечення суспільних відносин у глобальному інформаційному суспільстві має бути стандартизованим за своєю природою та окреслювати допустимі види поведінки й дозволені рамки взаємодії усіх категорій зацікавлених суб'єктів. Вважаємо за доцільне вести мову саме про глобальний регуляторний механізм, оскільки фрагментація нормативно-правового регулювання інформаційного суспільства за регіональною чи національною ознакою сприятиме існуванню кількох центрів впливу у кіберпросторі та дискримінаційному становищу менш впливових гравців. Глобальність інформаційного суспільства вимагає глобальних стандартів регулювання. Зрозуміло, що в силу технологічних, культурних, історичних умов розвитку різних держав та народів буде складно забезпечити абсолютну внутрішню єдність інформаційного суспільства. Саме тому доречно говорити про сегментацію глобального

інформаційного суспільства (європейський, американський, азійський сегменти тощо), яка проявлятиметься в адаптації універсальних стандартів до конкретних умов, пов'язаних з рівнем розвитку відповідного суб'єкта в межах певного регіону. У той же час, поняття сегментації повинно використовуватися лише для зручності і зникнути по завершенню транзитивного періоду, що знадобиться світові для переходу до системи взаємодії на основі універсальних принципів, що створюють рівні можливості для кожного.

Якщо з самого початку зусилля міжнародної спільноти будуть сконцентровані на виробленні національних та регіональних стандартів, то протиріччя, які об'єктивно існують між існуючими регіональними системами з їх центрами впливу, завжди стоятимуть на перешкоді виробленню універсального правового регулювання глобального інформаційного суспільства. Наразі вже окреслилась така тенденція до регіоналізації. На сучасному етапі відповідні регіональні напрацювання ще можна використати для загального блага, втім уже завтра зараз знайти компроміс буде не так просто. Якщо ж найближчим часом процес обговорення не буде виведений на глобальний рівень, то протиріччя між ключовими гравцями будуть поступово лише загострюватись, а боротьба за контроль над Інтернетом та кіберпростором в цілому може мати непередбачувані наслідки. Як показує досвід багатьох міжнародних організацій, процес гармонізації нормативно-правового регулювання може бути надзвичайно дискусійним та затяжним. З огляду на це, вважаємо за доцільне розпочати формування стандартів з широкого суспільного обговорення на глобальному рівні, допоки окремі суб'єкти ще не виробили власних жорстких позицій, що могли б завадити їм прийти до вироблення спільного загальноприйнятого нормативно-правового забезпечення розвитку глобального інформаційного суспільства.

58 Наразі розрізняють чотири можливі шляхи розвитку регулювання інформаційного простору:

1. Доктрина абсолютної свободи: відкидає ідею регулювання медіа

як таку. З поширенням нових цифрових технологій, зокрема Інтернету, прихильників цього підходу побільшало серед національних суб'єктів регулювання (винятком є Австралія), що можна пояснити в першу чергу відсутністю необхідних знань та неготовністю взяти на себе відповідальність за розробку стандартів поведінки у новій сфері суспільних відносин. За абсолютну свободу від регулювання виступають також широкі маси безпосередніх користувачів, які отримують певні переваги від користування відкритими комунікаційними системами. Втім, як показує досвід використання медіа технологій попередніх поколінь, відкритий доступ повинен відповідним чином регулюватися з метою попередження зловживань. Відсутність регуляторного механізму призведе, зрештою, до обмеження доступу та комунікації.

2. Саморегулювання: найчастіше на його користь виступають самі ІТ-компанії та виробники контенту, які вбачають у ньому вирішення проблем, пов'язаних з образливим контентом та захистом прав користувачів. Однак, як свідчать ініціативи у сферах авторського права та електронної торгівлі, навіть прихильники саморегулювання погоджуються з необхідністю створення глобальної структурованої мережі, в рамках якої відбувалася б комунікативна активність, не остання роль у впорядкуванні якої відводилася б саморегулюванню;
3. Закритий клуб чи інституційна модель, побудована за принципом «зверху-донизу»: цей підхід спрямований на заповнення прогалін, спричинених ухилянням національних урядів від вирішення регуляторних питань. Відповідні рішення розробляються в рамках Організації економічної співпраці та співробітництва (ОЕСР), Великої вісімки (G8), СОТ, а також новими інституціями, що формуються в корпоративному секторі. Це може створити ситуацію, коли найбільш сильні економічно суб'єкти будуть диктувати правила гри усім іншим, а медіа сприйматимуть як бізнес, засоби розваги та тотального контролю над публічною інформацією;

4. Інституційний підхід: в основу покладено демократизацію глобального управління, що знаходить своє відображення в окремих ініціативах ООН та концепції «космополітичної демократії». Доступ громадянського суспільства до участі у процесах на зразок Всесвітнього саміту з інформаційного суспільства (ВСІС) є надзвичайно важливим для побудови цієї регуляторної моделі, що сприятиме багатосторонності та різноманітності медіа, а зрештою — й участі громадськості у вирішенні питань публічного життя³⁹.

Найбільш життєздатним та демократичним є саме останній підхід, побудований на принципі багатосторонньої участі всіх зацікавлених суб'єктів у вирішенні питань, що їх безпосередньо стосуються, можуть стосуватися у майбутньому, або на їх власне переконання, є такими, що можуть прямо чи опосередковано зачіпати їх інтереси. При цьому таке обговорення повинне відбуватися на глобальному рівні на основі певної міжнародної платформи. Позитивним прикладом такого дискусійного форуму можна вважати ВСІС.

Діалог з питань глобального інформаційного та комунікаційного порядку розпочався в рамках Міжнародного союзу електров'язку (МСЕ) із прийняття у 1998 році резолюції, у якій ішлося про проведення під егідою ООН ВСІС⁴⁰. У 2001 році Рада МСЕ запропонувала проведення Саміту у два етапи: першого — в Женеві у 2003 році, другого — в Тунісі двома роками пізніше⁴¹. Генеральна Асамблея ООН прийняла Резолюцію 56/183, у якій прописувалася основна мета ВСІС — розвиток міжнародного універсального бачення та розуміння інформаційного суспільства, а також прийняття декларації основних принципів, на яких повинно будуватися глобальне в контексті членства та розподілу переваг інформаційне суспільство.

Ключовими питаннями, які мали б розглядатися в ході ВСІС, 39. Raboy M. Media and Democratization in the Information Society / M. Raboy // Communicating in the Information Society, edited by Bruce Girard and Sean O Siochru. - Geneva: UNRISD, 2003. - P. 113.

60 40. Resolution 73 of the ITU Plenipotentiary Conference [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: <https://www.itu.int/wsis/docs/background/resolutions/73.html>

41. Resolution 1179, ITU Council [Електронний ресурс]. – 2001. – Режим доступу до ресурсу: <http://www.itu.int/wsis/docs/background/resolutions/1179.html>

були: управління Інтернетом, безпека, вільне та відкрите програмне забезпечення, комунікаційні права, інтелектуальна власність, права людини та фінансування.

Однозначно позитивним аспектом у роботі WSIS став багатосторонній характер його учасників, серед яких були представники урядів, міжнародних організацій, приватного сектору та громадянського суспільства. Втім, лише представники національних урядів мали право голосу, усі інші надіялися статусом спостерігачів. Представники бізнес-структур, хоч і становили меншість, але отримали змогу взяти участь завдяки стратегічному партнерству.

Під час першого етапу Саміту в Женеві у грудні 2003 року було прийнято Женевську декларацію принципів⁴² та Женевський План дій⁴³, які описують загальне бачення інформаційного суспільства та кроки, до яких варто вдатися для його побудови на глобальному рівні. У ході роботи у Тунісі учасниками цього етапу Саміту було затверджено Туніське зобов'язання⁴⁴ та Туніський план дій⁴⁵, у яких окреслювалися кроки по управлінню Інтернетом та наводилося робоче визначення управління Інтернетом.

Питання управління Інтернетом виявилось надто складним для остаточного врегулювання на першому етапі WSIS, тому його розгляд було відкладено до зустрічі в Тунісі у 2005 році. Тим часом було прийнято рішення створити відкриту Робочу групу з питань управління Інтернетом для детального вивчення питання та вироблення відповідних рекомендацій. У Женевському Плані дій ішлося про необхідність сформулювати робоче визначення поняття “управління Інтернетом”. Після завершення першого етапу Саміту гострі дискусії щодо необхідності докорінного перегляду механізмів

42. Geneva Declaration of Principles, 12 December 2003 [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.itu.int/wsis/docs/geneva/official/dop.html>.

43. WSIS: Plan of Action, 12 December 2003 [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.itu.int/wsis/docs2/tunis/off/7.html>.

44. WSIS: Tunis Commitment, 18 November 2005 [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.itu.int/wsis/docs2/tunis/off/7.html>.

45. WSIS: Tunis Agenda for the Information Society, 18 November 2005 [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

управління глобальною мережею не припиняються. Країни, що розвиваються, висловлюють стурбованість та невдоволення фактичним зосередженням усієї повноти контролю над Інтернетом в руках США, які реалізують свою інформаційну політику за посередництва ICANN.

У липні 2005 року Робоча група видає рекомендацію про необхідність інтернаціоналізувати сферу управління Інтернетом, на що США відповідають офіційною заявою, яка містить їх відмову поступатися домінуючим становищем у цій сфері. Крім того, було досягнуто домовленості щодо створення Форуму по управлінню Інтернетом (IGF) у вигляді багатосторонньої платформи для обговорення питань публічної політики у сфері Інтернету. В свою чергу, Генеральний Секретар ООН змушений був розпочати так званий процес посиленої співпраці між урядами із залученням усіх зацікавлених сторін з метою забезпечення управління критичними інтернет-ресурсами відповідно до принципів, сформульованих у ході Женевського етапу Саміту.

Постежимо, як світова спільнота підійшла до створення нового майданчика для багатостороннього діалогу з питань формування політики у сфері Інтернету. Форум по управлінню Інтернетом створювався як відкрита платформа для участі всіх зацікавлених сторін, які мали спільними зусиллями визначати формат його діяльності, структуру, а також самостійно вирішувати, які питання належать до сфери його компетенції. Перше засідання IGF відбулося в Афінах у 2006 році. На ньому були присутні представники громадянського суспільства, приватного сектора, урядів та міжнародних організацій. Відкритість Форуму для всіх бажаючих та відсутність будь-яких процедурних правил щодо прийняття рішень значною мірою сприяли налагодженню конструктивного діалогу між учасниками⁴⁶.

Форуму вдалося заповнити той інституційний вакуум, що існував

62 46. Malcolm J. Appraising the Success of the Internet Governance Forum (21st November 2008) [Електронний ресурс] / J. Malcolm. – Режим доступу до ресурсу: <http://www.internetgovernance.org>.

у сфері управління Інтернетом. Вперше вдалося створити рівні умови для участі в обговоренні актуальних питань усіма зацікавленими сторонами, особливо представниками громадянського суспільства, які отримали реальну можливість впливати на формування політики в сфері Інтернету. Втім, IGF є доволі новим утворенням, якому ще належить подолати чимало труднощів, доки він зможе стати по-справжньому впливовим механізмом управління на міжнародній арені. Причинами для критики часто стають відсутність реальних важелів впливу через прийняття юридично обов'язкових рішень. Наразі Форум швидше нагадує платформу для обміну думками та ведення дискусій. Розвинені країни продовжують надавати перевагу випробуваням часом та надійним механізмам прийняття рішень на міжурядовому рівні. Однак, IGF принаймні дозволяє сформувати єдине бачення та розуміння ключових питань розвитку суспільства в інформаційну еру.

У червні 2014 році відбулася підсумкова зустріч на вищому рівні «WSIS+10» у штаб-квартирі МСЕ в Женеві (їй передували 6 попередніх погоджувальних зустрічей), на якій розглядалися здобутки й проблеми, пов'язані з втіленням ідей та реалізацією завдань, закріплених у чотирьох фінальних документах Саміту у 2003 та 2005 рр., а також обговорювалися пропозиції щодо нового бачення розвитку інформаційного суспільства після 2015 року. У ході зустрічей було розроблено й затверджено два фінальні документи — Доповідь WSIS+10 про імплементацію підсумків WSIS та Бачення WSIS+10 розвитку WSIS після 2015 року⁴⁷.

У своїй резолюції A/RES/68/302 від 31 липня 2014 року⁴⁸ Генеральна Асамблея ООН ухвалила провести у грудні 2015 року дводенне засідання на вищому рівні з метою оцінки здобутків WSIS

47. WSIS+10 Outcome Documents. – Geneva: ITU, 2014. – 49 p. [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf>.

48. UN GA Resolution 68/302 'Modalities for the overall review by the General Assembly of the implementation of the outcomes of the World Summit on the Information Society' dated 31 July 2014 [Електронний ресурс]. – Режим доступу до ресурсу: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/302

та імплементації підсумкових документів Саміту. У ході проведення 69-ї сесії ГА ООН її Другий комітет розгляне здобутки ВСІС та питання продовження мандату IGF, що повинен проходити процедуру поновлення кожні п'ять років (вперше наданий у 2006 р., поновлений — у 2010 р.). Ключовими проблемними моментами є джерела фінансування та надання IGF безстрокового мандату. Крім того, в рамках Першого комітету обговорять резолюцію про кібербезпеку та засоби зміцнення довіри, а робота Третього комітету включатиме, серед іншого, проблеми приватності, контролю та прав людини⁴⁹.

Ще однією важливою подією, що претензійно заявила про себе у сфері управління Інтернетом, стала Глобальна багатостороння зустріч, присвячена майбутньому управлінню Інтернетом — *NETmundial*, яка відбулася в Бразилії у квітні 2014 року. Співорганізаторами Зустрічі виступили Керівний комітет Бразилії з питань Інтернету (CGI.br) та /1Net — форум, що об'єднує представників різних секторів, що займаються управлінням Інтернету. Підсумковими документами *NETmundial* стали «Принципи управління Інтернетом» та «Дорожня карта подальшої еволюції екосистеми управління Інтернетом»⁵⁰.

Доволі активно розвивається регулювання окремих аспектів інформаційного суспільства в його європейському сегменті. Так, в рамках Ради Європи були прийняті:

- Конвенція про кіберзлочинність від 23 листопада 2001 року⁵¹;
- Додатковий протокол до Конвенції про кіберзлочинність щодо кримінальної відповідальності за акти расистського і ксенофобського характеру, що здійснюються через комп'ютерні системи від 28 січня 2003 року⁵²;

49. Agenda of the UN GA 69th Regular Session [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.un.org/en/ga/69/agenda/>

50. NETmundial Multistakeholder Statement dated April 24, 2014 [Електронний ресурс]. – Режим доступу до ресурсу: <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>

51. Convention on Cybercrime, 2001 [Електронний ресурс]. – Режим доступу до ресурсу: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

52. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003 [Електронний ресурс]. –

- Конвенція про захист фізичних осіб при автоматизованій обробці персональних даних від 28 січня 1981 року⁵³ та Додатковий протокол до Конвенції щодо органів нагляду і транскордонних потоків даних від 8 листопада 2001 року⁵⁴;
- Конвенція про інформаційне та правове співробітництво, що стосується «Послуг інформаційного суспільства» від 4 жовтня 2001 року⁵⁵;
- Конвенція про правовий захист послуг, що базуються на / чи складаються з умовного доступу від 24 січня 2001 року⁵⁶;
- Конвенція про захист прав людини та основоположних свобод, доповнена Протоколом № 11 від 1 листопада 1998 року⁵⁷;
- Рекомендація Комітету Міністрів країнам-членам Ради Європи CM/Rec(2008)6 про заходи стимулювання дотримання свободи самовираження та інформації у зв'язку з Інтернет-фільтрами від 26 березня 2008 року⁵⁸;
- Рекомендація Комітету Міністрів CM/Rec(2007)16 про засоби підвищення цінності Інтернету як суспільної служби від 7 листопада 2007 року⁵⁹;

Режим доступу до ресурсу: <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.

53. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981 [Електронний ресурс]. – Режим доступу до ресурсу: <http://conventions.coe.int/Treaty/en/Treaties/html/108.htm>

54. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 2001 [Електронний ресурс]. – Режим доступу до ресурсу: <http://conventions.coe.int/Treaty/en/Treaties/html/181.htm>

55. Convention on Information and Legal Co-operation concerning «Information Society Services», 2001 [Електронний ресурс]. – Режим доступу до ресурсу: <http://conventions.coe.int/treaty/en/Treaties/Html/180.htm>

56. European Convention on the Legal Protection of Services based on, or consisting of, Conditional Access, 2001 [Електронний ресурс]. – Режим доступу до ресурсу: <http://conventions.coe.int/Treaty/en/Treaties/Html/178.htm>

57. Convention for the Protection of Human Rights and Fundamental Freedoms, 1950 [Електронний ресурс]. – Режим доступу до ресурсу: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=1/16/2009&CL=ENG>

58. Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, 2008 [Електронний ресурс]. – Режим доступу до ресурсу: [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2008\)6&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75)

59. Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, 2007 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&B>

- Рекомендація Комітету Міністрів *CM/Rec(2007)11* про підтримку свободи самовираження та інформації в новому інформаційно-комунікаційному середовищі від 26 вересня 2007 року⁶⁰;
- Рекомендація Комітету Міністрів *CM/Rec(2007)3* про компетенцію суспільних засобів масової інформації в інформаційному суспільстві від 31 січня 2007 року⁶¹;
- Рекомендація Комітету Міністрів *Rec(2004)15* про електронне державне управління («e-врядування») від 15 грудня 2004 року⁶²;
- Рекомендація Комітету Міністрів *Rec(2002)12* про виховання демократичної громадської позиції від 16 жовтня 2002 року⁶³;
- Рекомендація Комітету Міністрів *Rec(2002)1* про ключові принципи стійкого просторового розвитку європейського континенту від 30 січня 2002 року⁶⁴;
- Декларація Комітету Міністрів про права людини та верховенство права в інформаційному суспільстві від 13 травня 2005 року⁶⁵;
- Декларація Комітету Міністрів про європейську політику у сфері

ackColorIntranet=FFBB 55&BackColorLogged=FFAC75

60. Recommendation CM/Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, 2007 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=1188541&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB 55&BackColorLogged=FFAC75>

61. Recommendation CM/Rec(2007)3 of the Committee of Ministers to member states on the remit of public service media in the information society, 2007 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=1089759&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB 55&BackColorLogged=FFAC75>

62. Recommendation Rec(2004)15 of the Committee of Ministers to member states on electronic governance («e-governance»), 2004 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=802805&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB 55&BackColorLogged=FFAC75>

63. Recommendation Rec (2002)12 of the Committee of Ministers to member states on education for democratic citizenship, 2002 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=313139&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB 55&BackColorLogged=FFAC75>

64. Recommendation Rec(2002)1 of the Committee of Ministers to member states on the Guiding principles for sustainable spatial development of the European Continent, 2002 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=257311&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB 55&BackColorLogged=FFAC75>

65. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, 2005 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=849061&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB 55&BackColorLogged=FFAC75>

- нових інформаційних технологій від 7 травня 1999 року⁶⁶;
- Резолюція Парламентської Асамблеї 1191 (1999) «Інформаційне суспільство та цифровий світ» від 26 травня 1999 року⁶⁷;
 - Рекомендація Конгресу місцевих та регіональних влад РЄ 54 (99) про інформаційне суспільство на місцевому та регіональному рівні від 16 червня 1999 року⁶⁸ тощо.

Медіа реформи є одним із зобов'язань України перед Європейським Союзом у рамках виконання Угоди про асоціацію, що була синхронно ратифікована сторонами у вересні 2014 року. Глава 14 Угоди (ст.ст. 389-395) присвячена інформаційному суспільству. У ній, зокрема, зазначається, що сторони зміцнюють своє співробітництво з розвитку інформаційного суспільства на користь приватних осіб і бізнесу через забезпечення загальнодоступності ІКТ та через кращу якість послуг за доступними цінами, що, в свою чергу, полегшить доступ до ринків послуг електронних комунікацій і сприятиме конкуренції й надходженню інвестицій у цю галузь.

Співробітництво має на меті імплементацію національних стратегій інформаційного суспільства, розвиток всеохоплюючої нормативно-правової бази для електронних комунікацій та розширення участі України у дослідницькій діяльності ЄС у сфері ІКТ. Сторони сприяють поступовому наближенню до права і нормативно-правової бази ЄС у галузі регулювання інформаційного суспільства і електронних комунікацій⁶⁹.

66. Declaration of the Committee of Ministers on a European policy for new information technologies, 1999 [Електронний ресурс]. – Режим доступу до ресурсу: <http://wcd.coe.int/ViewDoc.jsp?id=448133&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>

67. Resolution 1191 (1999) Information society and a digital world [Електронний ресурс] // Official Gazette of the Council of Europe. – May 1999. – Режим доступу до ресурсу: <http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta99/ERES1191.htm>

68. Resolution 1191 (1999) Information society and a digital world [Електронний ресурс] // Official Gazette of the Council of Europe. – May 1999. – Режим доступу до ресурсу: <http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta99/ERES1191.htm>

69. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]. – Режим доступу до ресурсу: [http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_\(body\).pdf](http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_(body).pdf)

На виконання Угоди про асоціацію Україна повинна забезпечити поступове приведення своїх чинних законів та майбутнього законодавства у відповідність до *acquis* ЄС. Зокрема, спеціальні терміни адаптації для кожного індивідуального акта викладені для телекомунікаційних послуг у Додатку XVII-3 Додатку XVII до Розділу IV Угоди⁷⁰, а для аудіовізуальних послуг – у Додатку XXXVII до Глави 15 Розділу V Угоди⁷¹.

На початку жовтня 2014 року в Києві відбулась презентація спільного проекту ЄС та Ради Європи «Зміцнення інформаційного суспільства в Україні», який має на меті зміцнення відкритого, інклюзивного, сталого підходу до управління Інтернетом, що ґрунтується на правах людини, а також сприяння свободі, різноманітності і плюралізму медіа та створенню дієвої системи захисту персональних даних. Проект розрахований майже на два роки та покликаний забезпечити виконання обов'язків і зобов'язань України перед Радою Європи, а також тих, що були взяті відповідно до Угоди про асоціацію з ЄС і Плану дій з лібералізації ЄС візового режиму для України. Одним із завдань проекту є сприяння участі ключових зацікавлених сторін з України в міжнародному діалозі щодо управління Інтернетом та прав людини.

Національне законодавство України потребує комплексного реформування з метою створення прогресивної нормативно-правової бази, яка б максимально сприяла інтеграції України до інклюзивного глобального інформаційного суспільства. Наразі основними чинними нормативно-правовими актами, що регулюють інформаційний простір України, є:

70. Додаток XVII «Нормативно-правове наближення» до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]. – Режим доступу до ресурсу: http://www.kmu.gov.ua/docs/EA/Annexes_title_IV/17_Annexes.pdf

71. Додаток XXXVII до Глави 15 «Політика з питань аудіовізуальної галузі» Розділу V «Економічне і галузеве співробітництво» Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]. – Режим доступу до ресурсу: http://www.kmu.gov.ua/docs/EA/Annexes_title_V/37_Annex.pdf

- ЗУ «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», затверджений розпорядженням Кабінету Міністрів України від 15 серпня 2007 р. № 653⁷²;
- Стратегія розвитку інформаційного суспільства в Україні, схвалена розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р ⁷³;
- рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року, введене в дію Указом Президента України № 449/2014 від 01.05.2014 року. У цьому документі наголошується на необхідності прийняття таких основоположних документів як Стратегія розвитку інформаційного простору України, Стратегія кібернетичної безпеки України та однойменного закону, а також внесення численних змін до чинного законодавства. Пропонується також розробити заходи протидії інформаційній агресії іноземних держав та негативному інформаційно-психологічному впливу⁷⁴.

З метою приведення законодавства України до європейських стандартів протягом останніх кількох місяців було розроблено проекти наступних документів:

- Стратегії розбудови інформаційного простору України;
- Доктрини інформаційної безпеки України, що повинна замінити документ з аналогічною назвою від 2009 року, що втратив чинність на підставі указу Президента України від 06.06.2014 № 504/2014 «Про рішення Ради національної безпеки і оборони

72. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», затверджений розпорядженням Кабінету Міністрів України від 15 серпня 2007 р. № 653 [Електронний ресурс]. – Режим доступу до ресурсу: <http://zakon4.rada.gov.ua/laws/show/537-16>

73. Стратегія розвитку інформаційного суспільства в Україні, схвалена розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р [Електронний ресурс]. – Режим доступу до ресурсу: <http://zakon2.rada.gov.ua/laws/show/386-2013-%D1%80/print1391673661173194>

74. Рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року, введене в дію Указом Президента України № 449/2014 від 01.05.2014 року [Електронний ресурс]. – Режим доступу до ресурсу: <http://zakon4.rada.gov.ua/laws/show/n0004525-14>

України від 28 квітня 2014 року «Про скасування деяких рішень Ради національної безпеки і оборони України» та визнання такими, що втратили чинність, деяких указів Президента України»;

- ЗУ «Про суспільне телебачення і радіомовлення»;
- ЗУ «Про реформування друкованих державних і комунальних ЗМІ»;
- ЗУ «Про прозорість медіа власності»;
- ЗУ «Про державний нагляд за доступом до публічної інформації»;
- ЗУ «Про посилення гарантій журналістської діяльності».

Таким чином, проведений аналіз засвідчує про нерозвиненість механізмів універсального регулювання суспільних відносин в глобальному інформаційному суспільстві. Велика кількість зацікавлених суб'єктів та різновекторність їх інтересів створюють додаткові перешкоди при виробленні єдиних, прийнятних для кожного регуляторних механізмів. Інклюзивність інформаційного суспільства свідчить на користь вироблення спільних глобальних підходів, що повинні лягти в основу нового світового порядку у цифрову епоху.

Україна має стати невід'ємною частиною загальноєвропейського інформаційного суспільства. З цією метою Україна має переглянути національну інформаційну політику та провести комплексну реформу законодавства у відповідності з європейськими стандартами.

4. Інституційна складова міжнародно-правового регулювання інформаційної сфери[©]

Інформаційне забезпечення людства завжди належало до однієї із найважливіших його потреб, тому її задоволенням займалася виключно держава. Зацікавленість міжнародної спільноти у регламентації інформаційної сфери виникає тоді, коли фактор інформаційної могутності держави у веденні міжнародних відносин почав відігравати ключову роль.

Серед ареалу всіх функціональних блоків взаємодії членів міжнародного співтовариства, що охоплюють усі можливі «куточки» втручання міжнародного права й виділені в результаті аналітичного розрізу світу, ноосфера вважається «наймолодшою» в плані інституційної складової міжнародно-правового регулювання, тобто не існує жодної організації, до функцій якої б входили цілковито питання міжнародно-правового режиму інформації та усіх аспектів управління Інтернетом.

Недоліком усієї системи міжнародних інституцій є являється їх абсолютна невпорядкованість. З цього приводу цікавим є висловлювання Даніеля Деднея, який заявляє, що світ має боятися не лише глобальної анархії, але й жорсткої ієрархії. Ідеальним, на його думку, може бути виключно союз взаємного обмеження суверенних держав⁷⁵. Фактично таким союзом і виступає системна множинність міжнародних інституцій, членами яких є суверенні держави. Проблема полягає лише в тому, щоб сформувати єдину ієрархічну систему інституцій, зайнятих питаннями інформаційної сфери буття людства.

Методика побудови ієрархічної системи була запропонована в

75. Cabrera L. World government is back, in geopolitics and in the academy, but what does the future hold for it? / L. Cabrera [Електронний ресурс] – Режим доступу: <http://aeon.co/magazine/society/will-a-world-government-work/>.

одному з наших попередніх досліджень і ґрунтується на наступних «операціях»: інвентаризації та зважені ієрархії⁷⁶. Перш ніж розглядати зазначені методи, слід зазначити, зауважимо, що не можна зупинитися на одній із магістралей — глобалізації чи регіоналізації, оскільки міжнародні інституції впродовж їх тривалого становлення та визнання міжнародної правосуб'єктності постійно перебувають на перетині обох магістралей руху. Паралельність пролягання кожної з магістралей руху міжнародних інституцій свідчить, з одного боку,

про поступальність їх історичного росту, а з іншого — про наявність спазмів унаслідок їх паралельності. Відповідні зрушення в балансі міжнародної системи лежать в основі функціональної наповненості діяльності міжнародних інституцій: їх функцій, компетенції та повноважень⁷⁷.

Для інформаційної сфери буття людства характерне переплетення магістралей глобалізації та регіоналізації, тобто зростання функціональної наповненості міжнародних інформаційних інституцій визначається викликами глобалізації та потребами реактивно відповідати на ці виклики від імені всього міжнародного співтовариства, оскільки навіть ті самі глобальні мережі не визнають регіонального поділу, а спрямовані на все людство.

Глобалізаційна магістраль становлення міжнародних інституцій характеризується відносинами делегування повноважень державами міжнародним інституціям, коли держави вже не здійснюють контролю за тим, яким чином використовуються повноваження, делеговані міжнародній інституції. Глобалізація виступає чи не найпотужнішим фактором як кількісного, так і якісного росту міжнародних інституцій. Вона ж стала поштовхом до побудови системної множинності міжнародних інституцій у 50-70-х роках ХХ століття. Разом з тим, ми не можемо відмовитися від магістралі регіоналізації,

76. Герасимчук Н. В., Хонін В. М. Функціональність сучасного міжнародного права / Н.В. Герасимчук, В.М. Хонін // Науковий вісник Ужгородського національного університету. Серія «Право». – Вип. 22. – Частина І. – Том 3. – Ужгород, 2013. – С. 156.

77. Герасимчук Н. В. Магістралі розвитку міжнародних інституцій: соціально-часовий вимір / Н. В. Герасимчук // Гілея: науковий вісник. – Випуск 86(№7). – Київ, 2014. – С. 388.

оскільки міжнародні інституції, задіяні в регламентації інформаційної сфери буття людства, складаються із регіональних департаментів (для прикладу: ICANN, Міжнародний союз електрозв'язку). Це пов'язано із особливостями цивілізаційного й правового розвитку різних континентів.

Таким чином, побудову єдиної ієрархічної системи міжнародних інституцій слід здійснювати в глобальному масштабі з урахуванням регіональних інтересів. Першим етапом має бути інвентаризація, що полягає в обліку та розподілі сфер діяльності існуючих міжнародних інституцій. В цьому є нагальна потреба, оскільки незважаючи на чималу кількість міжнародних інституцій, функціональні колізії, тавтології та нормативні прогалини не зупиняються, що підтверджується аналізом нормативної бази міжнародних інституцій. У зв'язку з цим, варто розглянути ті міжнародні «інформаційні» інституції, які виконують відповідні цьому напрямку функції.

Наступним у побудові універсальної моделі міжнародних інституцій є фундаментальний метод зваженої ієрархії, застосування якого забезпечить ранжування інвентаризованих міжнародних інституцій на основі їх статутного права за наступною схемою: міністерства — агентства — служби:

- спеціалізовані інституції, що формуватимуть політику в кожній окремій сфері, за статусом діятимуть на зразок міністерств;
- міжнародні інституції, які регламентуватимуть систему дозвільних рішень у межах окремої вузькоспеціалізованої галузі, функціонуватимуть на зразок агентств;
- міжнародні інституції, що здійснюватимуть контроль за функціонуванням відповідної сфери міжнародно-правового регулювання, а також виконання міжнародних програм та координацію з усіх питань, що належать до їх компетенції, матимуть форму служб.

Ранжування міжнародних інституцій за методом зваженої ієрархії слід здійснювати на основі аналізу статутного права міжнародних

інституцій, а саме тих функцій, повноважень та компетенцій, якими вони наділені. А відтак перейдемо до власне аналізу міжнародної нормотворчості міжнародних «інформаційних» інституцій та самого статутного права міжнародних інституцій, функціонально зайнятих в інформаційній сфері буття людства з метою наділення їх відповідними статусами «міністерства», «агентства» чи «служби».

До першого рівня ієрархії міжнародних інституцій віднесемо організації загального спрямування, в рамках яких створюються «департаменти» вузькоспеціалізованого характеру, орієнтовані на регламентацію інформаційної сфери. Серед них, наприклад, Всесвітня організація інтелектуальної власності, Європейська патентна організація. Вони фактично виконують функції, схожі на ті, якими наділені міністерства у суверенних державах.

Так, у рамках Всесвітньої організації інтелектуальної власності діє Центр з арбітражу та посередництва, створений у 1994 році з метою надання арбітражних та посередницьких послуг для врегулювання міжнародних комерційних спорів між приватними особами. В своїй діяльності він керується Правилами ВОІВ, що постійно оновлюються. Згідно з положеннями цих Правил, а також щорічних доповідей Генеральної Асамблеї Всесвітньої організації інтелектуальної власності, до функцій Центру з арбітражу та посередництва входить розгляд спорів у галузі доменних імен, зокрема тих, що пов'язані зі змінами політики, наприклад щодо механізмів охорони прав при введенні нових родових доменів верхнього рівня та появи інтернаціоналізованих доменних імен як родових доменів верхнього рівня (положення 2 Преамбули документа Генеральної Асамблеї ВОІВ від 3 вересня 2012 року)⁷⁸.

24 жовтня 1999 року функції Центру були розширені внаслідок набуття чинності Єдиної методики розгляду спорів щодо доменних імен, розробленої Інтернет-корпорацією з призначення доменних імен та номерів (ICANN) за сприяння Центру ВОІВ з арбітражу та

78. Центр ВОИС по арбитражу и посредничеству, в том числе в области доменных имен в Интернете // Доклад Генеральной Ассамблеи ВОИС, Женева, 1-9 октября 2012 года [Электронный ресурс] – Режим доступа: www.wipo.int/edocs/mdocs/govbody/ru/.../wo_ga_41_17_rev_2.doc

посередництва. Параграф 4а зазначеного документа містить вимоги щодо обов'язкових елементів спірної ситуації, за кумулятивної наявності яких Центр повноправно може виконувати свої функції, а саме: доменне ім'я, ідентичне або схоже з товарним знаком, що належить позивачу; відсутність прав чи законних інтересів щодо доменного імені; недобросовісні реєстрація та використання доменного імені⁷⁹.

Окрім питань інтелектуальної власності щодо доменних імен, до відання Всесвітньої організації інтелектуальної власності належать й інші аспекти «цифрового порядку денного»: права, що стосуються зберігання і передачі виконань та фонограм в цифрових системах, обмеження й винятки з прав, технологічні засоби захисту та права управління інформацією. Крім того, в рамках ВОІВ була напрацьована Спільна рекомендація щодо захисту прав промислової власності в Інтернеті з метою допомоги національній владі та судам, залученим у конфлікти з питань колізій між принципом територіальної дії прав та глобальної природи Інтернету. Пункт 5.474 вищезазначеного Посібника Всесвітньої організації інтелектуальної власності встановлює перелік питань, які уповноважена врегульовувати ВОІВ⁸⁰.

Характерно, що в установчому документі Всесвітньої організації інтелектуальної власності — Стокгольмській конвенції 1967 року, а саме в статті 4 «Функції», немає чіткого положення щодо регламентації міжнародною інституцією питань, що належать до кола інформаційної сфери буття людства, але є параграф (viii), який звучить наступним чином: «Організація...вживає будь-які інші належні дії»⁸¹. Таким чином, міжнародна інституція ВОІВ підтвердила актуальну тенденцію в царині права міжнародних інституцій — наділення міжнародної інституції правом на розширення повноважень без

79. Единая методика рассмотрения споров о доменных именах. Корпорация по распределению адресного пространства сети Интернет [Электронный ресурс] – Режим доступа: http://www.copyrighter.ru/lite/index.html?UDNRPpolicy_rus.htm

80. WIPO Intellectual Property Handbook. – WIPO publication, No.489 (E). – WIPO 2004 (2nd edition), reprinted 2008. – 488p. [Электронный ресурс] – Режим доступа: <http://apps.who.int/medicinedocs/documents/s21421en/s21421en.pdf>

81. Конвенция, учреждающая Всемирную Организацию Интеллектуальной Собственности [Электронный ресурс] – Режим доступа: <http://www.viniti.ru/download/russian/INNOV/vois.pdf>

потреби в додатковому запиті вищих національних органів влади держав-членів відповідної інституції. Таким чином, статутне право Всесвітньої організації інтелектуальної власності щодо питань захисту, поширення та доступу до інформації в інтернет-просторі складається виключно з похідних від установчого документа актів, спрямованих на виконання «функцій загальних справ».

ВОІВ, а також Європейська патентна організація, входять до числа повністю ноосферних організацій, залучених до регулювання усіх аспектів інтелектуального розвитку людства. Але можна виділити також міжнародні інституції з більш вузькою спеціалізацією. Мова, зокрема, йде про спеціалізовану установу ООН в галузі інформаційно-комунікаційних технологій - Міжнародний союз електрозв'язку. До інформаційних блоків функцій Міжнародного союзу електрозв'язку належить вирішення питань кібербезпеки, цифрового розриву та Інтернету. Відповідні функції були надані міжнародній інституції не Статутом та Конвенцією МСЕ 1992 року і не Регламентом радіозв'язку 2003 року як установчими документами, а допоміжними актами статутного права МСЕ. Маємо поступове розширення компетенції міжнародної інституції (зазначені у статті 1 Статуту Міжнародного союзу електрозв'язку 1992 р.⁸²). Вони зводяться до трьох типів:

1. На Всесвітньому саміті з інформаційного суспільства (ВСІС) глави держав та світові лідери надали повноваження МСЕ виконувати функції організації по напрямку діяльності С5 «Зміцнення довіри та безпеки при використанні інформаційно-комунікаційних технологій»⁸³.
2. Функції МСЕ з мобілізації людських, фінансових та технічних ресурсів для досягнення цільових показників, задекларованих на ВСІС, у сфері забезпечення сумісності електронних комунікацій, а також реалізації регіональних ініціатив, щоразу розширюються

82. Статут МСЕ [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/995_099

83. ITU Cybersecurity Activities [Електронний ресурс] – Режим доступу: <http://www.itu.int/en/action/cybersecurity/Pages/default.aspx>

в рамках регіональних самітів держав-членів МСЕ. Вперше відповідна функція була закріплена на Першій конференції Світового телекомунікаційного розвитку 1994 року. Пункт 9f Декларації з глобального телекомунікаційного розвитку (Буенос-Айрес) 1994 року закріплює за Міжнародним союзом електрозв'язку функції з надання консультацій національним законодавцям щодо створення стабільного та прозорого інформаційного середовища⁸⁴.

3. Міжнародний союз електрозв'язку прагне також займатися питаннями управління найбільш важливими ресурсами Інтернету згідно із мандатом, запропонованим йому в Резолюції № 1305 від 2009 року, а також структурно через Повноважну конференцію, Раду та світові конференції – розробляти нормативні документи щодо питань, зазначених у Додатку до згаданої Резолюції⁸⁵.

Міжнародний союз електрозв'язку можна вважати однією з міжнародних інституцій спеціального спрямування, що безпосередньо залучена до технічного забезпечення розвитку інформаційної сфери на міжнародному рівні, про що свідчить аналіз статутного права цієї організації.

Таким чином, проаналізувавши основні міжнародні інституції в інформаційній сфері, можна запропонувати створення нової універсальної організації, або ж реформування Міжнародного союзу електрозв'язку з наділенням його усіма необхідними функціями міністерства для розбудови повноправної «інформаційної» організації.

Характерною рисою інституційної складової міжнародно-правового регулювання інформаційної сфери буття людства є активна участь міжнародних неурядових організацій. Вони формують другий рівень ієрархії міжнародних інституцій - агентства, які своєю діяльністю сприяють нормативному наповненню інформаційної сфери. Всі вони вузькоспеціалізовані і ефективно виконують надані їм спеціалізовані

84. Buenos Aires Declaration on global telecommunication development for the 21st century [Електронний ресурс] – Режим доступу: <http://www.itu.int/itudoc/itu-d/wtcd/wtcd1994/badecl.txt>.
85. Resolution 1305 – Role of the dedicated group in identifying Internet-related public policy matters [Електронний ресурс] – Режим доступу: <http://www.itu.int/md/S09-CL-C-0105>

функції, про що свідчать швидкі темпи інформатизації глобалізованого суспільства. Серед основних акторів цієї групи виділимо Інженерну Раду Інтернету (IETF), Спільноту Інтернету (ISOC), Архітектурну Раду Інтернету (IAB), Форум Управління Інтернетом, Міжнародну організацію журналістів, Міжнародний фонд жінок, що працюють у ЗМІ, Міжнародну федерацію журналістів та інші.

Спільнота Інтернету як міжнародна неприбуткова організація була створена у 1992 році з метою забезпечення розвитку та доступності мережі Інтернет. Функції ISOC окреслені в засновницькому договорі міжнародної інституції «Announcing ISOC», авторами якого є її засновники Вінт Серф, Боб Кан та Ліман Шапен. Одна з функцій діяльності Спільноти Інтернету полягає у підготовці Робочих пропозицій (RFC) – інформаційних документів Інтернету, що містять технічні специфікації та стандарти, що широко використовуються в мережі Інтернет⁸⁶. Практично всі стандарти глобальної мережі існують у вигляді опублікованих заявок RFC. У такий спосіб, Спільнота Інтернету при допомозі Інженерної Ради сприяє формуванню нового інструменту статутного права міжнародних інституцій, правами на який не володіє жодна інша міжнародна інституція, в тому числі й міжурядова. Виконуючи свою статутну роль, Спільнота Інтернету відіграє також свою роль, проводячи щорічний форум з обговорення питань управління Інтернетом в рамках конференції «International Networking».

Функції Інженерної Ради Інтернету (IETF) – відкритої міжнародної спільноти проектувальників, вчених, мережевих операторів та провайдерів, створеної у 1986 році з метою розвитку протоколів та архітектури Інтернету, викладені в Робочих пропозиціях № 4677 (RFC 4677), що служить, певною мірою, установчим документом неурядової організації. До функцій IETF належать:

- ідентифікація проблем та пропозиції щодо їх вирішення в технічних аспектах організації Інтернету;

78 86. Cerf V., Kahn B., Chapin L. Announcing the Internet society [Електронний ресурс] / V. Cerf, B. Kahn, L. Chapin – Режим доступу: <http://www.internetsociety.org/internet/what-internet/history-internet/announcing-internet-society>.

- розробка специфікацій, стандартів та домовленостей за загальними архітектурними принципами Інтернету;
- винесення рекомендацій стосовно стандартизації протоколів;
- сприяння широкому розповсюдженню технологій та стандартів;
- організація дискусії для обміну інформацією в спільноті Інтернету між вченими, розробниками, користувачами, виробниками обладнання та послуг, мережевими адміністраторами тощо⁸⁷.

Проаналізувавши нормативну базу Інженерної ради Інтернету⁸⁸, слід зазначити, що статутне право цієї міжнародної інституції формують, на даний момент, 9013 документів, серед яких основну масу складають Робочі пропозиції (RFC), робочі проекти (як основа для кодифікації RFC), специфікації, рекомендації, що виступають фундаментом розширення функцій інтернет-інституцій. Будучи дочірньою організацією Спільноти Інтернету, Інженерна Рада Інтернету також виступила засновником такої інституції як Трест IETF.

У Робочій пропозиції 2850 (2000 р.) міститься Статут групи технічних радників ISOC, яким була створена Архітектурна Рада Інтернету (IAB). Пункт 2 установчого документа закріплює за нею наступні функції: 1) призначення членів Internet Engineering Steering Group; 2) нагляд за архітектурою Інтернету, включаючи його протоколи та пов'язані з ним процедури; 3) нагляд за створенням нових стандартів Інтернету; 4) редагування та публікація серії документів RFC; 5) консультації керівництва ISOC з технічних, архітектурних та процедурних питань, пов'язаних з Інтернетом та його технологіями⁸⁹.

Статутне право Архітектурної Ради Інтернету складається з наступних інструментів: звітні документи IAB, принципи архітектури

87. The TAO of IETF: A novice's guide to the Internet Engineering Task Force [Електронний ресурс] – Режим доступу: <http://www.ietf.org/rfc/rfc4677.txt>.

88. IETF documents statistics (all documents) [Електронний ресурс] – Режим доступу: <http://www.arkko.com/tools/allstats/>

89. Charter of the Internet Architecture Board (IAB) [Електронний ресурс] – Режим доступу: <http://www.iab.org/about/charter/>

Інтернету, тексти запитів до IANA, технічні коментарі, оголошення, технічні записки, інструкції, протоколи засідань IAB, робочі проекти (Internet drafts) та робочі пропозиції.

Міжнародна організація журналістів займається відмінними від вищезазначеного аспектами інформаційної сфери буття людства. Вона являє собою добровільне журналістське об'єднання, що було засноване у 1967 році на Конгресі в Копенгагені. Згідно зі Статутом Міжнародної організації журналістів, її основна функція полягає у захисті миру, зміцненні дружби і співпраці між народами з допомогою вільного, правдивого і чесного інформування громадськості, захисті свободи ЗМІ і прав журналістів.

Наступну групу в рамках цього ж рівня ієрархії міжнародних «інформаційних» організацій складають також неурядові інституції, які, проте функціонують за активної участі національних урядів. Мова, зокрема, йде про міжнародні некомерційні організації ICANN, IANA, Спільнота At-Large. Інтернет-корпорація з призначення доменних імен та номерів (ICANN) займає чільне місце в адмініструванні системи доменних імен в Інтернеті.

Фундамент статутного права ICANN становить Меморандум про взаємне порозуміння між Департаментом торгівлі Сполучених Штатів Америки та Інтернет-корпорацією з призначення доменних імен та номерів (1998 р.). Пункт В положення II під назвою «Ціль» визначає функції Корпорації, серед яких: 1) формування політики та напрямків розподілу блоків IP – адрес; 2) нагляд за роботою системи кореневих серверів; 3) нагляд за політикою встановлення обставин, за яких нові домени верхнього рівня будуть додані до кореневої системи; 4) координація присвоєння інших технічних параметрів в Інтернеті, необхідних для підтримання універсального сполучення в Інтернеті; 5) інші заходи, необхідні для координації визначених функцій з управління системою доменних імен (DNS)⁹⁰.

80 90. Memorandum of Understanding between the US Department of Commerce and Internet Corporation for Assigned Names and Numbers [Електронний ресурс] – Режим доступу: <https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en>.

У своїй діяльності ICANN керується Установчим договором від 21 листопада 1998 року, пункт 3 якого містить відкритий перелік функцій в сфері доменних імен, оскільки завершується положенням (v): «залучення до будь-якої іншої законної діяльності задля виконання положень від (i) до (iv)»⁹¹, а також щодо внутрішніх процедур з управління (для розбудови організаційної структури ICANN)⁹².

Відповідні функції ICANN розширювалися шляхом внесення шести Додатків до Меморандуму протягом 1998-2003 років, а також у 2006 році після прийняття «Підтвердження обов'язків ICANN в управлінні приватним сектором». Важливим документом, яким визнається правосуб'єктність міжнародної інституції ICANN, є «Положення політики, управління інтернет-іменами і адресами», прийняте 63 Федеральним регламентом (1998)⁹³. Згідно із преамбулою документа Уряд США визнає нову неприбуткову корпорацію, утворену акціонерами приватного сектора як адміністратора політики в сфері системи інтернет-адрес та номерів. Цим же документом влада США наділи ICANN повноваженнями укладати домовленості як на внутрішній, так і на зовнішній арені задля стабільності мережі Інтернет.

Статутне право ICANN складається з численних внутрішньо-організаційних актів, тринадцяти звітів Департаменту торгівлі США, домовленості з Університетом Південної Каліфорнії від 1998 року, низки функціональних контрактів виконання функції «Адміністрації адресного простору Інтернету (IANA)»⁹⁴. Безумовно, найбільш юридично, а не технічно наповненими є перехідні та імплементаційні угоди.

Функції IANA, що їх виконує до цього часу ICANN, полягають

91. Articles of Incorporation of Internet Corporation for Assigned Names and Numbers [Електронний ресурс] – Режим доступу: <https://www.icann.org/resources/pages/articles-2012-02-25-en>

92. Governance Guidelines. ICANN [Електронний ресурс] – Режим доступу: <https://www.icann.org/resources/pages/guidelines-2012-05-15-en>

93. Affirmation of Responsibilities for ICANN's Private Sector Management [Електронний ресурс] – Режим доступу: <https://www.icann.org/en/system/files/files/jpa-29sep06-en.pdf>

94. ICANN's Major Agreements and Related Reports [Електронний ресурс] – Режим доступу: <https://www.icann.org/resources/pages/agreements-2012-02-25-en>

в: 1) управлінні системою доменних імен; 2) координації глобальної мережі IP та AS номерів і занесенні їх до регіональних інтернет-реєстрів; 3) управлінні номерними системами інтернет-протоколів.

Крім того, політика Адміністрації адресного простору Інтернет здійснюється на основі контрактів між ICANN та Департаментом торгівлі США, а також Меморандуму взаємне порозуміння між відповідними суб'єктами.

В інституційному плані важливо також згадати ще про одну організацію в системі інституцій ICANN, а саме про Спільноту At-Large. Вона являє собою об'єднання індивідуальних користувачів Інтернету, які беруть участь у розвитку політики ICANN. Спільнота At-Large є інституцією, що діє на глобальній арені, керуючись моделлю *multi-stakeholder governance*. Архітектура At-Large складається із п'яти регіональних At-Large організацій, що діють в Африці, Азійському і Тихоокеанському регіонах, Європі, Латинській Америці і Карибському басейні та Північній Америці, а також із Консультативного комітету At-Large⁹⁵. Статутне право Спільноти переважно складається із заяв стосовно конкретних ініціатив ICANN (для прикладу: «Заява Розширеного консультативного комітету (At-Large) у зв'язку зі звітом щодо доменів верхнього рівня»⁹⁶), а також із рекомендацій.

Що стосується служб, то досить не просто виділити ті міжнародні інституції, що можуть здійснювати контроль за функціонуванням інформаційної сфери буття людства, хоча деякі з них наділені функцією розгляду спорів, наприклад згаданий Центр з арбітражу і посередництва при Всесвітній організації інтелектуальної власності. Існує нагальна потреба у створенні інституцій, які слідкуватимуть та реагуватимуть на порушення в інформаційній сфері.

Незважаючи на чималу кількість неурядових неприбуткових

95. At-Large Community. The Individual Internet User's Voice in ICANN [Електронний ресурс] – Режим доступу: <http://www.atlarge.icann.org/en/whatis.htm>

96. ALAC Statement on the SSAC Report on Dotless Domains, 22 September 2012 [Електронний ресурс] – Режим доступу: <http://www.atlarge.icann.org/correspondence/correspondence-22sep12-en.htm>

організацій, єдиної організації, яка б «керувала інформацією та кіберпростором» не існує, а зазначені вище інституції лише беруть участь у забезпеченні функціонування екосистеми Інтернету на різних рівнях його функціонування.

Так, дійсно, географія міжнародних «інформаційних» інституцій охоплює усі країни-члени Організації Об'єднаних Націй в контексті тих функцій, які покладені на спеціалізовані установи ООН: Всесвітню організацію інтелектуальної власності і Міжнародний союз електрозв'язку. Разом з тим, питання непрозорості глобального управління і відсутності доступу до глобальних мереж ще й досі залишаються найбільш актуальними для міжнародного співтовариства.

Таким чином, інституційна складова міжнародно-правового регулювання інформаційної сфери особливо активна з позиції міжнародної нормотворчості, про що свідчить незліченна кількість регламентів, рекомендацій, стандартів, інструкцій, заяв та інших актів статутного права міжнародних «інформаційних» інституцій. Важливо, що та кількість міжнародних інституцій, які своїм функціонуванням підтримують життєдіяльність інформаційної сфери, дозволяє уникати колізій та тавтологій у міжнародно-правовому забезпеченні інформаційного суспільства, але не запобігає появі прогалін.

Інформаційна сфера містить безліч аспектів, у тому числі й не врегульованих міжнародними інституціями. Отже, говорячи про перспективи

формування єдиної системи міжнародних інституцій у цій сфері, слід спочатку провести повну інвентаризацію інституцій і заповнити ті прогалини, що виникатимуть при цьому. Крім того, інституційна складова міжнародно-правового регулювання інформаційної сфери повинна набути чіткої структурованості відповідно до сфер компетенції та функцій міжнародних організацій.

5. Розбудова Національного багатостороннього механізму управління розвитком Інтернету в Україні на основі принципів Ради Європи[©]

Питання управління Інтернетом займають ключове місце в сучасній міжнародній політиці. Завдячуючи Всесвітній зустрічі на високому рівні з питань інформаційного суспільства (WSIS) у Женеві у 2003 році і в Тунісі у 2005 році, маємо актуальне визначення поняття «управління Інтернетом», яке хоча й абстрактно, але принципово вимагає врахувати інтереси усіх зацікавлених сторін, що беруть в ньому участь:

«Управління Інтернетом являє собою розробку та застосування урядами, приватним сектором та громадянським суспільством, при виконанні ними своєї відповідної ролі, загальних принципів та норм, правил, процедур прийняття рішень і програм, які регулюють еволюцію та застосування Інтернету»⁹⁷.

В Женевських принципах інформаційного суспільства питання повної і дієвої участі усіх зацікавлених сторін в управлінні Інтернетом, з урахуванням їх компетенції та повноважень у відповідних сферах впливу, є ключовими:

«49. Управління Інтернетом охоплює як технічні питання, так і питання державної політики, та повинно залучати всі зацікавлені сторони і відповідні міжурядові і міжнародні організації. У зв'язку з цим визнається, що:

- а) політичні повноваження з пов'язаних з Інтернет питань державної політики є суверенним правом держав. У них є права і обов'язки щодо пов'язаних з Інтернет питань міжнародної політики;*
- б) приватний сектор відіграє і повинен продовжувати відігравати важливу роль у розвитку Інтернет, як в технічній, так і в економічній сферах;*
- с) громадянське суспільство також відіграє важливу роль в питаннях Інтернету, особливо нарівні громад, і повинно продовжувати грати таку роль;*

97. Доповідь робочої групи з управління Інтернетом. – [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/development/ict/wgig_report.pdf

© **Пазюк Андрій Валерійович**, кандидат юридичних наук, керівник лабораторії з управління Інтернетом Української Асоціації міжнародного права, член Експертної ради Комітету Верховної Ради України з питань інформатизації та інформаційних технологій

- г) міжурядові організації відіграють і повинні продовжувати грати роль, сприяючи міждержавній координації з питань, пов'язаних з Інтернет;
- е) міжнародні організації також відіграють і повинні продовжувати грати важливу роль у розвитку технічних стандартів і відповідної політики стосовно Інтернету»⁹⁸.

Саме для налагодження і продовження діалогу між зазначеними зацікавленими сторонами на підставі пунктів 72, 73 і 77 Туніської програми під егідою Генерального секретаря Організації Об'єднаних Націй був заснований Міжнародний Форум з управління Інтернетом. Цей Форум не замінював інших організацій, а фактично набув статус щорічної міжнародної конференції, на якій обговорюються питання розвитку Інтернету⁹⁹. Проведенню щорічної конференції передують національні та регіональні форуми, що організовуються за участю зацікавлених сторін.

На європейському рівні щорічний форум з управління Інтернетом, що має назву *EuroDIG* відбувся в Берліні, 12-13 червня 2014 року¹⁰⁰. Активну участь в ньому взяли представники з України, як безпосередньо, так і віддалено за допомогою сучасних Інтернет-технологій дистанційної участі. В Україні 5-й Національний Форум з управління Інтернетом планується провести у жовтні 2014 року.

Якою є роль України в глобальному механізмі управління Інтернетом? Як держава може і повинна розвивати Інтернет для побудови інформаційного суспільства в нашій країні? Якими напрямками рухатися для досягнення цієї мети?

Відповіді на ці питання не лежать на поверхні, а потребують аналізу та публічного обговорення в широкому колі заінтересованих сторін — громадянського суспільства, державних органів, бізнесу, академічної та технічної спільнот. Ключовим досягненням міжнародної спільноти за останні 10 років, що минули з часу проведення Всесвітнього Саміту з питань інформаційного суспільства (WSIS), є визнання необхідності вирішення питань управління Інтернетом на принципах так званого «мультистейкхолдерізму» (MSH — англ.) або українською — багатосторонньої участі усіх зацікавлених сторін.

98. Женевська Декларація принципів «Побудова інформаційного суспільства: глобальна задача в новому тисячолітті», WSIS, грудень, 2003 [Електронний ресурс]. – Режим доступу : http://informationssociety.wordpress.com/basics/wsis_outcomes/dp/

99. What is the Internet Governance Forum? / [Electronic source] / IGF, Nairobi, 27-30 September 2011.. – Access mode : http://www.intgovforum.org/cms/2011/press/Backgrounder_What_is_IGF_final.doc

100. <http://www.eurodig.org/eurodig-2014/programme-overview>

Саме на цих засадах 23-24 квітня 2014 року у Бразилії відбулась Глобальна багатостороння конференція стосовно майбутнього управління Інтернетом, що пройшла під назвою «НетМундіаль».

Результатом підготовки та проведення конференції є внесок, який зробили зацікавлені сторони – уряди держав, громадянське суспільство, індустрія (бізнес-сектор), технічна та академічна спільноти – 188 пропозицій, що були покладені в основу заключного акту конференції – Багатосторонньої Декларації. Крім того, у ході дводенного заходу учасники з 97 країн мали можливість внести свій внесок у підсумковий документ. Під час засідань було розглянуто 1370 зауважень, висловлених громадськістю до проекту Декларації.

Декларація складається з двох частин: принципів управління Інтернетом та Дороговказу майбутньої еволюції екосистеми управління Інтернетом. Самі ж принципи також можна умовно поділити на матеріальні, що стосуються основоположних цінностей, та процесуальні, що присвячені процесу управління Інтернетом. Фактично Декларація узагальнила усі ті принципи управління Інтернетом, які упродовж останніх років, приймалися на різних рівнях різними форумами, міжурядовими та громадськими організаціями.

Враховуючи консенсуальний характер прийняття Декларації, до її тексту не увійшов принцип сільового нейтралітету. Щодо цього принципу існують протилежні погляди поміж зацікавлених сторін, а також як всередині бізнесової спільноти, так і серед держав.

Проте в документі наголошується на прихильності до концепції «відкритого Інтернету» та необхідності продовження дискусії щодо сільового нейтралітету на наступному ICF (Форумі з управління Інтернетом).

Громадянські організації висловили свої зауваження до фінального тексту Декларації у заяві, що була оприлюднена організацією Bestbits. Зокрема, поряд із схваленням дій Бразильського уряду щодо організації самого заходу і залученням представників громадянського суспільства до процесу вироблення політики, були висловлені зауваження щодо неврахування низки ключових питань, що перебувають у сфері впливу недержавного сектору. Серед них, не адекватне реагування на проблему сільового нейтралітету; неналежне відображення стурбованості міжнародної громадянської спільноти фактами суцільного (масового) неконтрольованого суспільством стеження, яке суперечить правам людини і принципу пропорційності у втручання до цих прав у визначених законом випадках.

Натомість згадування про звільнення від відповідальності посередників (передавачів інформації), яке може сприйматися позитивно, затьмарено забарвленим формулюванням про припустимість обмеження права на свободу вираження думок та приватність. На думку авторів заяви, Декларація не в повній мірі просуває ідею щодо захисту основоположних прав та пошуку компромісу для влади між різними зацікавленими групами¹⁰¹.

У коментарі, оприлюдненому в EDRI-gram (європейський журнал з цифрових прав), оцінка результатам «НетМундіалю» є ще більш гострою, а Декларація називається «документом лобістів від уряду та бізнесу Сполучених Штатів». Зокрема, зазначається, що «наростаюча проблема відповідальності посередників, які «волонтаристські» і свавільно блокують або видаляють контент внаслідок примусу держави, всупереч основним принципам міжнародного права, не визнаються як такі. І навіть гірше, і це активно заохочується — підсумковий документ закликає до приватного підтримання правопорядку через «співробітництво між усіма зацікавленими сторонами ... спрямоване на виявлення та реагування на незаконну діяльність у відповідності з «справедливим процесом»¹⁰².

Автор статті задає питання, що означає «справедливий процес», який використовується у реальному житті компаніями, які будуть здійснювати таке підтримання правопорядку власними силами у приватному порядку. І навіть, коли їхні контрактні умови передбачають можливість блокування, фільтрації, знищення, вилучення або втручання у приватні дані, цим компаніям вигадувати «справедливий процес». Як приклад, зазначається, що компанія *Google* вже впровадила законодавство США про авторські права на глобальній основі, *Microsoft* вже надала собі право читати ваше електронне листування, *GoDaddy* надала собі право видаляти ваші доменні імена, *VISA* вже надала собі право відслідковувати ваші платежі. Зрозуміло, що ні про «справедливість», ні про «процес» мова не йде. Наразі відсутній міжнародний договір, який би перешкоджав включати до контрактів положення, що обмежують права користувачів і дозволяють такі дії¹⁰³.

Слід відмітити, що проект Декларації передбачав можливість використання міжнародно-правових договорів як інструменту для вирішення питань, що стосуються таких специфічних тем з управління Інтернетом (розділ 3) як безпека та стабільність, зокрема з питань юрисдикції і взаємодії у правоохоронній сфері, інформаційної безпеки та запобігання

101. Civil society closing statement at NETmundial 2014 <http://bestbits.net/netmundial-response/>

102. Joe McNamee, NETmundial, multistakeholderism and fair process / EDRI-gram biweekly newsletter about digital civil rights in Europe, Number 12.9, 7 May 2014

103. Ibid.

кіберзлочинністю. У остаточній редакції слова про міжнародно-правові договори були замінені на міжнародне співробітництво, що підтверджує тезу про незацікавленість транснаціональних компаній підпадати під дію міжнародного права із захисту прав людини.

Проте, попри критику Багатостороння Декларація прийнята консенсусом за участю усіх зацікавлених сторін є вкрай важливим документом, в якому затверджені конкретні завдання щодо подальшого розвитку на організаційному рівні. Зокрема, стосовно реформування адміністрування асигнуванням (розподілом) імен та номерів (IANA), що має завершитися до вересня 2015 року.

Також йде мова про глобалізацію ІКАНН, що має забезпечити її підзвітність не лише Уряду Сполучених Штатів, а й іншим державам та зацікавленим сторонам, що представляють глобальне співтовариство. Ці два взаємопов'язаних питання є ключовими для подальшої еволюції екосистеми управління Інтернетом.

Важливі для України положення щодо розвитку національного багатостороннього механізму управління Інтернетом містяться у Дороговказі майбутньої еволюції управління Інтернетом (п.3, п. 4 розділу 1):

«3. Представники зацікавлених сторін, призначені для виконання багатосторонніх процесів управління Інтернетом, повинні відбиратися відкритим, демократичним і прозорим способом. Різні групи зацікавлених сторін повинні *самостійно управляти своїми процесами*, заснованими на всеосяжних, публічно відомих, чітко визначених і підзвітних механізмах.

4. Існує необхідність розвивати багатосторонні механізми *на національному рівні*, враховуючи той факт, що значна кількість питань з управління Інтернетом необхідно вирішувати саме на даному рівні. *Національні багатосторонні механізми повинні служити зв'язком між локальними дискусіями, регіональними та глобальними процесами. Отже, вільна координація та діалог між цими різними сферами є вкрай важливими»¹⁰⁴.*

Таким чином, Багатостороння Декларація може послужити основою та дороговказом для розбудови національного багатостороннього механізму управління Інтернетом в Україні. Яким же має бути змістовне наповнення цього механізму? Які цінності повинні бути покладені в основу?

Принагідним є доробок Ради Європи.

104. <http://netmundial.br/netmundial-multistakeholder-statement/>

Рада Європи не залишає поза увагою питання управління Інтернетом, ухвалюючи важливі документи, що демонструють спільне бачення цієї глобальної проблеми державами європейського континенту.

У 2011 році Комітет міністрів держав-членів Ради Європи прийняв на своєму 1121-му засіданні Декларацію про принципи управління Інтернетом. Цей документ є важливим для нашої держави не лише тому, що представляє собою спільне бачення і підходи до управління Інтернетом з боку європейських країн, а й тому, що покладає певні зобов'язання, що випливають із членства України в Раді Європи та участі в конвенціях цієї міжнародної організації. Зокрема, це випливає з зобов'язань забезпечити кожному, хто перебуває під юрисдикцією нашої держави, права і свободи, що захищаються Конвенцією про захист прав людини та основоположних свобод.

Декларація визначає засадничі європейські цінності щодо стійкого, соціально-орієнтованого і правового підходу до регулювання суспільних відносин в Інтернеті, спрямовані на забезпечення максимуму прав в Інтернеті за умови мінімуму обмежень, пропонуючи при цьому такий рівень безпеки, на який люди мають право очікувати.

Комітет міністрів Ради Європи закликав уряди всіх держав-членів підтримати принципи управління Інтернетом, а інші зацікавлені сторони (громадянське суспільство та бізнес) – прийняти їх до виконання у своїх власних ролях.

Зокрема, в документі наголошується, що механізми управління Інтернетом мають забезпечувати захист всіх основних прав і свобод, і підтверджувати свою універсальність, неподільність, взаємозалежність і взаємозв'язок відповідно до міжнародного права у сфері захисту прав людини. Вони також повинні забезпечити повну повагу демократії і верховенства права, повинні сприяти сталому розвитку. Розробка та впровадження механізмів управління розвитком Інтернету повинні забезпечити, у відкритий, прозорий і підзвітний спосіб, повну і рівноправну участь урядів, приватного сектору, громадянського суспільства, технічного співтовариства і користувачів, з урахуванням їх конкретних ролей та обов'язків.

В Декларації проголошені такі принципи управління Інтернетом:

1. Права людини, демократія і верховенство права
2. Управління усіма зацікавленими сторонами
3. Відповідальність держав

4. Розширення прав і можливостей користувачів Інтернету
5. Універсальність мережі Інтернет
6. Цілісність мережі Інтернет
7. Децентралізоване управління
8. Архітектурні принципи
9. Відкритість мережі
10. Культурне та мовне різноманіття

Отже, зазначені принципи закладають ідеологічний фундамент для національного багатостороннього механізму управління розвитком Інтернету в Україні. Організаційною формою або площадкою цього механізму є Український Форум з управління Інтернетом (IGF-UA). В Україні такий форум був проведений вже п'ять раз. П'ятий IGF-UA був проведений у жовтні 2014 року.

Проте його учасники – представники заінтересованих сторін, що опікуються питаннями розвитку інформаційного суспільства в Україні, – до цього часу не визначили основоположні засади його діяльності, що не сприяє ефективності та не запобігає конфлікту інтересів. Потрібна легітимізація участі усіх зацікавлених сторін в національному механізмі управління Інтернетом, що поділяють принципи його діяльності, шляхом приєднання до установчого документу. Пропонується сформулювати його як Меморандум, а для наповнення використати модельний документ – Кодекс добросовісної практики з інформування, участі та прозорості в управлінні Інтернетом, схвалений Асоціацією прогресивних комунікацій, Радою Європи та Європейською Економічною Комісією (ЄЕК) ООН у 2010 році¹⁰⁵.

Проект Меморандуму наведений нижче. До обговорення тексту та надання пропозицій запрошуються усі зацікавлені особи.

105. Code of good practice on information, participation and transparency in internet governance
http://www.intgovcode.org/images/c/c1/COGP_IG_Version_1.1_June2010.pdf

Проект

Меморандум про створення багатостороннього механізму управління розвитком Інтернету в Україні

Преамбула

Багатосторонній механізм управління розвитком Інтернету в Україні (MSH-UA¹⁰⁶) — це національна ініціатива громадянського суспільства, державного сектора, приватного (бізнес) сектора, академічної та технічної спільнот України (далі - заінтересовані сторони), спрямована на координацію спільних зусиль з метою розвитку Інтернету в Україні.

Необхідність створення MSH-UA ґрунтується на прихильності зацікавлених сторін Женевським принципам побудови глобального інформаційного суспільства, схваленим під час Всесвітнього саміту з питань інформаційного суспільства в грудні 2003 року, а також принципам управління Інтернетом, схваленим на Глобальній зустрічі зацікавлених сторін, присвяченій майбутньому управління Інтернетом (відомої також як NETMundial), у вигляді Багатосторонньої Декларації (*Multistakeholder Statement*) в Сан-Паоло в квітні 2014 року¹⁰⁷ (Женевська Декларація принципів 2003 р. і Багатостороння Декларація NETMundial 2014 р.¹⁰⁸ додаються і є невід'ємною частиною цього Меморандуму).

Організаційна структура MSH-UA

Організаційну структуру MSH-UA складає Український Форум з управління Інтернетом (IGF-UA), який проводить свою роботу у формі щорічної конференції, робочих груп і консультацій, що проводяться між зацікавленими сторонами в період між конференціями.

Мандат IGF-UA

IGF-UA — є громадською трибуною для вираження позицій зацікавлених сторін і національним внеском з боку українського народу у загальну справу розвитку глобального інформаційного суспільства на принципах, визначених у підсумкових документах Всесвітнього саміту інформаційного суспільства. IGF-UA є організаційною формою MSH-UA для вироблення та узгодження спільної позиції зацікавлених сторін з метою прийняття рішень консенсусом.

106. MSH-UA – абревіатура від англійського слова *Multistakeholder* (Багатосторонній) та UA (Україна)

107. <https://www.itu.int/wsis/docs/geneva/official/dop.html>

108. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>

Підтверджуючи свою прихильність мандату IGF, визначеному в п. 72 Туніської програми для інформаційного суспільства, а також розділяючи основоположні принципи Кодексу добродійної практики з інформування, участі та прозорості в управлінні Інтернетом, схвалені Асоціацією прогресивних комунікацій, Радою Європи та Європейською Економічною Комісією (ЄЕК) ООН¹⁰⁹, діяльність IGF-UA спрямована на:

- а) обговорення питань державної політики України, що стосуються ключових елементів управління Інтернетом з метою сприяння забезпеченню стійкості, надійності, безпеки, безвідмовності і розвитку Інтернету;
- б) полегшення і поглиблення діалогу між органами державної влади України, що займаються різними перехресними питаннями міжнародної та внутрішньодержавної політики щодо Інтернету, та обговорення питань, що не відносяться до компетенції якогось з існуючих органів;
- в) взаємодія з відповідними державними і міжурядовими організаціями та іншими установами з питань, що належать до їх компетенції;
- г) полегшення обміну інформацією і передовим досвідом і в зв'язку з цим використання повною мірою спеціальної компетенції академічних та технічних співтовариств;
- д) надання консультацій всім зацікавленим сторонам з пропозицією шляхів і засобів прискорення проникнення та прийнятності в ціновому відношенні Інтернету в Україні та інших країнах світу, в тому числі тих, що розвиваються;
- е) посилення та підвищення залучення зацікавлених сторін в існуючі та /або майбутні механізми управління Інтернетом;
- ж) визначення питань, які з'являються, доведення їх до уваги відповідних органів і широкої публіки і, у належних випадках, підготовку рекомендацій;
- з) підвищення компетентності в області управління Інтернетом в Україні, з максимально можливим залученням локальних носіїв знань і досвіду;
- і) просування та оцінку, на постійній основі, втілення принципів ВСІС в процесі управління Інтернетом;
- й) обговорення, серед іншого, питань, що стосуються критичних ресурсів Інтернету;
- к) допомогу у виробленні рішень з питань, що виникають через належне і неналежне використання Інтернету, особливо щодо повсякденних користувачів;

109. Code of good practice on information, participation and transparency in internet governance, Version 1.1, June 2010 http://www.intgovcode.org/images/c/c1/COGP_IG_Version_1.1_June2010.pdf

- л) публікацію своїх документів та висвітлення діяльності в кіберпросторі та медіа.

Принципи діяльності IGF-UA:

Принципи діяльності IGF-UA включають в себе:

- Принципи інформування
- Принципи участі

Принципи інформування

1. Принципами підготовки, проведення та надання звітності IGF-UA повинні бути відкритість, прозорість, всеосяжність, включеність всіх зацікавлених сторін і виключення будь-яких комерційних інтересів.
2. Вся інформація, що стосується прийняття рішень і роботи IGF-UA, має бути доступною всім зацікавленим сторонам і потенційним учасникам таким чином і в такому форматі, який є зручним для них. Винятки з цього принципу повинні бути публічно обговорені та пояснені.
3. IGF-UA через свої робочі органи повинен активно сприяти поширенню інформації через Інтернет або за допомогою інших засобів інформування та комунікацій і підвищувати поінформованість суспільства про свою роботу в цілому, з питань, якими він займається, про ті рішення, які приймаються і про процеси, в ході яких рішення будуть прийняті, в доступній для сприйняття і розуміння широкої громадськості формі.
4. IGF-UA повинен забезпечити зв'язок з зацікавленими сторонами, в тому числі і в офф-лайн режимі, для отримання ними додаткової інформації про роботу організацій, процеси прийняття рішень, а також про процеси, за допомогою яких ці рішення приймаються.
5. Спількування в рамках робочих органів IGF-UA має бути прозорим і підзвітним: всі офф-лайн зустрічі реєструються і розміщуються у вільному доступі он-лайн, все он-лайн комунікації відбуваються з дотриманням норм нетикету — документ RFC 1855 Netiquette Guidelines (1995)¹¹⁰.

Принципи участі

6. Процедура залучення до роботи в рамках заходів IGF-UA складається з приєднання до Меморандуму шляхом підписання, декларування власних інтересів і відсутності конфлікту інтересів.

- Участь у роботі IGF-UA не може служити забезпеченню власних інтересів чи інтересів пов'язаних осіб.
7. IGF-UA повинен закликати і надавати можливість всім бажаючим взяти участь в процесах прийняття рішень щодо розвитку інформаційного суспільства та Інтернету внести свій внесок в надії на те, що їхні пропозиції будуть враховані.
 8. IGF-UA повинен активно сприяти участі у своїй роботі всіх тих, на кого впливає або може вплинути, або тих, хто вважає, що на нього вплинули рішення IGF-UA. IGF-UA повинен прагнути залучити до обговорень осіб, які недостатньо представлені і охоплені, які перебувають у меншості, в тому числі як тих, хто користується Інтернетом, так і тих, хто поки не має доступу до Інтернету.
 9. Будь-яка особа або організація повинна мати можливість винести на обговорення питання про програму розвитку інформаційного суспільства, розробку стандартів, координації або управління Інтернетом, а також з менеджменту та структури організацій, пов'язаних з управлінням Інтернетом. Вони також повинні мати можливість брати безпосередню участь у таких дебатах, з використанням офлайн-ових та інших механізмів, що відповідають потребам відповідних спільнот, так і через дистанційну он-лайн участь у робочих групах і консультаціях зацікавлених сторін.
 10. Робочі органи IGF-UA повинен постійно проводити аналіз своєї діяльності з метою підвищення відкритості, якості, прозорості, своєчасності та відповідальності за прийняття рішень. Для досягнення цього будуть використані методи експертних оцінок та інші подібні чи інші методи оцінки. Результати такого аналізу мають бути оприлюднені.
 11. Будь-які заяви чи офіційні кроки від імені IGF-UA можливі лише з боку уповноважених на те осіб після попереднього відкритого обговорення кожного окремого питання.
 12. Порушення принципів роботи IGF-UA, зазначених у цьому Меморандумі, тягне за собою припинення участі представника зацікавленої сторони в його роботі, що не виключає можливості зацікавлену сторону направити нового представника замість виключеного для участі в роботі IGF-UA.

РОЗДІЛ ІІІ

ГАРМОНІЗАЦІЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ З ЄВРОПЕЙСЬКИМИ СТАНДАРТАМИ У СФЕРІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ШЛЯХ ЗАКОНОДАВЧИХ РЕФОРМ

ПІДРОЗДІЛ 3.1.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

6. Сучасний стан виконання Україною міжнародних зобов'язань із захисту персональних даних[©]

Право на приватність та захист інформації про особу залишається одним із найважливіших серед прав людини. Його актуальність значно зросла у зв'язку з тим, що із розвитком інформаційних технологій об'єми та масштаби обробки й обігу інформації, яка носить персоніфікований характер, збільшилися в рази. Відповідно, питання захисту персональних даних набуває особливого значення в умовах ХХІ ст.

На міжнародному рівні увагу цьому питанню почали приділяти в другій половині ХХ ст. Можна виділити два основні етапи становлення міжнародно-правового закріплення захисту персональних даних: спочатку це був один із елементів права на приватність, який згодом починає розглядатися як самостійний предмет міжнародного співробітництва.

На першому етапі захист персональних даних знайшов своє закріплення в положеннях міжнародних договорів щодо права на приватність. Так, у ст. 17 Міжнародного Пакту про громадянські та

© *Городиський Іван Михайлович*, кандидат юридичних наук, директор Центру верховенства права Українського католицького університету

політичні права 1966 р. було закріплено, що: «1. Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємниці його кореспонденції чи незаконних посягань на його честь і репутацію. 2. Кожна людина має право на захист закону від такого втручання чи таких посягань»¹¹¹. Аналогічне за змістом положення було включене і до ст. 16 Конвенції про права дитини 1989 р.¹¹².

Крім універсальних міжнародних договорів, відповідні норми містилися і в регіональних міжнародних договорах щодо захисту прав людини. Так, у ст. 8 Європейської конвенції про захист прав людини і основоположних свобод 1950 р. зазначено: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції»¹¹³. Положення щодо захисту права на приватність також містяться в ст. 11 Американської конвенції з прав людини 1969 р.¹¹⁴, ст. 7 Хартії основних прав Європейського Союзу¹¹⁵ тощо.

Однак, уже незабаром прийшло усвідомлення, що трактування захисту персональних даних лише як одного з елементів права на приватність є надто обмеженим, а це питання вимагає окремого особливого регулювання. Як зазначають В. М. Брижко, А. І. Радянська та М. Я. Швець, потреба в започаткуванні міжнародно-правового регулювання відносин з приводу захисту, обробки та передачі персональних даних була зумовлена тим, що: «У середині 1970-х рр. стало зрозумілим, що національні системи правового захисту даних, з

111. Міжнародний пакт про громадянські та політичні права від 16.12.1966 р. // Збірник нормативних актів з питань правозахисної діяльності / упоряд. С. Ф. Гончаренко. – К.: Юрінком Інтер, 1995. – С. 38 – 44.

112. Конвенція о правах ребенка от 20 ноября 1989 г. // Международные акты о правах человека. Сборник документов / Сост. и вступ. ст.: Карташкин В.А., Лукашева Е.А. – М.: Норма, Инфра-М, 1998. – С. 306 – 323

113. Европейская Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. // Международные акты о правах человека. Сборник документов / Сост. и вступ. ст.: Карташкин В.А., Лукашева Е.А. – М.: Норма, Инфра-М, 1998. – С. 539 – 569

114. American Convention on Human Rights of 22 November 1969 / Organisation of the American States. - Human Constitutional Rights Documents – [Електронний ресурс]. – Режим доступу : http://www.hrcr.org/docs/American_Convention/oashr.html

115. The Charter of Fundamental Rights of the European Union of 7 December 2000 / European Union. - Official Journal of the European Union of 30.03.2010. – 2010. – С 83. – Рр. 389 – 403

причин наявних особливостей національного менталітету і розходжень законодавчих систем (як за формою, так і за змістом), не можуть забезпечити принцип екстериторіальності персональних даних»¹¹⁶.

Організація з економічного співробітництва та розвитку (далі – ОЕСР) однією з перших серед міжнародних організацій почала вживати заходи в цьому напрямку. Результатом роботи спеціальної експертної групи, створеної в рамках цієї міжнародної організації, стала розробка «Базових принципів захисту недоторканності приватного життя і транскордонних потоків персональних даних ОЕСР» (англ. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*), схвалених Рекомендацією Ради ОЕСР від 23 вересня 1980 р., нова редакція яких була ухвалена у 2013 р.¹¹⁷ Попри те, що ОЕСР є організацією з обмеженим членством (станом на 01.09.2014 р. – 34 члени, Україна не є членом ОЕСР), ці принципи стали вагомим внеском в подальший розвиток міжнародного регулювання питання захисту персональних даних.

Певну увагу цьому питанню приділяє й Організація Об'єднаних Націй (далі – ООН). Зокрема, Генеральна Асамблея ООН своєю резолюцією № 95 (XIV) затвердила «Керівні принципи регулювання комп'ютерних файлів, які містять персональні дані» (англ. *Guidelines for the Regulation of Computerized Personnel Data Files*): Певна діяльність з цього приводу здійснюється і в рамках внутрішньо організаційного механізму ООН та організацій і органів, афілійованих з ним. В той же час, слід відзначити, що зусилля ООН в цій сфері є замалими, і як центральний елемент системи міжнародного співробітництва ця організація повинна приділяти значно більше уваги цьому питанню.

На сучасному етапі можна констатувати, що найбільш розвинутим

116. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В.М.Брижко, А.І.Радянська, М.Я.Швець. – К.: Тріумф, 2006. – С. 19

117. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) as amended on 11 July 2013 by C(2013)79 / OECD. – [Електронний ресурс]. – Режим доступу: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>

є міжнародне співробітництво із захисту персональних даних, яке здійснюється на європейському континенті, зокрема в рамках Ради Європи та Європейського Союзу. Україна є активним учасником цього співробітництва, а європейська інтеграція віднедавна остаточно стала стратегічним пріоритетом зовнішньої політики нашої держави. Відповідно, чинне законодавство України про захист персональних даних розроблялося саме з урахування стандартів, розроблених в рамках цих структур.

Якщо вести мову про Раду Європи, то ця організація, як і ОЕСР, почала займатися проблемами, пов'язаними із захистом персональних даних, із кінця 1970-х рр. Підсумком стало прийняття Конвенції № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 р. (далі – Конвенція № 108)¹¹⁸. Крім того, 8 листопада 2001 р. було прийнято Додатковий протокол до цього міжнародного договору¹¹⁹. Україна приєдналася до Конвенції та Додаткового протоколу у 2010 р. Крім того, необхідно відзначити цілу низку рекомендацій та рішень щодо захисту персональних даних, розроблених Радою Європи та її органами, зокрема Комітетом Міністрів.

У рамках Європейського Союзу ключовим документом із приводу регулювання захисту персональних даних є Директива № 95/46/ЄС Європейського парламенту та Ради ЄС «Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних» від 24 жовтня 1995 р.¹²⁰ Крім того, в рамках цього інтеграційного об'єднання було прийнято цілу низку інших директив, регламентів та заяв, що стосуються цього питання, а з 2012 р. триває процес реформування системи правового регулювання захисту персональних даних у рамках

118. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. // Офіційний вісник України від 14.01.2011 р. – 2010/2011. – № 58.

119. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 р. // Офіційний вісник України від 14.01.2011 р. – 2010/2011. – № 58.

120. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року / Європейський Союз. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_242

ЄС, який має завершитися з прийняттям нових основоположних документів з цього приводу і внесенням змін в існуючі¹²¹.

Якщо говорити про відповідність законодавства України міжнародним стандартам у сфері захисту персональних даних, то слід зазначити, що право на приватність є одним із конституційно закріплених прав громадян України. Ще у ст. 54 Конституції Української РСР було закріплено, що: «Особисте життя громадян, таємниця листування, телефонних розмов і телеграфних повідомлень охороняються законом» [13].

Водночас, у ст. 32 Конституції України, прийнятій 28 червня 1996 р., це право виписано значно ґрунтовніше і ширше. Зокрема, окрім положення: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України», в ній також встановлено, що:

- не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом;
- кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею;
- кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації¹²².

Як бачимо, ця норма увібрала в себе не тільки стандарти права на приватність, які містяться в Міжнародному Пакті про громадянські

121. Protection of personal data // Official web-site of the European Commission. – [Електронний ресурс]. – Режим доступу: <http://ec.europa.eu/justice/data-protection/>

122. Конституція (Основний Закон) Української Радянської Соціалістичної Республіки від 20.04.1978 № 888-IX // Відомості Верховної Ради УРСР від 11.07.1978 р. – 1978. – №18. – Ст. 268.

та політичні права 1996 р. і Європейській конвенції про захист прав людини і основоположних свобод 1950 р., а й стандарти щодо захисту персональних даних (заборона на збір інформації про особу без її згоди) та права на доступ до публічної інформації (право отримувати відомості про себе, які зберігаються в певних структурах), а також гарантії судового захисту та відшкодування за порушення таких прав. З цим погоджуються і європейські експерти, зокрема М. Жорж твердить, що: «право на захист даних було вперше впроваджено в Україні в якості основного права в зв'язку з правом на приватне життя у статті 32 Конституції України 1996 року»¹²³.

Водночас, попри прогресивний характер ст. 32 Конституції України, існувала потреба в розробці та прийнятті спеціального законодавства в сфері захисту персональних даних. Це був досить тривалий процес, який спочатку виявлявся у включенні відповідних норм в різноманітні законодавчі акти, що регламентують діяльність в інформаційній сфері.

Вперше проект Закону України «Про захист персональних даних» № 2618, зареєстрований 10 січня 2003 р., авторства 5 народних депутатів, розглядався Верховною Радою України й був прийнятий за основу, однак в подальшому так і не був ухвалений в цілому. Новий проект Закону був зареєстрований у Верховній Раді України 25 березня 2003 р. і прийнятий як Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 р.¹²⁴, (далі – Закон).

Ухвалення цього Закону стало важливим кроком на шляху до подальшої розробки нормативного забезпечення організаційно-правової бази захисту персональних даних України. Крім цього законодавчого акта варто назвати також такі нормативні акти, як Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства

123. Конституція України прийнята на V сесії Верховної Ради України 28 червня 1996 р. (зі змінами) // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

124. Закон України «Про захист персональних даних» від 01.06.2010 №2297-VI // Офіційний вісник України від 09.07.2010 р. – 2010. – № 49. – С. 199.

про захист персональних даних» № 3454-VI від 2 червня 2011 р.¹²⁵; Типовий порядок обробки персональних даних; Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних; Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації. Останні три документи були затверджені Наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014р.

Важливим джерелом є також норми законодавства в інших сферах, пов'язаних із захистом, зберіганням та обробкою персональних даних. Зокрема, можна навести приклад Закону України «Про Єдиний державний демографічний реєстр» № 5492-VI від 20.11.2012 р., предмет якого напряму пов'язаний цією проблематикою і який містить цілу низку норм щодо обробки персональних даних.

Прийняття цього Закону стало вагомим кроком на шляху до імплементації Україною своїх міжнародних зобов'язань щодо захисту персональних даних. У той же час, його ухвалення є лише частиною цього процесу, оскільки інколи прийняті на національному рівні норми не відповідають міжнародним стандартам. Тому дослідження відповідності національного законодавства міжнародним нормам є важливою складовою дослідження стану виконання Україною міжнародних зобов'язань із захисту персональних даних.

Загалом експерти досить позитивно оцінюють існуючу вітчизняну законодавчу базу стосовно захисту персональних даних. Наприклад, М. Жорж відзначає: «На загальному рівні законодавча система відповідає обсягу європейського законодавства»¹²⁶. А. Погребна

125. Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» №3454-VI від 2 червня 2011 р. // Офіційний вісник України – 2011. – № 48.

126. Аналіз Закону України про захист персональних даних : DGI/DP/expertiseUKR(2012) /

твердить, що: «незважаючи на недосконалість Закону, його прийняття безперечно є позитивним кроком на шляху вдосконалення українського законодавства і приведення його у відповідність до європейських стандартів»¹²⁷.

У той же час лунають і критичні зауваження стосовно прийнятих та розроблених нормативно-правових актів. Так, Г. Саттон вважає, що: «Закон (Закон України «Про захист персональних даних» - прим. авт.) важкий для виконання та містить очевидні внутрішні суперечності. Деякі з його положень нереально жорсткі»¹²⁸.

Очевидно, що однією з головних проблем існуючого вітчизняного законодавства в сфері захисту персональних даних та його реалізації є його неповна відповідність існуючим європейським стандартам (в тому числі, Конвенції № 108 та Директиві ЄС). На це вказують і експерти (зокрема М. Жорж та Г. Саттон), наводячи конкретні приклади такої невідповідності після аналізу положень вітчизняного законодавства. Так, Г. Саттон виділяє:

- неповну імплементацію принципів, закріплених в ст. 5 Конвенції № 108 в зміст ст. 6 Закону;
- права суб'єкта персональних даних, згідно зі ст. 8, не включають в себе весь перелік відповідних прав, що містяться в Конвенції № 108 та Директиві ЄС);
- визначення поняття «обробка персональних даних», що міститься в ст. 2 Закону, не повною мірою відповідає Директиві ЄС;
- суперечність підстав обробки конфіденційних даних ст. 8 Директиви ЄС;
- обмеженість змісту інформації, яка підлягає реєстрації в наглядовому органі та внесенню в державний реєстр, порівняно із Директивою ЄС тощо¹²⁹.

М. Жорж, Г. Саттон. – Страсбург : Рада Європи, 2012. – 63 С.

127. Погребна А. Коментар до Закону України «Про захист персональних даних» / А. Погребна // Юридичний журнал. – 2010. – №7. – [Електронний ресурс]. – Режим доступу: <http://www.justinian.com.ua/article.php?id=3579>

128. Аналіз Закону України про захист персональних даних : DGI/DP/expertiseUKR(2012) / М. Жорж, Г. Саттон. – Страсбург : Рада Європи, 2012. – 63 С.

129. Аналіз Закону України про захист персональних даних : DGI/DP/expertiseUKR(2012) /

Це лише невелика частина критики Закону щодо його невідповідності європейським стандартам, висловленої експертами. Необхідно наголосити, що після прийняття Закону до нього було внесено цілу низку змін, однак і на сучасному етапі залишається ціла низка проблем, пов'язаних із приведенням законодавства України про захист персональних даних у відповідність із європейськими стандартами.

Порівняльний аналіз Закону із нормами Конвенції № 108, Директиви ЄС та інших документів дозволяє виявити проблеми, пов'язані з невідповідністю законодавства у цій сфері на сучасному етапі. Загалом можна констатувати, що українське законодавство в сфері захисту персональних даних у цілому відповідає положенням Конвенції № 108 та Додаткового протоколу до неї. В той же час, відповідності Директиві ЄС досягнуто не скрізь. Так, з-поміж іншого, можна навести наступні приклади:

- невідповідність положень Закону щодо визначення того, яка інформація є конфіденційною (ст. 5) та конфіденційності самого процесу обробки персональних даних (ст. 6 – 7) положенням Директиви ЄС, зокрема ст. 16 – 17. В цьому випадку необхідним є приведення норм Закону у відповідність із європейськими стандартами в частині більш чіткого визначення того, яка саме інформація повинна розглядатися як конфіденційна, а також включити в Закон вимоги щодо конфіденційності обробки персональних даних та прописати підстави і межі втручання у приватне життя громадян;
- нечітко прописано повноваження володільця персональних даних (термінологія Закону, в Директиві ЄС використовується термін «оператор персональних даних»). Існує необхідність включення в Закон більш широкого і чіткого переліку його повноважень, зокрема щодо обробки персональних даних із урахуванням положень Директиви ЄС;
- положення законодавства України щодо створення та

функціонування Єдиного державного демографічного реєстру передбачають обробку надто широкого переліку персональних даних¹³⁰. Це прямо суперечить ст. 5 Конвенції № 108 і ст. 6 Директиви ЄС щодо відповідності об'єму та змісту персональних даних, які підлягають збору та обробці, заявленій меті. Видається за доцільне внесення змін у відповідне законодавство з метою недопущення зловживань;

- недосконалими є положення пункту 2 частини четвертої ст. 29 Закону, які врегульовують транскордонну передачу персональних даних. Необхідним є приведення змісту цієї норми у відповідність із Главою III Конвенції № 108 та Главою IV Директиви ЄС.

Це лише частина недоліків, які існують у вітчизняному законодавстві щодо захисту персональних даних. Їх вирішення полягає не тільки у приведенні положень нормативних актів у відповідність із європейськими та міжнародними стандартами в цій сфері, а й у подальшому впорядкуванні і вдосконаленні існуючих механізмів. На жаль, регламентований обсяг і заявлена тема дослідження не дозволяють розглянути питання в повному обсязі. В той же час, у наступних дослідженнях видається можливим викласти концептуальні пропозиції стосовно вдосконалення існуючого правового регулювання захисту персональних даних в Україні.

Таким чином, можна констатувати, що захист персональних даних є важливою складовою міжнародного співробітництва в інформаційній сфері. Йому приділяється велика увага як на рівні норм міжнародних договорів, так і в практиці діяльності міжнародних організацій. Україна є активним учасником міжнародно-правових відносин, бере активну участь в діяльності міжнародних організацій і виступає стороною основних міжнародно-правових актів в цій сфері, в тому числі Конвенції № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 р. Курс нашої держави на євроінтеграцію зумовлює також приділення

108 особливої уваги актам Європейського Союзу в цій сфері, зокрема 130. Закон України «Про Єдиний державний демографічний реєстр» № 5492-VI від 20.11.2012 р. // Офіційний вісник України від 14.12.2012 р. – 2012. – № 93. – С. 122.

Директиві про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних від 24 жовтня 1995 р. Саме європейські стандарти складають основу міжнародних зобов'язань України в цій сфері.

Оцінюючи стан виконання Україною міжнародних зобов'язань у сфері захисту персональних даних, необхідно підкреслити, що національне законодавство є відносно новим. Саме це зумовлює існування цілої низки невідповідності його норм європейським стандартам. В той же час, стан виконання Україною цих зобов'язань можна оцінити як досить високий, зокрема в контексті стандартів, установлених Конвенцією № 108 Ради Європи. Серед основних невідповідностей, які потребують усунення, можна назвати положення стосовно визначення конфіденційності інформації та процесу її обробки; повноважень володільця персональних даних; транскордонної передачі персональних даних; окремих норм законодавства щодо Єдиного державного демографічного реєстру.

Усунення цих недоліків сприятиме як подальшій імплементації Україною взятих на себе зобов'язань щодо захисту персональних даних, модернізації національного законодавства в цій сфері, так і процесам інтеграції нашої держави до Європейського Союзу і в світовий інформаційний простір.

7. Досвід зацікавлених сторін у формуванні та реалізації державної політики у сфері електронного доступу до публічної інформації[©]

2014-й рік — четвертий рік дії Закону України «Про доступ до публічної інформації». Можна вважати, що становлення практики його застосування вже відбулося, її аналіз дасть можливість виявити певні досягнення, недоліки та їх причини. Право на доступ до інформації є одним із фундаментальних прав кожної правової демократичної держави. Доступність публічної інформації направлена як на забезпечення інтересів особи щодо реалізації своїх прав і свобод, так і на її участь у справах суспільства та держави; є основою здійснення громадського контролю за діяльністю публічної адміністрації, громадських організацій, станом економіки, екології та інших сфер суспільного інтересу.

Стаття 1 Закону України «Про доступ до публічної інформації» надає визначення об'єкта правового регулювання — публічної інформації: *«Публічна інформація — це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом. Публічна інформація є відкритою, крім випадків, встановлених законом»*¹³¹.

Ідея про доступ до публічної інформації базується на концепції, що є конкретний споживач, який потребує від публічної адміністрації інформації, що напряду з ним пов'язана. Однак, під цю характеристику

131. Закон України «Про доступ до публічної інформації» // Відомості Верховної Ради України. — 2011. — № 32. — ст. 314.

підпадає не так багато випадків. Особиста потреба в інформації часто традиційно вирішується за рахунок паперових засобів передачі інформації, в той же час як електронна документація розрахована на невизначене коло осіб. Відповідно, сама модель доступу до публічної інформації з використанням електронних засобів комунікації давно вийшла за межі образу споживача інформації із своїх справ. Уже не потрібно обґрунтовувати особистими потребами пошук різноманітної інформації, яку створюють органи державної влади та все ширше розміщують на своїх сайтах. Саме на основі концепції «доступу до публічної інформації», характерної для 70-х років ХХ століття, було сформовано й розвинене концепцію «відкритої держави» та «відкритого уряду». Організація економічного співробітництва та розвитку (Organisation for Economic Cooperation and Development) в 2005 р. визначила: «З точки зору громадськості, відкрита держава — це та, де бізнес, громадські організації та громадяни можуть: 1) «знати» — отримувати релевантну та зрозумілу інформацію; 2) «придбати» — отримувати сервіси та взаємодіяти з державою; 3) «створювати» — брати участь у процесі прийняття рішень. Принципи правильного управління — прозорість та підзвітність; чесність та рівність; дієвість та результативність; повага до закону та високі стандарти етичної поведінки — складають основу того, на чому будується відкрита держава»¹³².

Однак, беручи до уваги транзитивний характер українського суспільства, для України актуальними залишається розвиток за обома концепціями.

Розглянемо основні об'єкти, суб'єкти та їх функції в формуванні та реалізації державної політики у сфері електронного доступу до публічної інформації, встановлені національним законодавством.

Стаття 5 Закону України «Про звернення громадян» встановлює, що доступ до публічної інформації забезпечується шляхами: «1) систематичного та оперативного оприлюднення інформації:

132. Офіційний сайт OECD. – [Електронний ресурс]. – Режим доступу: <http://www.oecd.org/dataoecd/1/35/34455306.pdf>.

в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет; на інформаційних стендах; будь-яким іншим способом; 2) надання інформації за запитами на інформацію». Встановлюється сукупність суб'єктів державної політики у цій сфері. Суб'єктами відносин у сфері доступу до публічної інформації є: 1) запитувачі інформації¹³³ — фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень; 2) розпорядники інформації; 3) структурний підрозділ або відповідальна особа з питань запитів на інформацію розпорядників інформації (стаття 12). Розпорядниками публічної інформації статтею 13 Закону визначено: 1) суб'єкти владних повноважень — органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання; 2) юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, — стосовно інформації щодо використання бюджетних коштів; 3) особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, — стосовно інформації, пов'язаної з виконанням їхніх обов'язків; 4) суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, — стосовно інформації щодо умов постачання товарів, послуг та цін на них. До розпорядників інформації, зобов'язаних оприлюднювати та надавати за запитами інформацію, визначену в цій статті, у порядку, передбаченому цим Законом, прирівняно суб'єктів господарювання, які володіють: 1) інформацією про стан довкілля; 2) інформацією про якість харчових продуктів і предметів побуту; 3) інформацією про аварії, катастрофи, небезпечні природні

133. Термін «запитувач інформації», враховуючи вимогу Закону щодо обов'язковості оприлюднення (що забезпечує широке невизначене коло споживачів інформації) публічної інформації (статті 14 та 15) є не зовсім відповідним меті закону. На наш погляд, більш адекватним був би термін «споживач публічної інформації».

явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян; 4) іншою інформацією, що становить суспільний інтерес (суспільно необхідною інформацією). Одночасно до суб'єктів державної політики у цій сфері віднесено деякі *інституції парламентського та громадського контролю*: «1) Парламентський контроль за дотриманням права людини на доступ до інформації здійснюється Уповноваженим Верховної Ради України з прав людини, тимчасовими слідчими комісіями Верховної Ради України, народними депутатами України. 2) Громадський контроль за забезпеченням розпорядниками інформації доступу до публічної інформації здійснюється депутатами місцевих рад, громадськими організаціями, громадськими радами, громадянами особисто шляхом проведення відповідних громадських слухань, громадської експертизи тощо» (стаття 17). Також частиною 1 статті 23 визначено участь у здійсненні політики у цій сфері *інституцій державного та судового контролю* та встановлено норми щодо права на оскарження рішень, дій чи бездіяльності розпорядників інформації: «Рішення, дії чи бездіяльність розпорядників інформації можуть бути оскаржені до керівника розпорядника, вищого органу або суду».

Особливу увагу з огляду на цілі дослідження привертають відносини, пов'язані з обігом публічної інформації в електронній формі. По-перше, частиною 1 статті 15 встановлено 12 основних видів публічної інформації, що підлягають обов'язковому оприлюдненню невідкладно, але не пізніше п'яти робочих днів з дня затвердження документа — за наявності у розпорядника інформації офіційного веб-сайту така інформація *оприлюднюється на веб-сайті із зазначенням дати оприлюднення документа і дати оновлення інформації* (частина 2 статті 15). По-друге, статтею 19 встановлено, що запити на інформацію можуть подаватися в усній, письмовій чи іншій формі (поштою, факсом, телефоном, електронною поштою) на вибір запитувача (частина 3), який має містити: ім'я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є (частина 5). Для спрощення процедури оформлення письмових запитів на інформацію частиною

6 статті 19 передбачено, що особа може подавати запит шляхом заповнення відповідних форм запитів на інформацію, які можна отримати в розпорядника інформації та на офіційному веб-сайті відповідного розпорядника. Зазначені форми мають містити стислу інструкцію щодо процедури подання запиту на інформацію, її отримання тощо.

Зазначені нормативно-правові акти можна вважати національною концепцією, що визначає як загальну інформаційну політику держави на ближню перспективу, таку, що встановлює основні напрями розвитку інформаційних відносин між державою, суспільством та людиною, так і національну політику щодо формування та реалізації цифрових відносин між усіма суб'єктами електронного врядування та електронної демократії, що сформовано у сфері електронного доступу до публічної інформації.

Участь законодавчої влади. Визнання певних «прогалин» у забезпеченні прав громадян на доступ до публічної інформації призвела до прийняття змін та доповнень до всього інформаційного блоку законодавчих актів України, що налічує близько 60 законів¹³⁴.

Питання також обговорювалось на парламентських слуханнях на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні». Рекомендації, схвалені за їх результатами, пропонують уряду: 1) розробити та внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законодавчих актів України з урахуванням практики застосування Закону України «Про доступ до публічної інформації» та з метою усунення правових колізій, що виникли внаслідок прийняття Закону України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації»; а також щодо засад оприлюднення органами державної влади відкритих даних та відповідальності за їх недотримання¹³⁵.

134. Закон України від 27.03.2014 р. № 1170-VII про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації» Відомості Верховної Ради. – 2014. – № 22. – ст.816

135. Постанова Верховної Ради України від 3 липня 2014 року № 1565-VII // Відомості Верховної

Окрім того, Уповноваженим Верховної Ради України з прав людини у 2014 році вперше в щорічному Звіті з прав людини про стан дотримання прав і свобод людини і громадянина сформульовано спеціальний розділ 10 «Дотримання права на доступ до публічної інформації», в якому проаналізовано питання 1) щодо реагування органів місцевої влади на запити про надання публічної інформації ; 2) щодо офіційних веб-сайтів обласних, районних державних адміністрацій, міських рад обласних центрів та міст обласного значення; 3) веб-сайти Верховної Ради України, Кабінету Міністрів України, Адміністрації Президента України та міністерств ; 4) обмеження доступу до інформації ; 5) судова практика¹³⁶.

Участь судової влади забезпечується як формуванням механізмів доступу до судової інформації¹³⁷, так і розв'язанням спорів у цій сфері у судовому порядку.

- 1) Конституційний Суд України, розглянувши три питання щодо відкриття конституційного провадження у справі за конституційним зверненням щодо офіційного тлумачення Закону України «Про доступ до публічної інформації» прийняв ухвали щодо відмови у їх відкритті¹³⁸.

Ради. – 2014. – № 33. – ст.1163.

136. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина. – К., 2014. – 552 с. [Електронний ресурс] Перевірено 09.09.2014 р. URL: http://www.ombudsman.gov.ua/images/stories/01042014-decl/dopovid_2014b.pdf

137. Ґрунтується на нормах Закону України «Про доступ до судових рішень» // Відомості Верховної Ради України. – 2006. – № 15. - ст. 128. [Електронний ресурс] Перевірено 09.09.2014 р. URL: <HTTP://ZAKON2.RADA.GOV.UA/LAWS/SHOW/3262-15>

138. Ухвала Конституційного Суду України: 1) від 30 серпня 2011 року № 36-у/2011 (Справа № 2-37/2011) про відмову у відкритті конституційного провадження у справі за конституційним поданням Тернопільської обласної ради щодо офіційного тлумачення окремих положень Конституції України, Закону України „Про місцеве самоврядування в Україні“, Закону України „Про статус депутатів місцевих рад“, Закону України „Про доступ до публічної інформації“ <http://www.ccu.gov.ua/doccatalog/document?id=151255>;

2) від 25 червня 2013 року № 29-у/2013 (Справа № 2-26/2013) про відмову у відкритті конституційного провадження у справі за конституційним зверненням Міжнародної благодійної організації «Екологія-Право-Людина» щодо офіційного тлумачення положень частин першої, другої, третьої статті 21 Закону України «Про доступ до публічної інформації» <http://www.ccu.gov.ua/doccatalog/document?id=209000>; 3) від 31 жовтня 2013 року № 49-у/2013 (Справа № 2-50/2013) про відмову у відкритті конституційного провадження у справі за конституційним зверненням громадянина Свєтїфєєва Микити Ігоровича щодо офіційного тлумачення положень частини другої статті 21 Закону України «Про доступ до публічної інформації» <http://www.ccu.gov.ua/doccatalog/document?id=209000>.

- 2) Вищі суди України періодично узагальнюють практику застосування судами законодавства про доступ до інформації¹³⁹.
- 3) Аналіз судової практики з вирішення спорів між запитувачами публічної інформації та її розпорядниками, здійснений Управлінням з питань підготовки конституційних подань та дотримання права на доступ до публічної інформації Секретаріату Уповноваженого Верховної Ради України з прав людини,¹⁴⁰ вивчення судової практики та судової статистики Вищого адміністративного суду України, виявив низку недоліків щодо: 1) відсутності статистичної звітності адміністративних судів, яка б надала можливість відстежити кількісні показники розгляду адміністративних справ, пов'язаних із застосуванням Закону; 2) визначення предметної підсудності, якщо розпорядник публічної інформації не є суб'єктом владних повноважень; 3) однозначного розуміння терміна «публічна інформація»; 4) однозначного розуміння відмінності між інформаційним запитом на підставі Закону України «Про доступ до публічної інформації» та зверненням громадян на підставі Закону України «Про звернення громадян»; 5) неоднакових підходів судів до мотивування рішень щодо розв'язання однакових за суттю спорів з приводу доступу до публічної інформації; 6) неоднакової судової практики тлумачення положень Закону щодо надання інформації, яка має гриф «для службового користування».

Участь органів державної влади та органів місцевого

gov.ua/doccatalog/document?id=226117.

139. Постанова Пленуму Вищого адміністративного суду України від 30.09.2013 р. № 11 «Про практику застосування адміністративними судами положень Закону України від 13 січня 2011 року № 2939-VI «Про доступ до публічної інформації»» [Електронний ресурс] Перевірено 09.09.2014 р. url: <http://zakon2.rada.gov.ua/laws/show/v0011760-13> та Оглядовий лист Вищого господарського суду України від 12.06.2014 р. № 01-06/770/2014 р. «Про деякі питання практики застосування господарськими судами законодавства про інформацію (за матеріалами справ, розглянутих у касаційному порядку Вищим господарським судом України)» - [Електронний ресурс] Перевірено 09.09.2014 р. url: <http://zakon2.rada.gov.ua/laws/show/v-770600-14>

140. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина. – К., 2014. – 552 с. [Електронний ресурс] Перевірено 09.09.2014 р. url: http://www.ombudsman.gov.ua/images/stories/01042014-decl/dopovid_2014b.pdf

самоврядування забезпечувалась шляхом: 1) розширення доступу до публічної інформації через збільшення категорії інформації, що повинна розміщуватися публічною адміністрацією в мережі Інтернет; 2) більш чіткою регламентації надання доступу до публічної інформації; 3) здійснення відповідного державного контролю за виконанням вимог законодавства та сприйняття ініціатив громадського контролю.

Важливим кроком для забезпечення прав громадян було рішення щодо організації надання засудженим послуг доступу до глобальної мережі Інтернет¹⁴¹, що надається: 1) у відокремлених приміщеннях житлової зони поза межами локальних дільниць відділень соціально-психологічної служби у місці, доступному для відвідування усіма засудженими установи; 2) або у комп'ютерному класі загальноосвітнього навчального закладу установи; 3) у структурних дільницях установ виконання покарань, де передбачено тримання засуджених у приміщеннях камерного типу — у відокремлених приміщеннях обладнуються ізольовані робочі місця доступу до мережі Інтернет. Встановлено, що перелік веб-ресурсів, до яких надається доступ для користування засудженими установи, затверджується комісією установи у складі начальника установи та керівників структурних підрозділів установи. Перелік щокварталу переглядається та доповнюється за заявами засуджених. Забороняється доступ засуджених до веб-ресурсів, не включених до переліку, таких, що демонструють жорстокість, насильство, агресію, носять еротичний або порнографічний зміст тощо, а також до соціальних мереж та користування електронною поштою. Комісія установи також надає дозвіл на користування засудженими засобами IP-телефонії та відеозв'язку через мережу Інтернет (Skype).

Важливим питанням державної політики у цій сфері є формування системи опублікування публічної інформації в мережі Інтернет. Так, Державний комітет телебачення і радіомовлення України оприлюднив

141. Див.: Порядок організації надання засудженим до позбавлення волі доступу до глобальної мережі Інтернет, затверджений Наказом Міністерства юстиції України від 01.08.2014 р. № 1275/5 // Офіційний вісник України від 05.09.2014 — 2014 р., № 69, стор. 324, стаття 1950. [Електронний ресурс] Перевірено 09.09.2014 р. url: <http://zakon2.rada.gov.ua/laws/show/z0991-14>

результати моніторингу інформаційного наповнення офіційних веб-сайтів органів виконавчої влади за перше півріччя 2014 року¹⁴². Моніторинг охопив 72 центральних та 25 місцевих органів виконавчої влади¹⁴³. У висновках регуляторний орган відзначив, що інтернет-сторінки органів влади недостатньо інформативні щодо систем обліку публічної інформації, адрес електронної пошти керівників органів, їх заступників, керівників структурних підрозділів, основних функцій структурних підрозділів, правил внутрішнього трудового розпорядку, порядку та умов проходження конкурсу на заміщення вакантних посад тощо. Зокрема, системи обліку публічної інформації деяких органів виконавчої влади оновлюються нерегулярно та містять відомості лише про частину документів, які перебувають у суб'єктів владних повноважень.

Участь громадськості здійснювалася шляхом: 1) реалізації громадських ініціатив із надання незалежної інформації стосовно виконання відповідних державних функцій; 2) інформування громадян про свої права та допомоги у відстоюванні цих прав, зокрема — через суд; 3) ініціювання перед публічною адміністрацією як вирішення поточних та перспективних проблем подолання недоліків у виконанні державних функцій, так і внесення змін та доповнень у правові норми, що регулюють виконання державних функцій.

Можна відзначити реалізацію «Transparency International — Україна» пілотних проектів громадського контролю: 1) «Прозорість

142. Аналітична довідка Державного комітету телебачення і радіомовлення України за результатами проведеного моніторингу інформаційного наповнення офіційних веб-сайтів органів виконавчої влади у першому півріччі 2014 року [Електронний ресурс] Перевірено 09.09.2014 р. url: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113636&cat_id=112507%А0

143. Моніторинг інформаційного наповнення офіційних веб-сайтів органів виконавчої влади здійснюється Державним комітетом телебачення і радіомовлення України на виконання пункту 9 постанови Кабінету Міністрів України від 29.08.2002 № 1302 «Про заходи щодо подальшого забезпечення відкритості у діяльності органів виконавчої влади» та згідно з Порядком проведення моніторингу інформаційного наповнення веб-сайтів органів виконавчої влади, затвердженим наказом Держкомтелерадіо України від 12.10.2012 № 273. Метою моніторингу є оцінка рівня інформаційного наповнення офіційних веб-сайтів органів виконавчої влади відповідно до вимог нормативно-правових актів, які регламентують розміщення певних видів інформації на відповідних веб-сайтах. Об'єктами моніторингу є офіційні веб-сайти міністерств, інших центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій.

державних закупівель органів публічної влади України: етика розкриття інформації»¹⁴⁴, який було реалізовано у 2012 році проведенням аналізу та проведенням рейтингування 100 офіційних веб-сайтів органів публічної влади України в частині оприлюднення ними інформації про власні закупівлі; 2) «Громадянське суспільство та медіа за прозорі місцеві бюджети!» реалізується Одеською обласною організацією ВГО КВУ в партнерстві з «Transparency International – Україна» (розпочато 2014) <http://ti-ukraine.org/news/oficial/4857.html>; 3) Впровадження Стандарту відкритості та прозорості державних закупівель для органів місцевого самоврядування України (2013 р.) - <http://ti-ukraine.org/what-we-do/projects/project-2744.html>; 4) моніторинг майнових декларацій державних службовців – під громадський контроль (2013) <http://ti-ukraine.org/what-we-do/projects/project-2739.html> тощо.

Також є цікавими громадські ініціативи «Общественный контроль»¹⁴⁵ <http://4road.net/> та «УкрЯма»¹⁴⁶ <http://ukryama.com/>, «Наші гроші»¹⁴⁷ <http://nashigroshi.org> та інші.

Активне впровадження ІКТ в систему суспільно-політичних відносин суттєво розширює можливості громадян щодо їх громадської участі, створює умови для формування якісно нового рівня активності громадян, які користуються сучасними електронними технологіями не тільки в особистих цілях, а й в цілях суспільно-політичної участі на всіх рівнях публічного управління.

144. Як органи влади та створені ними підприємства інформують громадськість про власні закупівлі за бюджетний коштів? Результати громадського аудиту наповненості сайтів замовників торгів / за заг. ред. О.С. Хмари. – К.: ФОП Рибалко І.О., 2013. – 24 с. - http://ti-ukraine.org/system/files/library/tiuk_broshure_a5_inet.pdf

145. Проект «Общественный Контроль» объединяет граждан всех городов Украины, общественные организации и активных людей, небезразличных к проблемам дорожного сектора, ЖКХ, торговли и прочим.

146. Сайт объединяет тех, кто столкнулся с некомпетентностью дорожных и иных служб Украины, которые не выполняют свои обязательства.

147. Идея сайту «Наші гроші» з'явилась після серпня 2010 року, коли під тиском журналістів, громадських діячів і деяких політиків сталися зміни в тендерному законодавстві України. Ці зміни дозволили отримати суспільству більш широкий доступ за лаштунки розподілу бюджетних коштів. Разом з тим кількість інформації, яка з'являється у «Віснику державних закупівель», виявилась настільки великою, що жодній редакції чи громадському об'єднанню не під силу відслідкувати все, що варте уваги. «Наші гроші» проводять вибірково аналіз тендерів України.

8. Нарис концепції змін до законодавства України у сфері доступу до публічної інформації[©]

*Свобода інформації є основним правом людини і критерієм усіх видів свобод, захисту яких Об'єднані Нації себе присвятили*¹⁴⁸.

Протягом кількох останніх десятиліть спостерігається тенденція до світового визнання права особи на інформацію - «права знати». На сьогодні близько 80% населення світу мешкає в державах, які прийняли нормативно-правові акти, що регулюють порядок реалізації права на інформацію. Як на міжнародному, так і на рівні окремих держав утвердження цього права пройшло шлях від визнання свободи розповсюдження інформації — до гарантованого права отримати від держави інформацію, що перебуває в її розпорядженні. Тлумачення суті цього права також поступово уточнювалося. Наразі загальновизнаним є його розуміння як невід'ємної частини права на вільне вираження своїх поглядів, що гарантується статтею 34 Конституції України, статтею 19 Міжнародного пакту про громадянські та політичні права та статтею 10 Конвенції про захист прав людини і основоположних свобод.

13 січня 2011 року Верховна Рада України прийняла Закон України «Про доступ до публічної інформації» (далі — «Закон»), який 9 травня 2011 року набрав чинності. Аналіз практики застосування Закону вже протягом майже чотирьох років свідчить про існування певних недоліків його положень. Ці недоліки призводять до неоднозначної практики реалізації права на доступ до публічної інформації, стримують вибудовування однакової судової практики як ефективного засобу захисту від порушення цього права. Якщо

148. Созыв международной конференции по вопросу о свободе информации: Резолюция 59 (1) первой сессии Генеральной Ассамблеи ООН, 14 декабря 1946 г.

не вжити заходів для підвищення рівня якості положень Закону шляхом внесення змін, ефективна імплементація інституту доступу до публічної інформації в українському суспільстві буде практично неможливою, невідвратною стане також втрата й так невисокого рівня довіри суспільства до цього інституту.

Відповідно, наразі актуальним є питання зміни положень Закону з метою підвищення рівня їх якості. Нижче надається обґрунтування необхідності зміни певних положень Закону на підставі аналізу адміністративної та судової практики його застосування.

1. Реалізація права на доступ до публічної інформації без перебільшення починається із законодавчого визначення, що є публічною інформацією. Відповідно до статті 1 Закону публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

З наведеного визначення умовно можна виокремити щонайменше дві групи суттєвих ознак публічної інформації. До першої групи ознак, з приводу яких на практиці не виникає суперечностей, можна віднести те, що інформація має бути відображена та задокументована будь-якими засобами та на будь-яких носіях. Відповідно, це готовий продукт для надання за запитом. Щодо цих ознак явних суперечностей на практиці не виникало, що свідчить про задовільний рівень юридичної техніки викладення відповідної частини положення Закону. З огляду на це зупиняємось на них детально наразі не є доцільним.

До другої групи можна віднести решту ознак, які містяться у визначенні, і саме вони на практиці знайшли неоднакове тлумачення.

122 Законодавче визначення вказує, перш за все, на те, що публічною інформацією є вся інформація, яка наявна у суб'єкта владних

повноважень, незалежно від автора цієї інформації та способу потрапляння її у володіння суб'єкта владних повноважень. На це вказує словосполучення «або яка знаходиться у володінні суб'єкта владних повноважень», що за своїм змістом охоплює всю інформацію: що була створена суб'єктом владних повноважень, що була ним отримана як при виконанні ним своїх обов'язків, так і незалежно від них, а також ту, що не створена або не отримана суб'єктом владних повноважень у вигляді вхідної кореспонденції ззовні, але наявна у його володінні. Так, наприклад, мова йде про інформацію, що міститься в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації. Відповідно, вся інформація, яка є у суб'єкта владних повноважень, є публічною інформацією.

Таке тлумачення по суті дається також у науково-практичному коментарі до Закону України «Про доступ до публічної інформації», підготовленому Центром суспільних медіа за підтримки Міжнародного фонду «Відродження» і Програми сприяння Парламенту¹⁴⁹, та повною мірою відображає концепцію максимальної відкритості інформації, якою володіє суб'єкт владних повноважень, — концепцію, з метою імплементації якої було розроблено Закон.

Однак, є й інша позиція. Так, у Довідці про вивчення та узагальнення практики застосування адміністративними судами положень Закону України «Про доступ до публічної інформації», підготовлений Вищим адміністративним судом України¹⁵⁰, зокрема, вказується, що за визначенням публічної інформації, передбаченим Законом, можна виокремити такі ознаки публічної інформації:

- «1) готовий продукт інформації, який отриманий або створений лише в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством;
- 2) заздалегідь відображена або задокументована будь-якими засобами та на будь-яких носіях інформація;

149. <http://www.pdp.org.ua/materials-pdp/2685-api-comment>.

150. http://www.vasu.gov.ua/ua/news_legislation.html?_m=publications&_t=rec&id=2964&s=print.

- 3) така інформація знаходиться у володінні суб'єктів владних повноважень або інших розпорядників публічної інформації;
- 4) інформація не може бути публічною, якщо створена суб'єктом владних повноважень не під час виконання суб'єктами владних повноважень своїх обов'язків;
- 5) інформація не може бути публічною, якщо створена не суб'єктом владних повноважень.

У разі відсутності перелічених ознак в інформації, така інформація не належить до публічної.

Отже, визначальним для публічної інформації є те, щоб вона була заздалегідь готовим, зафіксованим продуктом, отриманим або створеним лише суб'єктом владних повноважень у процесі виконання своїх обов'язків. Щодо не суб'єктів владних повноважень, то вони можуть бути тільки розпорядниками такої інформації.»

Як бачимо, розуміння публічної інформації, викладене у вказаній Довідці, очевидно відрізняється від попереднього. З огляду на вказані в ній ознаки не вся інформація, якою володіє суб'єкт владних повноважень, є публічною, а лише та, що створена або отримана суб'єктом владних повноважень у процесі виконання своїх обов'язків. При цьому, враховуючи п. 5 наведеного в Довідці переліку ознак публічної інформації, отримана суб'єктом владних повноважень інформація має бути створена іншим суб'єктом владних повноважень.

Однак, така позиція є спірною хоча б тому, що виходячи із положень Закону, публічною інформацією також може бути інформація, до якої суб'єкт владних повноважень не має жодного відношення. Так, відповідно до положень статті 13 Закону розпорядниками інформації для цілей цього Закону визнаються, зокрема, суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, - стосовно інформації щодо умов постачання товарів, послуг та цін на них. До розпорядників інформації, зобов'язаних оприлюднювати та надавати за запитами інформацію, визначену в цій статті, у порядку, передбаченому цим Законом, прирівнюються суб'єкти господарювання, які володіють:

- 1) інформацією про стан довкілля;
- 2) інформацією про якість харчових продуктів і предметів побуту;
- 3) інформацією про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян;
- 4) іншою інформацією, що становить суспільний інтерес (суспільно необхідною інформацією).

З огляду на вказане, слід визнати, що техніко-юридичні недоліки допущені законодавцем у визначенні публічної інформації, спричинилися до неоднозначної практики його тлумачення.

Враховуючи принципову важливість чіткого розуміння, що є публічною інформацією, для ефективної практики реалізації права на доступ до публічної інформації вважаємо за необхідне внести зміни до положення частини першої статті 1 Закону, а саме викласти це положення у наступній редакції: «Публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, яка знаходиться у володінні суб'єктів владних повноважень, інших визначених цим Законом розпорядників публічної інформації в межах, передбачених цим Законом».

Таким чином, існує необхідність внесення змін до частини першої статті 1 Закону щодо визначення поняття публічної інформації.

2. Іншим недоліком Закону можна вважати те, що він не передбачає безоплатного надання публічної інформації обсягом понад 10 сторінок особі, яка знаходиться в скрутному матеріальному становищі й не має можливості ознайомитися з такою інформацією у визначеному розпорядником місці для роботи запитувачів з документами чи їх копіями. Так, наприклад, позбавлені можливості отримати публічну інформацію особи, які знаходяться в умовах обмеження свободи (в місцях, в яких особи примусово утримуються за судовим рішенням або рішенням адміністративного органу

відповідно до закону) та у яких немає джерела фінансового доходу. З огляду на зазначене пропонується доповнити Закон положенням, яке б надавало право на безоплатне отримання публічної інформації вказаній категорії осіб.

Таким чином, вважаємо за необхідне доповнити статтю 21 Закону положеннями щодо надання права на безоплатне отримання публічної інформації певній категорії осіб, коли задоволення запиту на інформацію передбачає виготовлення копій документів обсягом понад 10 сторінок.

3. Відповідно до частини третьої статті 9 Закону Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень (далі — «Перелік відомостей»), не може бути обмеженим у доступі. Це положення Закону було імplementовано Указом Президента України «Питання забезпечення органами виконавчої влади доступу до публічної інформації» від 5 травня 2011 року № 547/2011. Так, підпунктом 9 пункту 2 вказаного Указу доручається Кабінету Міністрів України, центральним органам виконавчої влади, Раді міністрів Автономної Республіки Крим, обласним, Київській, Севастопольській міським, районним державним адміністраціям забезпечити безумовне виконання Закону України «Про доступ до публічної інформації», затвердити переліки відомостей, що становлять службову інформацію, та оприлюднити їх в установленому порядку. Відповідно, наразі кожен з вищезазначених органів виконавчої влади затвердив перелік відомостей, про який ідеться. Затвердження таких переліків створило умови для усталеної практики, коли, всупереч вимогам статті 6 та частини першої статті 9 Закону, які визначають вичерпні підстави для обмеження доступу до інформації через присвоєння їй грифу «для службового користування», Перелік відомостей

повсякчасно використовується розпорядниками інформації, включаючи суди, як підстава для відмови у наданні запитуваної інформації. Іншими словами, вказане положення Закону розуміється розпорядниками інформації як таке, що надає необмежену дискрецію вирішувати, яку інформацію він може не давати за інформаційними запитами, — необхідно тільки скласти Перелік такої інформації і потім посилатись на нього, відмовляючи у наданні інформації. Інколи можна побачити в Переліку відомостей навіть категорії інформації, обмеження доступу до якої прямо заборонено Законом (наприклад, інформацію щодо використання бюджетних коштів).

Перелік відомостей може складатися лише з абстрактних категорій інформації, яка може бути віднесена до службової, безвідносно до конкретної інформації (конкретного документа). Тобто, по суті йдеться про перелік категорій відомостей, які можуть бути віднесені до службової інформації у разі дотримання відповідних вимог Закону (статті 6 та 9). Функціонально перелік відомостей є нічим іншим як орієнтиром для запитувачів щодо інформації, яка може бути у володінні у відповідного розпорядника та доступ до якої у разі дотримання умов, передбачених Законом, у кожному конкретному випадку може бути обмежено. Однак, вказана функція також є сумнівною, оскільки Перелік відомостей не вказує на наявність чи відсутність у розпорядника конкретної інформації.

Враховуючи вказане та усталену повсякчасну практику використання Переліку відомостей як підстави для відмови у наданні публічної інформації, вбачається за доцільне вилучити положення частини третьої статті 9 Закону і, таким чином, взагалі ліквідувати інститут Переліку відомостей.

Таким чином, із Закону доцільно вилучити положення частини третьої статті 9.

4. Закон України «Про захист персональних даних», який набрав чинності 1 січня 2011 року, передбачає, що персональні дані

особи — це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Положення цього Закону чітко регламентують права суб'єкта персональних даних та порядок обробки персональних даних. З іншого боку, положення статті 10 Закону передбачають інший порядок доступу до інформації про особу.

У цьому контексті актуальним є рішення Європейського суду з прав людини «Щокін проти України»¹⁵¹. У цій справі Європейський суд визнав порушення права заявника, гарантоване статтею 1 Першого протоколу до Конвенції про захист прав людини та основоположних свобод. Європейський суд вказав, що законодавство, на підставі якого здійснювалось обмеження права заявника не відповідало вимозі якості закону, оскільки на той час існувало два чинних нормативно-правових акта, які по-різному врегульовували порядок оподаткування діяльності заявника. Такий стан законодавства не забезпечує адекватного захисту від свавільного втручання органів державної влади у права особи.

Відповідно, для усунення ризику незаконного обмеження права особи внаслідок застосування двох актів, що по-різному регулюють порядок доступу до інформації про особу, вважаємо за доцільне статтю 10 Закону вилучити.

5. Відповідно до положень статті 6 Конвенції Ради Європи про доступ до офіційних документів, у разі надання доступу до офіційного документа особа, яка звернулась із запитом, вправі ознайомитися з оригіналом чи копією або отримати копію цього документа у будь-якій доступній формі чи форматі за власним вибором, якщо тільки висловлена нею перевага не є нерозумною.

У випадку обмеження доступу до частини інформації, яка міститься в офіційному документі, орган державної влади повинен, незважаючи на це, надати доступ до решти інформації, яка міститься у документі.

151. Рішення Європейського суду з прав людини у справі «Щокін проти України» від 14 жовтня 2010 року № 23759/03 та № 37943.06, п. 56.

Будь-які пропуски мають бути чітко помічені. При цьому, у разі коли неповна версія документа неправильно передає його зміст або є беззмістовною, або якщо видача частини документа становить безпідставні складнощі для владної установи, то у видачі документа може бути відмовлено¹⁵².

Відповідно до частини другої статті 7 Закону України «Про інформацію» ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом. Виходячи із вказаного положення, логічним є твердження, що особа має право обирати форму, в якій їй повинна надаватись публічна інформація. Системний аналіз положень статей 9, 14, 15, 19 Закону також свідчить, що він імпліцитно передбачає право запитувати інформацію саме у формі копії документа, в якому вона міститься. Однак, відсутність чіткого положення, яке б вказувало на таке право особи, призводить до різної практики щодо цього питання.

Так, наприклад, в ухвалі від 24 квітня 2014 року Донецький апеляційний адміністративний суд (справа № 805/2112/13-а) вказав, що, оскільки законодавством передбачено право на отримання інформації, вимоги позивача щодо зобов'язання відповідача надати копію документа, в якому міститься запитувана інформація, замість листа, яким останній повідомляв інформацію, задоволенню не підлягають.

З огляду на вказане, з метою приведення положень Закону у відповідність до вимог Конвенції про доступ до офіційних документів та підвищення рівня якості Закону пропонується доповнити Закон положенням про обов'язок розпорядника інформації на вимогу запитувача надавати інформацію у формі копії документа (у разі його наявності та технічної можливості зробити копію) з вилученою з неї інформацією, доступ до якої обмежено (наприклад, конфіденційною інформацією).

¹⁵² http://crimecor.rada.gov.ua/komzloch/control/uk/publish/article.jsessionid=C75D14A4396DDB62F4F196E8FD76B58E?art_id=49046&cat_id=46352

6. Відповідно до статті 8 Конвенції Ради Європи про доступ до офіційних документів запитувач, чий запит був відхилений, повинен мати доступ до процедури оскарження в суді або до іншого незалежного та безстороннього органу, передбаченого законом. У пояснювальній записці до вказаної Конвенції вказується, що орган оскарження повинен мати повноваження або самостійно скасовувати рішення розпорядника інформації, яке на його думку суперечить законодавству, або звернутися до розпорядника з проханням переглянути свою позицію. Існування в державі позасудового незалежного органу оскарження неправомірної відмови у наданні інформації вважається доброю практикою.

Зараз можна почути різні пропозиції щодо концепції незалежного позасудового контрольного органу, який би забезпечував дотримання права на доступ до інформації. Одні відстоюють необхідність нормативного закріплення вказаного інституту на рівні Конституції України. Інші наполягають на необхідності створення нового органу державної влади з відповідними повноваженнями в межах існуючої системи державних органів.

Щодо першого варіанта необхідно зауважити: дійсно, в деяких європейських державах діють так звані інформаційні комісари, в повноваження яких входить здійснення заходів для контролю за дотриманням права на доступ до інформації та поновлення порушеного права у разі виявлення порушення. Незалежність цієї посадової особи забезпечується, зокрема, тим, що вона структурно та функціонально не підпорядковується жодному органу державної влади. Однак, створення такого інституту в нашій правовій системі потребує: а) значного часу, оскільки внесення змін до Конституції України є складною і довготривалою процедурою; б) значних фінансових витрат, оскільки передбачає створення фактично нового органу державної влади із своїм апаратом державних службовців; в) певного часу для встановлення усталеної ефективної співпраці із державними органами. Крім того, на практиці діяльність такого

органу (посадової особи) потребуватиме координації та узгодження з діяльністю Омбудсмана України, який також на підставі положення статті 101 Конституції України здійснює парламентський контроль за дотриманням прав людини.

Другий варіант, а саме створення нового органу в межах існуючої системи державних органів також не вбачається відповідним. Який би орган не утворив Уряд або парламент у межах своїх повноважень, він не може вважатися незалежним від них і, відповідно, ефективність здійснення таким органом контрольної функції одразу ставиться під сумнів.

У зв'язку з викладеним більш ефективним та раціональним видається третій варіант вирішення порушеного питання, а саме внесення змін до відповідних законів України і наділення вже існуючого органу державної влади відповідними повноваженнями. Виникає питання щодо органу, який може мати такі повноваження. Відповідь очевидна — такі повноваження в українській правовій системі доцільно надавати тільки Омбудсману, оскільки цей інститут: а) є за своєю природою контрольним механізмом за дотриманням прав людини з боку органів державної влади; б) інституційно та функціонально є незалежним від будь-якої гілки влади; в) має усталену практику співпраці з державними органами; г) має вже функціонуючий апарат державних службовців, який з наданням нових повноважень необхідно доповнити лише в частині розширення штату спеціалістів відповідного напрямку діяльності.

Зауважимо, що первісно проект Закону України «Про доступ до публічної інформації» містив положення, які передбачали надання Омбудсману повноваження в сфері доступу до публічної інформації. Однак, чомусь такі необхідні положення було вилучено, і наразі, через чотири роки після прийняття Закону необхідно знову повернутися до цього питання. До того ж ще існує ще один аргумент на користь надання вказаних повноважень Омбудсману: з січня 2014 року Омбудсман України виконує аналогічні функції у сфері захисту персональних даних.

Таким чином, вбачаємо необхідність доповнення Закону та Закону України «Про Уповноваженого Верховної Ради України з прав людини» положеннями щодо надання Омбудсману повноважень у сфері доступу до публічної інформації, зокрема позасудового незалежного органу для оскарження неправомірної відмови у наданні інформації.

7. Відповідно до частини четвертої статті 6 Закону інформація з обмеженим доступом має надаватися розпорядником інформації, якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше. Це означає, що відмова у наданні інформації буде обґрунтованою лише за умови наявності мотивованого висновку розпорядника інформації про те, що законні підстави для обмеження у доступі до запитованої інформації, які існували раніше, продовжують існувати й на день надання запитувачу такої інформації (тобто, кожного разу, відмовляючи у наданні такої інформації, необхідно з'ясовувати наявність підстав указаних в частині другій статті 6). Такий обґрунтований висновок має надаватися розпорядником інформації в листі, яким він відмовляє у наданні запитованої інформації з мотивів обмеження доступу до неї. Відповідно, відмова у наданні публічної інформації лише в зв'язку з тим, що колись такій інформації було присвоєно гриф «для службового користування» або до цього на аналогічний запит було надано відмову, не може вважатися законною.

Однак, проблема виникає у разі, якщо запитується інформація, який гриф «для службового користування» присвоєно іншим розпорядником інформації. Складно уявити, щоб питання зняття грифу ефективно розглядалось розпорядником, який його не присвоював.

З огляду на вказане пропонується доповнити Закон положенням, яким передбачити порядок перенаправлення розпорядником інформації запиту вказаної категорії до розпорядника, який присвоював гриф, для розгляду та надання відповіді.

Законом України «Про внесення змін до Закону України «Про

Уповноваженого Верховної Ради України з прав людини» щодо національного превентивного механізму» N 5409-VI від 02.10.2012 до Закону України «Про Уповноваженого Верховної Ради України з прав людини» було внесено, зокрема, статтю 19-1(Виконання Уповноваженим функцій національного превентивного механізму). Положення цієї статті надали Уповноваженому з прав людини можливість залучати на договірних засадах (на платній або безоплатній основі) до регулярних відвідувань місць несвободи представників громадських організацій, експертів, учених та фахівців, у тому числі й іноземних. За два роки функціонування національного превентивного механізму результати діяльності мережі незалежних моніторів засвідчили свою ефективність. Фактично діяльність моніторів є основою ефективною реалізації національного превентивного механізму. Щодо реалізації права на доступ до публічної інформації необхідно зазначити, що одним із способів забезпечення доступу до публічної інформації є надання інформації за запитами. Однак, не володіючи інформацією про стан адміністративної практики з надання відповідей за запитами на інформацію, практично неможливо дати об'єктивну оцінку, а також встановити системні проблеми адміністративної практики у цій сфері та, відповідно, заходи для їх усунення. Для цього, враховуючи позитивний досвід функціонування мережі незалежних моніторів у межах національного превентивного механізму, вважаємо за доцільне створення такої мережі для моніторингу адміністративної практики з надання відповідей на інформаційні запити. З метою реалізації такої ідеї також необхідно внести зміни до Закону України «Про Уповноваженого Верховної Ради України з прав людини».

Питання зміни законодавства у сфері доступу до публічної інформації є нагальним та необхідним. По-перше, необхідно покращити якість положень Закону України «Про доступ до публічної інформації», по-друге, необхідно створити незалежний та позасудовий механізм контролю за дотриманням права на доступ до публічної інформації шляхом надання відповідних повноважень Уповноваженому Верховної Ради України з прав людини.

ПІДРОЗДІЛ 3.2.

ЗАБЕЗПЕЧЕННЯ СВОБОДИ ТА ПЛЮРАЛІЗМУ ЗМІ

9. Правове регулювання діяльності засобів масової інформації в рамках права Європейського Союзу[©]

Протягом перших 25 років свого існування Європейське співтовариство не виробило всеосяжної комплексної політики щодо засобів масової інформації (далі – ЗМІ). І тільки в 1980-ті роки, коли супутникове телебачення ввело транснаціональний вимір у телевізійну діяльність, розпочалася демонополізація, з'явилося комерційне телебачення. Сектор набув економічного значення, а разом з цим Спільнота почала вибудовувати систему аудіовізуальної політики і регулювання. Мета полягала в тому, щоб створити справді європейську сферу ЗМІ, принаймні в аудіовізуальній царині, і реалізувати стратегію зміцнення позицій європейської аудіовізуальної продукції в галузі. Більше того, до прийняття Маастрихтського договору (1992 р.) Європейське співтовариство не мало безпосередніх договірних повноважень вживати заходи у галузі ЗМІ. Лише тоді до Договору про заснування Європейських співтовариств (1957 р.) було введено статтю 128 (тепер – ст. 167 Договору про функціонування Європейського Союзу (ДФЄС)), присвячену регулюванню діяльності в сфері культури, яка серед іншого регулювала і діяльність аудіовізуальних ЗМІ.

© *Терехова Тетяна Андріївна, аспірантка кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка*

Розглядаючи проблему правового регулювання діяльності засобів масової інформації в ЄС, треба визначитися з тим, що саме розуміють під цим терміном в міжнародному праві і передусім у межах європейського правового простору¹⁵³. В першу чергу треба відзначити, що в рамках міжнародного права не вироблено якогось сталого переліку видів ЗМІ. Більше того, в міжнародному праві й праві ЄС відсутній якийсь універсальний документ, який регулював би їх діяльність.

Наприклад, в Рекомендації Комітету Міністрів Ради Європи державам-членам CM/Rec(2007)15 до ЗМІ відносять: друківані медіа (газети, періодичні видання), медіа, які поширюють інформацію через електронні комунікаційні мережі, такі, як телерадіомовлення (радіо, телебачення та інші лінійні аудіовізуальні медійні послуги), новинні послуги он-лайн (он-лайн випуски газет та інформаційних повідомлень), нелінійні аудіовізуальні медійні послуги (відео на замовлення)¹⁵⁴. В той же час, в резолюції Парламентської асамблеї Ради Європи (ПАРЄ) 428 (1970) «Щодо декларації про засоби масової інформації та права людини» говориться про «друковані та інші засоби масової інформації»¹⁵⁵ (п. А1). Інша рекомендація ПАРЄ № 1950 (2011) «Захист журналістських джерел інформації» використовує більш широке поняття — «сучасні ЗМІ все ширше використовують можливості мобільних і мережевих засобів комунікації. У них ширше застосовується інформаційний і візуальний контент, одержаний не від журналістів»¹⁵⁶ (п. 11). У рамках ще однієї рекомендації Комітету Міністрів Ради Європи запропоновано принципово інший підхід до ЗМІ взагалі: «широке поняття ЗМІ, яке включає всіх

153. Гнатівський М.М. Європейський правовий простір. Концепція та сучасні проблеми. – К.: Прометей, 2005.

154. Рекомендація CM/Rec(2007)15 Комітету Міністрів країнам-членам Ради Європи щодо висвітлення виборів засобами масової інформації [Електронний ресурс]. – Режим доступу: http://www.medialaw.kiev.ua/laws/laws_international/155/.

155. Резолюція 428 (1970) Отноительно декларации о средствах массовой информации и правах человека [Електронний ресурс]. – Режим доступу: http://www.data.minsk.by/books/ce_massmedia/3.html.

156. Рекомендація 1950 (2011). Защита журналистских источников информации [Електронний ресурс]. – Режим доступу: <http://medialaw.asia/document/-9606>.

учасників, пов'язаних з виробництвом та розповсюдженням, серед потенційно великої кількості людей, контенту (наприклад, інформації, аналізу, коментарів, думок, освіти, культури, мистецтва і дозвілля у друкованій, аудіо, візуальній, аудіовізуальній чи іншій формі) і способи застосування, які спрямовані на те, щоб сприяти інтерактиву масових комунікацій (наприклад, в соціальних мережах) або іншій, заснованій на контенті широкомасштабній інтерактивній діяльності (наприклад, ігри в режимі «он-лайн»), при цьому зберігаючи (у всіх цих випадках) редакційний контроль або нагляд над контентом»¹⁵⁷.

У рамках Заключного акта НБСЕ (1975 р.) до сфери ЗМІ було віднесено друковані засоби, радіо, телебачення, кіно і телеграфні агентства (частина IV, гл. 2)¹⁵⁸. У рішеннях Ради ООН з прав людини до видів ЗМІ відносять – «друковані ЗМІ, радіо, телебачення, Інтернет»¹⁵⁹. Разом з тим, у ключовій директиві в рамках регулювання транскордонної діяльності, пов'язаної зі ЗМІ в ЄС, – 2007/65/ЄС «Про внесення змін до Директиви Ради 89/552/ЄЕС про координацію деяких положень, закріплених у законах, правилах або адміністративних заходах в державах-членах, що стосуються телевізійного мовлення»¹⁶⁰, вказується, що вона регулює лише діяльність «аудіовізуальних ЗМІ», якими є «передавання рухомих зображень зі звуком або без, в тому числі німі фільми, але не охоплює передачу звуку або радіо-послуги. ... Окрім надання програм як основної мети аудіовізуальних медіа послуг, до поняття таких послуг включено текстовий контент, який супроводжує

157. Рекомендация CM/Rec (2011)7 Комитета министров государствам-членам о новом понятии СМИ (Принята Комитетом министров 21 сентября 2011 года на 1121-ом заседании постоянных представителей министров) [Электронный ресурс]. – Режим доступа: http://cyberpeace.org.ua/files/ii_e_14.pdf.

158. Заключительный акт Совещания по безопасности и сотрудничеству в Европе (Хельсинки, 1 августа 1975 года) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. XXXI. – М., 1977. – С. 544–589.

159. Резолюция Совета ООН по правам человека №12/16 от 2 октября 2009 г. «Свобода мнений и их свободное выражение» [Электронный ресурс]. – Режим доступа: http://cyberpeace.org.ua/files/ii_a_2.pdf.

160. Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (Text with EEA relevance) // OJ L 332, 18/12/2007, pp. 27 – 45.

програми, наприклад субтитрування та електронні програмні гіди» (п. 22), а також «аудіовізуальні медіа послуги на замовлення», які «подібні до телевізійного мовлення», наприклад, змагаються за ту ж аудиторію, а характер і засоби доступу до послуги дають користувачам небезпідставні очікування на нормативно-правовий захист у рамках дії цієї Директиви» (п. 23). У свою чергу, в Конвенції ООН «Про міжнародне право спростування» (1952 р.), замість терміна «ЗМІ» використовують термін «інформаційні агентства», який «означає будь-яку організацію в галузі друку, радіо, кіно, телебачення або телефотографії»¹⁶¹ (ст. 1 п. 2). Досить цікавим є системний підхід, запропонований нещодавно в Раді Європі, до визначення «нового, широкого поняття ЗМІ, яке включає всіх учасників, пов'язаних з виробництвом та розповсюдженням, серед потенційно великої кількості людей, контенту (наприклад, інформації, аналізу, коментарів, думок, освіти, культури, мистецтва і дозвілля у друкованій, аудіо, візуальній, аудіовізуальній чи іншій формі) і способи застосування, які спрямовані на те, щоб сприяти інтерактивним масовим комунікаціям (наприклад, у соціальних мережах) або іншій заснованій на контенті широкомасштабній інтерактивній діяльності (наприклад ігри в режимі «он-лайн»), при цьому зберігаючи (в усіх цих випадках) редакційний контроль або нагляд над контентом»¹⁶².

У документах ЄС ситуація є наступною. В ДФЄС згадуються лише «аудіовізуальний сектор» (ст. 167 п. 2). Директива 2010/13/EU «Про аудіовізуальні медіа послуги», у свою чергу, визначає як такі «телевізійне мовлення згідно з визначенням, наведеним у пункті (е) цієї частини, або аудіовізуальну медіа послугу на замовлення»¹⁶³ (ст. 1 п. 1.a.i). У Директиві 2003/33/ЄС щодо зближення законів, правил та адміністративних положень держав-членів, пов'язаних з

161. Конвенція о международном праве опровержения (1952 г.) [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/decl_conv/conventions/correct.shtml.

162. Рекомендация CM/Rec (2011)7 Комитета министров государствам-членам о новом понятии СМИ // Международное информационное право. Учебное пособие. / А.В. Задорожний, А.В. Пазюк. – Том 1. – К., 2013. – С. 766–802, 769–770.

163. 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) (codified version) // Official Journal. – L 95. – 15.4.2010. – P. 1 – 24.

рекламою та спонсорством тютюнових виробів, згадуються лише друковані ЗМІ, радіомовлення і ЗМІ «сфери послуг інформаційного суспільства»¹⁶⁴ (ст. 1). В резолюції Європарламенту (2008/2129 (INI)) «Медіаграмотність у цифровому світі» (2008 р.) виділяють «аудіовізуальні та друковані, традиційні і цифрові... нові» види ЗМІ (п. В)¹⁶⁵. В інших документах згадуються також різні он-лайн послуги у ЗМІ.

У доктрині міжнародного права підходи до правого регулювання ЗМІ також різні. Німецький дослідник Г. Штромайер вважає, що варто використовувати термін «мас-медіа», до якого належать: друковані засоби масової інформації; аудіовізуальні засоби масової інформації (радіо і телебачення); засоби масової інформації, що працюють у режимі «он-лайн», або інтернет-мультимедійні ЗМІ¹⁶⁶. О. Кастендік, Е. Доммерінг і А. Шоєр відзначають, що окреме правове регулювання існує для преси і мовних ЗМІ¹⁶⁷. Росіянин Ю.М. Колосов, використовуючи термін «ЗМІ» стверджує, що до них відносять «електрозв'язок та інформаційно-комунікаційні технології (радіомовлення, телевізійне мовлення, передача інформації з мереж комп'ютерного зв'язку), а також поширення тиражованої друкованої, звукової та візуальної продукції у вигляді книг, газет, журналів, кінострічок, компакт-дисків тощо. Використовується також термін «масові комунікації», який включає не тільки поширення інформації, а й взаємні контакти між джерелами інформації та її споживачами, тобто зворотній інформаційний зв'язок»¹⁶⁸. Українська дослідниця І.А. Кисарець вказує, що складовими європейського медіа-ринку є

164. Directive 2003/33/EC of the European Parliament and of the Council of 26 May 2003 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products (Text with EEA relevance) // OJ. – L 152. – 20/06/2003. – P. 16 – 19.

165. European Parliament resolution of 16 December 2008 on media literacy in a digital world (2008/2129(INI)) // Official Journal. – 23.2.2010. – P. 9.

166. Штромайер, Герд. Політика і мас-медіа / Пер. з нім. А. Орган. – К.: Вид. дім «Києво-Могилянська академія», 2008. – 303 с.

167. Castendyk O., Dommering E.J., Scheuer A. European Media Law. – Alphen aan den Rijn: Kluwer Law International 2008. – 1426 p.

168. Международное право: учебник для бакалавров / под ред. А. Н. Вылегжанина. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2012. – 904 с.

видавництво, преса, радіо та телебачення, репродукція медіа, відео, реклама¹⁶⁹. У цьому випадку хотілося б зазначити: важко погодитися з тим, що все перераховане є однорівневими категоріями, оскільки, наприклад, реклама входить як один з видів діяльності на телебаченні, радіо й у пресі.

Таким чином, можна відзначити, що в праві ЄС під «ЗМІ» розуміють аудіовізуальні ЗМІ й так звані нові ЗМІ, тобто ті, що функціонують у мережі Інтернет або використовують для передачі мобільний зв'язок. Саме такі види ЗМІ переважно підпадають під регулювання права ЄС, маючи певні особливі режими правового регулювання. Друковані мас-медіа також відносяться до ЗМІ, проте в рамках права ЄС не мають особливого правового режиму, на відміну від вищезгаданих (регулюється лише питання реклами в них тютюнових виробів).

У рамках права ЄС правове регулювання ЗМІ здійснюється при одночасному використанні як актів первинного права — норм засновницьких договорів (ДЄС і ДФЄС), так і вторинного права — директив та регламентів (законодавство ЄС), а також рішень Суду ЄС і міжнародних договорів. Певну роль у розумінні існуючого законодавства ЄС і перспектив його розвитку відіграють акти рекомендаційної сили (повідомлення і рішення Європейської Комісії, рішення Ради ЄС, резолюції Європейського Парламенту тощо). Основним на сьогодні документом для регулювання діяльності аудіовізуальних ЗМІ в ЄС є консолідована Директива 2010/13/ЄС про аудіовізуальні медіа послуги (2010 р.), яка встановила ключові терміни та принципи діяльності на ринку аудіовізуальних ЗМІ. Проте, цей документ не забезпечив гармонізацію всієї сфери аудіовізуальних ЗМІ в ЄС, він лише вирішив низку питань, пов'язаних з їх діяльністю, як послуг. Певні аспекти діяльності ЗМІ врегулювали інші акти вторинного права. Зокрема, ряд питань щодо авторських прав у процесі діяльності аудіовізуальних і нових ЗМІ вирішено в рамках *Директиви Ради 93/83/ЄЕС «Про координацію деяких*

169. Європейський Союз: економіка, політика, право: енциклопедичний словник / Гол. ред. В. В. Копійка. – К.: Київський університет, 2011. – С. 137.

положень авторського права і суміжних прав при застосуванні їх до супутникового мовлення і кабельної ретрансляції»¹⁷⁰. Вона забезпечує високі стандарти захисту для авторів, акторів, виробників фонограм та дикторів, а також колективний та обов'язковий менеджмент прав кабельної ретрансляції через колективні об'єднання, які репрезентують різноманітні категорії правовласників. Директива 2006/116/ЕС встановлює строк авторського права в 70 років після смерті автора на літературні, художні, кінематографічні або аудіовізуальні твори. Для останніх двох категорій обчислення строку захисту починається після смерті останньої особи, яка залишилася з числа безпосередніх власників. Це автори сценаріїв, автори діалогів і музики. Та ж Директива визначає на 50 років умови захисту основних прав, що випливають із згаданого вище (виконавців, виробників фонограм або фільмів і організацій теле- і радіомовлення). Інша Директива (96/9/ЕС) забезпечує захист баз даних, як створених на папері, так і електронних, протягом 15 років після їх створення, що робиться для забезпечення привабливого середовища для інвестицій в них, зберігаючи інтереси користувачів. Європейська Конвенція з питань авторського права і прав, які відносяться до нього в сфері закордонної супутникової трансляції, перебуває на стадії розробки¹⁷¹.

Проблеми гармонізації національного законодавства про рекламу і спонсорство в ЗМІ інших, ніж аудіовізуальні ЗМІ, врегульовані у Директиві № 2003/33/ЕС «Про зближення законів, правил та адміністративних положень держав-членів, що стосуються реклами і спонсорства тютюнових виробів»¹⁷², яка забороняє рекламу і спонсорство для сигарет та інших тютюнових виробів. Заборону реклами лікарських засобів значно обмежено

170. Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission // OJ. – L 248. – 06/10/1993. – P. 15 – 21.

171. Муссіс Н. Вступ до Європейського Союзу. Право, економіка, політика. Вип. 15. Європейський Союз і його громадяни. / Н. Муссіс. – К.: ВЦ «Київський університет», 1999. – 45 с.

172. Directive 2003/33/EC of the European Parliament and of the Council of 26 May 2003 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products (Text with EEA relevance) // OJ. – L 152. – 20/06/2003. – P. 16 – 19.

в рамках критеріїв, установлених в директиві № 2001/83/ЄС «Про кодифікацію права Співтовариства щодо лікарських засобів для людини»¹⁷³ (зі змінами аж до директиви 2010/84/EU), яка забороняє рекламу для широкої публіки певних лікарських засобів, в першу чергу, зрозуміло, в ЗМІ. Важливим для рекламного ринку в ЗМІ є Регламент № 1924/2006 «Про харчування і користь для здоров'я від продуктів»¹⁷⁴, яким визначено певні часові та матеріальні вимоги до реклами продуктів харчування, зокрема встановлено до неї принцип пропорційності. Обмеження щодо застосування забороненої комерційної практики у мас-медіа, недобросовісної комерційної практики, наприклад, такої, що вводить в оману, і агресивних методів, що застосовуються в аудіовізуальних медіа-послугах, встановлено в рамках Директиви 2005/29/ЄС «Про несправедливу комерційну практику бізнес-споживачів на внутрішньому ринку»¹⁷⁵. Ряд директив присвячено також проблемам мережевої передачі сигналу мовлення для аудіовізуальних ЗМІ – Директиви 95/51¹⁷⁶, 96/19 і 1999/64¹⁷⁷. Цими директивами встановлено гармонізовані вимоги щодо спеціальних або виняткових прав користуватися мережевою інфраструктурою кабельного телебачення і протидіяти обмеженням на використання телекомунікаційних мереж для доставки кабельного телебачення.

Певним чином діяльності ЗМІ торкаються також норми ст.

173. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use // OJ. – L 311. – 28/11/2001. – P. 67 – 128.

174. Regulation (EC) No 1924/2006 of the European Parliament and of the Council of 20 December 2006 on nutrition and health claims made on foods // OJ. – L 404. – 30/12/2006. – P. 9 – 25.

175. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance) // OJ. – L 149. – 11/06/2005. – P. 22 – 39.

176. Commission Directive 95/51/EC of 18 October 1995 amending Directive 90/388/EEC with regard to the abolition of the restrictions on the use of cable television networks for the provision of already liberalized telecommunications services // OJ. – L 256. – 26/10/1995. – P. 49 – 54.

177. Commission Directive 1999/64/EC of 23 June 1999 amending Directive 90/388/EEC in order to ensure that telecommunications networks and cable TV networks owned by a single operator are separate legal entities (Text with EEA relevance) // OJ. – L 175. – 10/07/1999. – P. 39 – 42.

45-48 ДФЄС, що передбачають свободу пересування осіб в ЄС. Мова йде, зокрема, про журналістів, які можуть вільно працювати у всьому ЄС. Діяльності ЗМІ, за певних умов, може стосуватися ст. 207 ДФЄС (спільна торгова політика). Наприклад, якщо буде відбуватися міжнародний продаж певних аудіовізуальних творів для ЗМІ, які можуть вплинути на культурне і мовне розмаїття в Союзі, то рішення, замість прийняття кваліфікованою більшістю буде потребувати одностайності в Раді.

Щодо власне місця правового регулювання діяльності ЗМІ в правовій системі ЄС, то тут варто відзначити наступне. Як відомо, діяльність ЄС базується на кількох принципах, закріплених в його засновницьких договорах: Договорі про Європейський Союз (ДЄС) і Договорі про функціонування Європейського Союзу (ДФЄС), які діють зараз в редакції Лісабонського договору 2007 р.¹⁷⁸. Це є принцип наділення компетенцією, який передбачає, що Союз діє тільки в межах компетенції, наданої йому за Договорами державами-членами, для досягнення цілей, встановлених договором (ст. 5 п. 2 ДЄС), згідно з яким виділено три сфери компетенцій: а) виключна компетенція ЄС (ст. 3 ДФЄС); б) спільна компетенція ЄС з державами-членами (ст. 4 ДФЄС); в) компетенція ЄС, спрямована на координацію дій держав-членів (ст. 6 ДФЄС). З цього випливає другий принцип — принцип субсидіарності, суть якого у вузькому тлумаченні, передбаченому в ДЄС, полягає в тому, що ЄС діє в сферах компетенцій, що зазначені вище у пунктах «б» і «в», лише в тій мірі, в якій передбачені цілі не можуть бути досягнуті на національному рівні (ст. 5 п. 3). Відповідно до принципу пропорційності зміст і форма дій ЄС не виходять за рамки того, що необхідно для досягнення цілей засновницьких договорів (ст. 5 п. 4). На даний момент жодна компетенція ЄС у сфері ЗМІ в засновницьких договорах не встановлена. Проте, ще в 1974 р. Суд ЄС встановив, що мовлення (транскордонне) має бути визнане послугою за змістом статті 49

178. Основополагающие акты Европейского Союза: учредительные документы Европейского Союза, Хартия Европейского Союза об основных правах, Лиссабонский договор 2007 г. с комментариями / Под ред. С. Ю. Кашкина. – М.: ИНФРА-М, 2008. – 704 с.

ДЗЄС. Зараз у договорах існує лише побічне відсилання до ЗМІ в рамках розділу «культура» (ст. 167 ДФЄС), що відноситься до тієї частини, де компетенція ЄС спрямована на координацію дій держав-членів. У цій статті передбачено, що «Діяльність Союзу прагне заохочувати співробітництво держав-членів і, якщо необхідно, підтримувати і доповнювати їх діяльність в... художній і літературній творчості, в тому числі в аудіовізуальному секторі» (ст. 167 п. 2). З цією метою Союз може діяти як зовні, так і всередині держав-членів. У рамках діяльності зовні, щодо держав — не членів (за термінологією ЄС «третіх країн»), може як укласти договори з третіми країнами та компетентними міжнародними організаціями у сфері культури, а особливо виділено Раду Європи (ст. 167 п. 3), що має важливе значення для регулювання співробітництва в сфері ЗМІ, а також створення європейського інформаційного простору. Діяльність з укладання таких договорів також підпадає під регулювання ст. 207 ДФЄС, що вже в рамках «спільної торгової політики», яка вже відноситься до виключної компетенції ЄС і, відповідно, «Рада постановляє одноголосно стосовно ведення переговорів та укладення угод... у сфері торгівлі культурними та аудіовізуальними послугами, коли подібні угоди ризикують завдати шкоди культурному і мовному розмаїттю Союзу» (ст. 207 п. 4а). Щодо діяльності всередині ЄС, то тут у сфері культури, а отже і ЗМІ, органи Союзу можуть ухвалювати два типи рішень: 1) відповідно до звичайної законодавчої процедури Європейський парламент і Рада після консультацій з Комітетом регіонів ухвалюють «заохочувальні заходи — виключаючи при цьому будь-яку гармонізацію законодавчих та підзаконних актів держав-членів»; 2) «Рада за пропозицією Комісії приймає рекомендації» (ст. 167 п. 5).

Отже, як бачимо з цих статей, ЄС не наділений у сфері ЗМІ в рамках ст. 167 ДФЄС якимисьь прямо встановленими правами з гармонізації національного законодавства, він може лише заохочувати та рекомендувати державам-членам вживати певні дії в рамках свого національного законодавства в сфері ЗМІ. Як з цього приводу

слушно зауважив К. Д. Классен, стаття 167 вказує, що неекономічна («програмістська») сторона мовлення залишається в основній сфері національної відповідальності¹⁷⁹. Інші говорять, що ЄС лише має «культурну додаткову функцію»¹⁸⁰ і не має мандата на розробку всеосяжної культурної політики ЄС. Суд ЄС також звернув увагу на подвійну роль мовлення — з одного боку, економічної активності, а з іншого — політичного та культурного публічного виконання завдань, причому, він дозволив державам-членам обмежувати свободу надання послуг (справа C-288/89 Gouda). ЄС лише сприяє культурному співробітництву між державами-членами і підтримує їх дії. Додаткові заходи слід розуміти як вираження принципу субсидіарності. В той же час, діяльність у сфері ЗМІ є також одним із видів підприємницької діяльності, яка підпадає під регулювання правом ЄС і засновницькими договорами в рамках діяльності у внутрішньому ринку ЄС. Крім того, як ми зазначали, транскордонне мовлення передбачає надання певних послуг населенню держав-членів, а отже є також діяльністю в рамках однієї з чотирьох головних свобод ЄС — свободи надання послуг, а отже й такою, що регулюється правом ЄС (ст. 56-57 ДФЄС). Свободу надання послуг можна здійснювати в різних формах. У нашому випадку мова йде про транскордонне переміщення самої лише послуги, без переміщення надавача та отримувача послуги (наприклад, теле- або радіопередачі). При цьому важливою є також наявність достатньої інфраструктури, яка уможливорює стабільне і неперервне здійснення оплачуваної економічної діяльності на території відповідної держави¹⁸¹.

Саме як «послуги» визначила діяльність ЗМІ Зелена книга ЄС (1992р.), які, відповідно, мають зазнавати регулювання органами Європейського Союзу відповідно до убезпечення від економічної

179. Oppermann T., Classen C.D., Nettesheim M. Europarecht. Ein Studienbuch. / T. Oppermann, C.D. Classen, M. Nettesheim. – Berlin: Beck-Verlag, 2009. – P. 477.

180. Wemmer B. Die neuen Kulturklauseln des EG-Vertrages. Eine Analyse der Art. 128 EGV und Art. 92 Abs. 3 lit. d) EGV. / B. Wemmer. – Frankfurt/M., Berlin, Bern, New York, Paris, Wien, 1996. – 219p.

181. Judgment of the Court (Fifth Chamber) of 11 December 2003 in Case C-215/01 (Reference for a preliminary ruling from the Amtsgericht Augsburg): Bruno Schnitzer (Freedom to provide services — Directive 64/427/EEC — Skilled services in the plastering trade — National rules requiring foreign skilled-trade undertakings to be entered on the trades register — Proportionality) // Reports of Cases. – 2003. – P. 95.

концентрації. Це означає, що Союз має, наприклад, брати до уваги плюралізм засобів масової інформації, коли йдеться про застосування законодавства про конкуренцію ЄС в секторі засобів масової інформації. У всіх цих видах діяльності ЄС може ухвалювати акти з узгодження національного законодавства держав-членів у формі регламентів або директив. Різниця в юридичній силі цих актів полягає в тому, що у першому випадку акт має безпосередньо застосовуватися в державах-членах як такий без додаткової імплементації в національне законодавство (ст. 288 ДФЄС) і, як відзначає С. Ю. Кашкін, тоді держави здійснюють уніфікацію свого законодавства¹⁸², а у випадку директив — держави-члени мають досягнути певного результату, встановленого в директиві, але вибір форм і способів досягнення такої трансформації залишається на розсуд держав-членів (ст. 288 ДФЄС), відповідно відбувається процедура гармонізації законодавства. Саме як реалізацію права ЄС на лібералізацію послуг визначив директиву 89/552/ЄЕС про транскордонне телебачення М. Гердеген¹⁸³. Такої ж думки тримався і Суд ЄС ще 1974 р., проте тоді мова йшла не про транскордонне, а про прикордонне мовлення (справа 155/73 «Sacchi»), причому ці послуги були для нефізичних продуктів — телебачення. Суд визначив, що за відсутності конкретних договірних положень, що цьому суперечать, телевізійні програми за своєю природою повинні розглядатися як надання послуг.

Разом з тим, Директивою 2006/123/ЕС «Про послуги на внутрішньому ринку» встановлено широкий перелік послуг, які виключаються із загального режиму надання послуг. Зокрема, із загального режиму вилучаються: послуги, пов'язані з персональним захистом даних; телекомунікаційні послуги; послуги в аудіовізуальному секторі. Ці виключення йдуть в продовження практики Суду ЄС, який ще раніше у справі C-384/93 «Alpine Investments» (1995 р.), в якій Суд підтвердив законність законодавчої заборони так званих «холодних дзвінків», тобто телефонних дзвінків з пропозицією будь-

182. основополагающие акты Европейского Союза: учредительные документы Европейского Союза, Хартия Европейского Союза об основных правах, Лиссабонский договор 2007 г. с комментариями / Под ред. С.Ю. Кашкина. — М.: ИНФРА-М, 2008. — 704 с.

183. Гердеген М. Европейське право / Пер. з німецької. / М. Гердеген. — К.: «К.І.С.», 2008. — 528 с.

яких товарів або послуг, що здійснюються поза волею абонента, навіть якщо така заборона є лише в одній з країн, яка надає транскордонні послуги. Проте, за основу для видання директиви про аудіовізуальні послуги були обрані саме статті ДФЕС, що регулюють право заснування та надання послуг в ЄС (ст. 53(1) і 62). Це є цілком обґрунтовані дії за такою схемою: аудіовізуальні послуги є послугами, проте ці послуги не регулюють в рамках звичайного режиму послуг. Навіть після прийняття Директиви «Телебачення без кордонів» все ще залишається ряд невіршених питань, зокрема про юрисдикцію над мовними компаніями та моніторингу контенту програм, що призводить до проблем юрисдикції над ними між деякими державами-членами. Оскільки Директива «Про телебачення» просто передбачила мінімальні стандарти, організатори ЗМІ переважно оселилися в державах-членах з ліберальними системами регулювання і нагляду, хоча ретранслявали його й на інші.

Суд ЄС в своїх рішеннях також підкреслив право держав-членів обмежити ступінь недискримінації з міркувань переважання суспільного інтересу за умови, що національне законодавство з мовлення не гармонізоване на європейському рівні. Як відповідні причини були, зокрема, визнані: національні авторські права¹⁸⁴; національні цілі соціальної / культурної політики, наприклад, на користь плюралістичної / некомерційної системи мовлення¹⁸⁵. В той же час цікавим є приклад фрагментації міжнародного права в рамках прийняття рішень з однієї справи в сфері аудіовізуальних ЗМІ. Так, Європейський суд з прав людини в своїх справах, ґрунтуючись на ст. 10 ЄКПЛ (свобода преси), визначив, що монополія є несумісною з вимогами Конвенції про права людини (наприклад, EGMRE 276 «Informationsverein Lentia u.a.»), проте Суд ЄС з аналогічної проблеми

184. Judgment of the Court of 18 March 1980. – SA Compagnie generale pour la diffusion de la television, Coditel, and others v Cine Vog Films and others. - Reference for a preliminary ruling: Cour d'appel de Bruxelles - Belgium. – Provision of services : Cable diffusion of television. – Case 62/79. // European Court reports. – 1980. – P. 881.

185. Judgment of the Court of 3 February 1993. – Vereniging Veronica Omroep Organisatie v Commissariaat voor de Media. – Reference for a preliminary ruling: Raad van State – Netherlands. – Freedom to provide services – Free movement of capital – National legislation designed to preserve a pluralistic and non-commercial broadcasting network. – Case C-148/91. // European Court reports. – 1993. – P. I-00487.

в рішенні зі справи С-260/89 «ERT» пояснив, що, виходячи з певних міркувань, монополія є сумісною з вимогами ДЗЄСп. Але, постачання фізичних об'єктів для мовлення, наприклад, відеокасет, залежить від вільного руху товарів (ст. 28 ДЗЄСп).

Законодавство ЄС про конкуренцію продовжує бути ще одним важливим інструментом для втручання ЄС у сферу регулювання діяльності засобів масової інформації¹⁸⁶. Як було зазначено Судом ЄС ще в 1982 р., законодавство про конкуренцію, безсумнівно, належить до сфери телекомунікацій¹⁸⁷. Хоч законодавство ЄС про конкуренцію не містить жодних положень, напряму пов'язаних з медіа, воно сприяє забезпеченню конкуренції на європейському ринку, правда, тільки з економічної або ринкової точки зору. Злиття та поглинання медіа-компаній чи компаній в будь-якій іншій галузі відбувається за однаковими принципами. Статті 101 і 102 ДФЄС визначають загальні принципи, що стосуються конкурентного законодавства, які забороняють змову та експлуатацію домінуючим становищем на ринку. Крім того, в рамках спеціального регламенту ЄС присвяченого злиттю — № 4064/89 «Про контроль злиття між підприємствами» — говориться про існування такого явища, як злиття «у вимірі ЄС», що починається від об'єднання капіталів з певних сум, від яких має бути отримано дозвіл Комісії. Крім того, встановлене право держав-членів вжити відповідних заходів щодо захисту законних інтересів у випадках злиття «у вимірі ЄС» (ст. 21 п. 4). ЗМІ прямо згадуються як такий законний інтерес. До цих пір існує лише один випадок, коли цей принцип був застосований¹⁸⁸. В рамках подальшої регламентації злиття в рамках ЄС у Регламенті № 139/2004 були встановлені додаткові критерії злиття, які повинні бути доведені до Комісії ЄС. На основі цього регламенту Генеральна Дирекція з конкуренції прийняла рішення з приводу великої кількості дій, пов'язаних зі злиттям ЗМІ. Більшість із них були оголошені

186. Council of Europe. (2004). Transnational media concentrations in Europe. Brussels: Council of Europe [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.incd.net/docs/transnationalmedia.pdf>.

187. British Telecommunications, Decision of 10 December 1982 // OJ. – L 360. – 1982. – P. 36.

188. Newspaper Publishing, M.423 (European Commission March 14, 1994).

сумісними з принципами внутрішнього ринку відповідно до ст. 6 п. 1b щодо регламенту про регулювання злиття¹⁸⁹.

Щодо загроз культурному плюралізму і конкуренції в рамках ЄС через розширення великими медіа-компаніями в ЄС своєї діяльності на сусідні держави, то в 2004 р. Європейська комісія визнала, що такої загрози по суті не існує, бо «перебуваючи на різних національних ринках, медіа-компанії не будуть мати на кожному з них домінуючого становища»¹⁹⁰. Але, як наголосив Європарламент, ще на початку 1990-х років «обмеження на концентрацію мають важливе значення в секторі засобів масової інформації не тільки з економічних причин, а й, насамперед, як засіб забезпечення різноманітної інформації і свободи преси»¹⁹¹, плюралізм має бути у центрі уваги, все ж таки не з економічної, а скоріше ідеологічної точки зору.

Додаткове правове регулювання для засобів передачі аудіовізуальних і нових ЗМІ мають ст. 170-172 ДФЄС щодо регулювання транс'європейських мереж в сфері телекомунікацій. Власне їхнім завданням є також реалізація послуг, яка в основному націлена на функціонування eEurope і інформаційного суспільства для всіх. Згідно з цими статтями Європарламент і Рада ЄС можуть ухвалювати акти відповідно до звичайної законодавчої процедури. Так, у 1996 р. було ухвалено рішення Ради №1692/96/ЄС щодо загальних принципів розробки транс'європейських транспортних мереж¹⁹².

Таким чином, вважаємо, що в рамках права ЄС, як особливого правопорядку, існує цілий ряд норм і принципів, присвячених

189. DG Competition. (2009, June 25). Cases by NACE code J. Retrieved June 28, 2009 [Електронний ресурс]. – Режим доступу до ресурсу: http://ec.europa.eu/competition/mergers/cases/index/by_nace_j_.html.

190. Council of Europe. (2004). Transnational media concentrations in Europe. Brussels: Council of Europe [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.incd.net/docs/transnationalmedia.pdf>.

191. The European Parliament «Resolution on Media Take-overs and Mergers» // OJ. – С 68. – 1990. – P. 137–138.

192. Decision № 1692/96/EC of the European Parliament and of the Council of 23 July 1996 on Community guidelines for the development of the trans-European transport network // OJ. – L 228. – 09/09/1996. – P. 1–103.

регулюванню різного роду інформаційних відносин, в тому числі і в Інтернеті. Ці відносини регулюються як в рамках засновницьких договорів, такі і норм вторинного права. Важливу роль відіграють норми міжнародних договорів, укладені за участі ЄС (наприклад Орхуської конвенції про екологічну інформацію (1998 р.)) та рішення Суду ЄС. Важливими для правового регулювання телекомунікацій є різноманітні технічні стандарти Міжнародного союзу електрозв'язку, ЄВТЕЛСАТ тощо. Разом ці норми і принципи утворюють галузь «інформаційне право ЄС».

10. Основні проблеми правового регулювання дифамації в Європі та в Україні[©]

У 2013 році міжнародна неурядова організація «*Index on Censorship*» у своїй щорічній доповіді в черговий раз наголосила на необхідності реформувати застарілу законодавчу базу, яка потенційно є носієм «охолоджуючого ефекту» для свободи слова¹⁹³. Одним з чинників такого негативного впливу на свободу вираження думки є недосконалість правої бази, яка регулює відносини дифамації.

Дифамація — це усне чи письмове висловлення думки, яке негативно позначається на репутації іншої особи. Загальним предметом дифамаційного права є захист права на репутацію. Законодавство про дифамацію зазвичай охоплює всі нормативні акти, що захищають репутацію і почуття громадян. Такі закони оперують широким спектром термінів — наруга над честю, приниження гідності, наклеп, образа тощо. Форма та зміст законодавства про дифамацію мають суттєві відмінності в різних країнах. Деякі держави навіть ухвалили окремі кодекси про дифамацію, хоча в більшості країн положення про дифамацію містяться в загальних законах, наприклад — у кримінальних та цивільних кодексах.

Головними питаннями, що стоять перед законодавцями у сфері дифамації, є: встановлення різниці між наведенням фактів і висловленням поглядів; межі критики публічних осіб; урахування суспільної важливості поширюваних відомостей; встановлення відповідальності за поширення дифамаційних повідомлень.

Відповідні закони повинні запроваджувати ефективний механізм захисту особи від зловмисних звинувачень, які наносять шкоду не

193. Time to step up: The EU and freedom of expression. Report, December 2013 [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.indexoncensorship.org/wp-content/uploads/2013/12/Time-to-Step-Up-The-EU-and-freedom-of-expression.pdf>.

© *Кукіна Зінаїда Олександрівна*, кандидат юридичних наук, асистент кафедри європейського та порівняльного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

тільки моральному, але й фізичному стану індивіда. З іншого боку, в світі снує багато випадків, коли дифамаційне право використовується впливовими особами з метою приховування важливої інформації, яка повинна бути відкритою для населення. Досконале дифамаційне законодавство повинно будуватися на принципі балансу між, з одного боку, захистом свободи

вираження поглядів та здатністю ЗМІ поширювати інформацію, яка містить публічний інтерес, а з другого – правом на захист репутації.

Одним з головних «охолоджувачів» свободи слова є кримінальна відповідальність за поширення дифамації. Журналісти, які знають, що за поширення певної інформації вони можуть бути ув'язнені (що, звичайно, негативно відобразиться на подальшій кар'єрі), будуть стриманіші в поширенні певної інформації. Внаслідок такого тиску на журналістів громадяни можуть позбутися наглядача і стримувача влади в особі представника засобу масової інформації, який робить великий внесок у розкриття неправомірної діяльності держави і її представників. Так, саме завдяки журналістським розслідуванням був розкритий корупційний скандал, пов'язаний з італійським прем'єр-міністром Сільвіо Берлусконі, а також виявлене неправомірне жорстоке поводження американських солдатів з ув'язненими у в'язниці Абу-Грейб тощо.

В Європі рух за відміну кримінальної відповідальності за наклеп почався ще в 2007 році, коли Парламентська Асамблея Ради Європи прийняла резолюцію, присвячену декриміналізації дифамації¹⁹⁴. Раду Європи підтримали і Спеціальний доповідач ООН з питань захисту та поширення права на свободу слова, і Представник ОБСЄ з питань свободи ЗМІ. Спеціальний доповідач ООН відзначив, що «санкції за дифамацію не повинні бути настільки значними, щоб справляти охолоджувальний вплив на свободу слова й вираження переконань та на право шукати, одержувати й поширювати інформацію; карні

194. PACE Resolution 1577 (2007), 'Towards decriminalisation of defamation' [Електронний ресурс]. – Режим доступу: <http://assembly.coe.int/main.asp?Link=/documents/adopt-edtext/ta07/eres1577.htm>.

санкції й, зокрема позбавлення волі, не повинні застосовуватися ніколи»¹⁹⁵. Доповідач також закликав держави скасувати всі закони, що передбачають кримінальну відповідальність за дифамацію, і застосовувати цивільно-правові норми. Європейський Суд з прав людини багаторазово зазначав, що домінантне становище держави робить необхідним «вияв нею витримки в застосуванні кримінального переслідування за дифамацію». Судова практика Європейського суду ще не поставила кримінальне переслідування за дифамацію поза законом, але неодноразово було зазначено, що держава може вдаватися до таких заходів, лише діючи «як гарант громадського порядку» і там, де ці заходи «покликані достатньо, але без надмірності реагувати на безпідставні чи несумлінні дифамаційні звинувачення». На рівні ЄС Група високого рівня Європейської комісії з питань свободи ЗМІ та плюралізму також рекомендувала державам-членам гармонізувати законодавство, яке регулює питання дифамації¹⁹⁶.

Незважаючи на єдність поглядів міжнародної спільноти щодо декриміналізації дифамації, не всі європейські держави втілили розроблені на міжнародному рівні принципи. Майже у всіх державах-членах ЄС досі не скасовані закони, які встановлюють кримінальну відповідальність за наклеп. Тільки Хорватія, Кіпр, Ірландія та Сполучене Королівство внесли відповідні зміни у національне законодавство. 20 з 28 держав-членів ЄС досі використовують ув'язнення як міру покарання за дифамацію. В Словаччині, наприклад, найдовший строк ув'язнення за поширення наклепницької інформації, сягає 8 років, в Італії - 6-ти, в Австрії та Німеччині - 5-ти. При цьому, в Італії навіть за часів Муссоліні максимальним строком ув'язнення за наклеп було три роки. Крім ув'язнення, європейські країни використовують ще й інші застарілі форми покарання. Так, в Голландії та Іспанії звинувачені в дифамації позбавляються політичного

195. Index on Censorship, 'UN rapporteur calls for end to criminal defamation laws' (3 June 2011) [Електронний ресурс]. – Режим доступу: <http://www.indexoncensorship.org/2011/06/un-rapporteur-calls-for-end-to-criminal-defamation-laws/>.

196. 'A free and pluralistic media to sustain European democracy', The Report of the High Level Group on Media Freedom and Pluralism (January 2013) [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/hlg/hlg_final_report.pdf.

права обирати і бути обраними, а в Болгарії ще й займатися певним видом діяльності.

За даними організації *International Press Institute (IPI)*, кримінальна відповідальність не тільки прописана в законах, але й широко застосовується судовими установами європейських держав. Крім того, деякі держави, як наприклад, Хорватія в 2013 р., внесли в законодавство ще й додатковий вид правопорушення дифамаційного характеру - «осуд» (поширення фактів, які можуть нанести шкоду честі та репутації особи перед третьою особою). Минулого року саме за таке правопорушення хорватський суд притягнув до відповідальності журналіста, який поширив інформацію про фінансові проблеми клініки, яка частково фінансується за рахунок державних коштів.

Закони європейських держав недостатньо чітко відображають принцип, розроблений на основі судової практики Європейського суду з прав людини щодо захисту репутації публічних осіб. Так, за загальним правилом межі допустимої критики на адресу публічних осіб ширші, ніж щодо приватних. У справі Лінгенс проти Австрії 1986 р. Європейський суд з прав людини зазначив, що межі допустимої критики стосовно політичного діяча як такого ширші, ніж стосовно приватної особи¹⁹⁷. На відміну від останньої, перший повинен проявляти більшу терпимість до пильної уваги журналістів і всього суспільства, до кожного його слова та дії. Не дивлячись на цей європейський принцип, у Франції, Німеччині, Італії та Португалії покарання за наклеп на публічну особу носить жорсткіший характер, ніж за наклеп на приватну. Крім того, застосовуються спрощені процесуальні процедури, якщо мова йде про публічних осіб. Наприклад, якщо приватна особа повинна особисто подати позов з приводу дифамації, то судовий розгляд щодо наклепу на публічну особу може бути ініційований прокурором.

В деяких країнах встановлюється окрема відповідальність за образу певних високопосадовців. Так, у ряді європейських монархій

197. Case of Lingens v. Austria № 9815/82, 8/07/1986 p.

існують так звані «закопи про образу її величності» (*luse-majestū laws*). Тільки Люксембург та Великобританія скасували таку образу як окремиий вид злочину.

Ще одним недоліком дифамаційного законодавства європейських країн є поширення кримінальної відповідальності на об'єкти — прапор, гімн, герб, державні установи, які не можуть володіти репутацією за своєю природою та, відповідно, не можуть захищатися від дифамації. Звичайно, за наругу над державними символами необхідно встановлювати відповідальність, але вона має бути пропорційною до вини. Але, на думку ІРІ, ув'язнення до 5 років у Німеччини, до 3-х — в Польщі та до 2-х — в Португалії та Бельгії — занадто суворе покарання.

Можна говорити про те, що одним з першочергових завдань урядів європейських країн є скасування кримінальної відповідальності за наклеп та переведення дифамаційних справ у цивільну площину. Якщо ж навіть декриміналізація не буде здійснена повною мірою, то вбачається необхідним звузити коло злочинів, за які настає кримінальна відповідальність, обмежуючись поширенням неправдивої інформації, що веде до вкрай небезпечних наслідків та шкоди. В Європі основна проблема регулювання відносин дифамації та пошуку справедливого балансу між свободою слова та захистом репутації полягає в тому, що існують значні невідповідності між європейськими стандартами, встановленими на рівні ЄС, та національним регулюванням відповідних питань.

Щодо українського законодавства, то на сьогодні воно взагалі не знає терміна «дифамація». Відсутнє чітке регулювання видів відповідальності, розподілу прав та обов'язків відповідача і позивача у справах про наклеп, відсутній детальний перелік підстав звільнення від відповідальності або її пом'якшення в подібних справах, немає існуючих у країнах розвинутих демократій «привілеїв» щодо суб'єктів дифамаційних відносин та ін.

Першою справою, пов'язаною з дифамацією, за якою Україну було

визнано порушницею ст. 10 Європейської конвенції з прав людини, була справа «Українська Прес-група» проти України. Український суд визнав заявника, приватну компанію «Українська Прес-група», винним в опублікуванні під час передвиборної кампанії 1999 р. в газеті «День» статей про кандидатів у президенти — Н. Вітренко та П. Симоненка. У цих статтях містилися описи ділових якостей останніх, зокрема їхньої спроможності виконати заявлені програмні цілі та бути гідними лідерами. Обидва кандидати подали позов до національного суду з метою захисту честі та ділової репутації. Позивачі виграли справу й отримали грошове відшкодування, а також спростування згаданих статей.

Після програшу в національному суді «Українська Прес-група» звернулася до Європейського суду з прав людини із заявою про порушення права журналістів на вільне висловлення поглядів. Заявник наполягав на тому, що національний суд не зміг розрізнити оціночні судження, висловлені в статті, і факти. За твердженням заявника, рішення національного суду містило політичну цензуру щодо вільного поширення інформації про посадових осіб. Визнаючи право на захист ділової репутації пані Вітренко та пана Симоненка, Європейський суд дійшов висновку, що українське законодавство не спромоглося надати належний захист праву на свободу висловлення поглядів. З погляду прецедентної практики Суду, поняття правдивості та неправдивості не можуть застосовуватися до оціночних суджень. Крім того, Суд взяв до уваги стан дотримання свободи слова в Україні за даними численних звітів та рекомендацій.

За законодавством України, що діяло на час вирішення справи, не було розмежування фактів та оціночних суджень, а отже правдивість необхідно було доводити стосовно кожного з цих елементів. Суд постановив, що такі правові норми становлять загрозу належному виконанню ст. 10 Європейської конвенції з прав людини (ЄКПЛ). Було зазначено, що відповідачеві у справах про честь і гідність у національному суді не потрібно було доводити правдивість оціночних суджень, з яких саме й складалася стаття про політиків-позивачів.

Суд наголосив на тому, що, обираючи політичну кар'єру, особа мусить усвідомлювати ступінь своєї публічності та особливої уваги з боку преси і громадськості.

З огляду на загальний контекст справи, Суд дійшов висновку, що покарання заявників за дифамацію вочевидь було непропорційним меті, яку при цьому переслідувала держава, адже не існувало нагальної суспільної потреби, яка переважила б інтерес громадськості в політичному обговоренні передвиборної кампанії в Україні та конкретних її учасників зокрема. До того ж, судові рішення про відповідальність заявників ґрунтувалися на законодавчих положеннях, що були несумісними з принципами ст. 10 ЄКПЛ. Суд зауважив також, що наведені в рішеннях аргументи стосовно відповідальності заявників не були достатніми. Отже, Європейський суд постановив, що мало місце порушення ст. 10 ЄКПЛ¹⁹⁸. Ця справа Європейського суду стала поштовхом для вивчення правової категорії дифамації.

Як уже зазначалося, при поширенні недостовірної інформації стосовно приватного життя публічних осіб вирішення справ про захист їхньої гідності, честі чи ділової репутації має свої особливості. Тут слід враховувати положення Декларації про свободу політичних дебатів у засобах масової інформації (Декларація), схваленої 12 лютого 2004 р. на 872-му засіданні Комітету Міністрів Ради Європи, а також рекомендацій, що містяться в Резолюції 1165 (1998) Парламентської Асамблеї Ради Європи про право на недоторканність приватного життя. Зокрема, у згаданій Резолюції зазначається, що публічними фігурами є особи, які обіймають державні посади і (або) користуються державними ресурсами, а також усі ті, хто відіграє певну роль у суспільному житті (у галузі політики, економіки, мистецтва, соціальної сфері, спорті чи в будь-якій іншій галузі). У ст.ст. 3, 4, 6 Декларації зазначається, що, оскільки політичні діячі та посадові особи, які обіймають публічні посади або здійснюють

198. Price Monroe E., Krug P. The Enabling Environment For Free And Independent Media. Contribution to Transparent and Accountable Governance. – Occasional Papers Series of USAID. – Washington, DC, 2002 [Електронний ресурс] / Monroe E. Price, P. Krug. – Режим доступу: http://www.usaid.gov/our_work/democracy_and_governance/publications/pdfs/pnacm006.pdf.

публічну владу на місцевому, регіональному, національному чи міжнародному рівні, вирішили апелювати до довіри громадськості та погодилися «виставити» себе на публічне політичне обговорювання, вони підлягають ретельному громадському контролю і потенційно можуть зазнати гострої та сильної громадської критики в засобах масової інформації з приводу того, як вони виконували або виконують свої функції. При цьому зазначені діячі та особи не повинні мати більшого захисту своєї репутації та інших прав порівняно з іншими особами.

Важливим для нашої країни на сучасному етапі є наближення до правових систем провідних країн світу, правильне розуміння та запровадження категорій, застосовуваних Європейським судом з прав людини, в українську судову практику, гармонізація понятійного апарату й суті відповідних понять для підвищення рівня захисту честі, гідності, прав та свобод громадян України як на її території, так і за кордоном¹⁹⁹.

Зважаючи на це, доцільним видається:

- ввести в українське законодавство термін «дифамація» і кодифікувати норми про захист честі та гідності особи в єдиний нормативний акт, що мав би назву «Закон про дифамацію», з метою встановлення конкретної межі між захистом репутації і свободою висловлення;
- визначити в єдиному законі термін «дифамація» як правопорушення, що передбачає поширення недостовірних фактичних відомостей про особу, які принижують її честь, гідність та ділову репутацію і є зловживанням свободою висловлення поглядів;
- встановити критерії дифамації, а саме: неправдивість висловлювання; наявність фактичних даних, а не оціночних; завдання шкоди конкретній особі та її репутації;
- розмежувати письмовий і усний наклеп для спрощення встановлення відповідальності;

199. Луць Л. А. Європейські міждержавні правові системи: загальнотеоретична характеристика: дис. д-ра юрид. наук: 12.00.01 / Львівський національний ун-т ім. Івана Франка. – Л., 2004. – С.127.

- обмежити процедуру подання позову з питань дифамації 1 роком від дати оприлюднення, за винятком особливих обставин, а також забезпечити достатньо розумні строки виконання кожного етапу провадження з питань дифамації з тим, щоб обмежити негативний вплив затримки на свободу висловлення поглядів;
- встановити відповідальність залежно від характеру наклепу та особи, про яку було поширено недостовірну інформацію;
- виділити публічних осіб в окрему категорію зі звуженням їхнього права на порушення справ, пов'язаних із дифамацією;
- надати переваги наявним нематеріальним правовим засобам компенсації будь-якої шкоди репутації, завданої дифамацією, до яких належать: публікація, вибачення, виправлення та (або) відповідь, публікація судового рішення, яким висловлювання визнаються дифамацією;
- присуджувати матеріальну компенсацію лише у випадках, коли нематеріальні правові засоби виявляються недостатніми для компенсації шкоди репутації, завданої дифамацією (матеріальна компенсація завжди має бути пропорційною завданій шкоді; компенсація за фактичні фінансові збитки або матеріальну шкоду, спричинену дифамацією, має присуджуватися тільки у разі точного встановлення обсягу цих збитків);
- встановити найвищу межу рівня нематеріальної компенсації шкоди, завданої репутації (такий найвищий рівень компенсації має застосовуватися тільки в найбільш серйозних справах);
- скасувати судову заборону як запобіжний засіб під час провадження у справі з питань дифамації з метою запобігання обмеженню свободи висловлення поглядів;
- встановити, що накладання постійної заборони має здійснюватись у формі судової постанови й після повного завершення справедливого судового розгляду по суті справи;
- надавати відповідачам ефективні засоби захисту у випадках, коли позивач порушує явно необґрунтовану справу з метою стримування свободи висловлення поглядів, а не з метою захисту своєї репутації.

Таким чином, можна говорити про те, що законодавче регулювання інституту дифамації є недосконалим як в європейських державах, так і в Україні. Але якщо в Європі основною проблемою є усунення певних недоліків з існуючої розвиненої законодавчої бази, то в Україні така база практично відсутня. Багатьох категорій дифамаційного права, великою мірою розвинутого за кордоном, ще немає в українському законодавстві або вони представлені окремими нормами, які не можуть ефективно регулювати відповідні відносини.

Спільною проблемою як для Європи, так і для України є декриміналізація відповідальності за здійснення наклепу. Прийнятий на загальноєвропейському рівні принцип скасування кримінальної відповідальності за дифамаційні правопорушення вже починає діяти на практиці (в основному в національних судах держав-членів ЄС), але ще не втілений в писаному законодавстві. В Україні була небезпека введення кримінальної відповідальності за наклеп, коли в 2012 році в Верховній Раді був зареєстрований Проект Закону «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України щодо посилення відповідальності за посягання на честь, гідність та ділову репутацію людини» № 11013. Позитивним моментом є те, що проект так і залишився проектом. Негативним явищем залишається відсутність необхідних законодавчих ініціатив щодо розробки та прийняття ефективної законодавчої бази для регулювання відносин, які складаються з приводу дифамації.

ПІДРОЗДІЛ 3.3.

ПРАВА ЛЮДИНИ В ІНТЕРНЕТІ

11. **Захист прав людини он-лайн як пріоритетне завдання Ради Європи**[©]

Рада Європи постійно приділяє увагу захисту прав людини в он-лайн середовищі та наголошує, що стандарти і цінності Ради Європи застосовуються як до офлайн, так і до он-лайн середовища. Ця теза неодноразово повторювалась в різних контекстах в інших рекомендаціях і декларація Комітету Міністрів і резолюціях Парламентської Асамблеї Ради Європи.

Питанням гарантування свободи слова в Інтернеті приділяється увага кожного разу, адже ця свобода забезпечила розвиток Інтернету та його поширення по всьому світу як комунікаційного засобу.

В Декларації про свободу комунікацій в Інтернеті від 28 травня 2003 року²⁰⁰, Комітет Міністрів застеріг держави від здійснення попереднього контролю контенту, розміщеного в Інтернеті, за допомогою загальних заходів з фільтрації та блокування. Заклик дотримуватися умов статті 10 (2) Європейської конвенції про захист прав людини та основоположних свобод, зокрема вживати заходи на основі прийняття попереднього або остаточного рішення про незаконність чітко визначеного контенту компетентними національними органами з дотриманням критерію пропорційності

200. Декларації про свободу спілкування в Інтернеті, Страсбург, 28.05.2003 (затверджена Комітетом Міністрів на 840-му засіданні заступників міністрів). – [Електронний ресурс]. – Режим доступу: http://www.medialaw.kiev.ua/laws/laws_international/77/

© *Пазюк Андрій Валерійович*, кандидат юридичних наук, керівник лабораторії з управління Інтернетом Української Асоціації міжнародного права, член Експертної ради Комітету Верховної Ради України з питань інформатизації та інформаційних технологій

впливає також з практичного тлумачення цих положень Конвенції Європейським Судом з прав людини. Єдиним прийнятним винятком із загальної заборони попередньої цензури в Інтернеті є встановлення фільтрів для захисту неповнолітніх, зокрема, в місцях, доступних для них, таких як школи або бібліотеки.

У подальшому вимога щодо попередження державної і приватної цензури була зазначена в *Декларації про права людини і верховенство права в інформаційному суспільстві*²⁰¹ від 13 травня 2005 року. А *Рекомендація про заходи з пропагування поваги свободи слова та інформації з огляду на інтернет-фільтри*²⁰² включає в себе керівні принципи використання та управління інтернет-фільтрами в цілому і, зокрема, у сфері захисту дітей та молоді.

*Рекомендація Комітету Міністрів державам-членам про заходи щодо пропагування суспільної цінності Інтернету*²⁰³ підкреслює значну залежність людей від Інтернету як найважливішого інструменту у їх повсякденній діяльності (комунікації, отриманні інформації, знань, здійсненні комерційних операцій) і зумовленого цим закономірного очікування, що інтернет-послуги будуть доступними і недорогими, безпечними, надійними і відмово-стійкими. Позиція Ради Європи та держав-членів є принциповою, адже для забезпечення повної участі людей у соціальній та економічній діяльності в Інтернеті та для ефективної реалізації демократичної громадянської відповідальності, держави зобов'язані забезпечити всі права та основоположні свободи людини в онлайн-середовищі, включно з правом на повагу до приватного життя, правом на свободу віросповідання, заборонаю дискримінації, захистом людської гідності, правом на свободу зборів

201. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society CM(2005)56 final, 13 May 2005. – [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?id=849061>

202. Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282008%296&Language=lanEnglish&Ver=original>

203. Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet (Adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers' Deputies) [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?id=1207291>

та об'єднань, правом на захист власності, правом на освіту та забезпечення відкритості і безпеки в Інтернеті.

29 вересня 2010 року Рада Європи ухвалила одночасно три визначальні для розвитку правової платформи інформаційного суспільства документи: *Декларацію про Цифровий порядок денний для Європи*, *Декларацію про мережеву нейтральність* та *Декларацію про управління ресурсами IP-адрес в інтересах суспільства*, про які йдеться далі.

Комітет Міністрів Ради Європи не залишив поза увагою політичні пріоритети у сфері розвитку інформаційного суспільства, що були проголошені міністрами, відповідальними за політику інформаційного суспільства держав-членів Європейського Союзу та Європейської економічної зони, у Гранадській міністерській декларації про цифровий порядок денний для Європи (*Гранадська міністерська декларація*)²⁰⁴ та, згодом, Європейською комісією в рамках повідомлення *Цифровий порядок денний для Європи*²⁰⁵. Серед яких, напрямки діяльності для підвищення економічної активності та забезпечення економічних та соціальних переваг для європейських громадян в онлайн-середовищі.⁵

Прийнявши *Декларацію про Цифровий порядок денний для Європи*²⁰⁶, Комітет Міністрів Ради Європи підтвердив та підтримав відповідні цілі політики Європейського Союзу, що пропагують суспільну цінність Інтернету, встановлюють важливі орієнтири для його доступності для всіх громадян і також вирішують проблеми зміцнення цифрової економіки на благо як громадян, так і бізнесу, торуючи шлях для створення єдиного ринку для інтернет-контенту та продукції в державах-членах Європейського Союзу.

Гранадська міністерська декларація та Цифровий порядок денний

204. The Granada Ministerial Declaration on the European Digital Agenda was agreed on the occasion of the Informal Ministerial Meeting in Granada, Spain, 18 and 19 April 2010.

205. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions: "A Digital Agenda for Europe", COM(2010)245.

206. Declaration of the Committee of Ministers on the Digital Agenda for Europe (Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies). – [Електронний ресурс]. – Режим доступу: https://wcd.coe.int/ViewDoc.jsp?id=1678251#P21_2774

для Європи підтримують науково-дослідні та інноваційні стратегії ІКТ, що мають суспільну цінність у вирішенні проблем освіти, навколишнього середовища, енергетики, охорони здоров'я і демографічних проблем. Наріжним каменем політики ЄС стосовно Інтернету є орієнтир на користувачів Інтернету, як активних учасників і компетентних партнерів у розвитку цифрового суспільства, та їх потреби щодо розширення спроможності повною мірою використовувати економічні, соціальні і культурні можливості та переваги, пропоновані в Інтернеті та ІКТ.

Гранадська міністерська декларація та Цифровий порядок денний для Європи мають за мету сприяти створенню, виробництву і розповсюдженню творчого контенту, в тому числі культурно-публіцистичного характеру в онлайн-середовищі. В цьому відношенні, вони сигналізують, зокрема, про необхідність прийняття бізнес-моделей, пов'язаних з інтелектуальною власністю. Крім того, вони підтверджують актуальність державної політики в області оцифрування і розповсюдження європейської культурної спадщини з метою пропагування базових цінностей плюралізму і культурного та мовного розмаїття.

Низка документів Ради Європи, що стосуються захисту і реалізації прав та основоположних свобод в Інтернеті, поділяють бачення й цілі напрямків діяльності вищезгаданої Гранадської декларації та Цифрового порядку денного для Європи. Спільність цілей, що переслідують Рада Європи та Європейський Союз у питаннях державної політики відносно управління Інтернетом, також підкреслюється в рамках загальноєвропейського діалогу з питань управління Інтернетом (EuroDIG), який рішуче підтримує Рада Європи.

Приймаючи *Декларацію про мережеву нейтральність*²⁰⁷, Комітет міністрів Ради Європи виходив з пріоритетності прав людини над

207. Declaration of the Committee of Ministers on network neutrality (Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies) – [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?id=1678287>

комерційними інтересами ІКТ-індустрії. Вільний обмін ідеями та інформацією, що в сучасному суспільстві забезпечується електронними комунікаціями, вимагає створення необхідних ринкових умов. Конкурентоспроможне середовище, в якому заохочуються інновації, забезпечується доступність та продуктивність мережі і зниження витрат, - все це сприяє вільній циркуляції широкого кола послуг і контенту в Інтернеті. Натомість, практика обмеження контенту і послуг або ускладнення в підключенні пристроїв, що здійснюється під час адміністрування трафіку в мережах, може негативно впливати на право користувачів на доступ і поширення інформації в Інтернеті, гальмуватиме розробку та впровадження нових інструментів і послуг.

З огляду на вищезазначене, у Декларації наголошується, що користувачі повинні мати максимально повний можливий доступ до інтернет-контенту, програм та послуг за власним вибором, незалежно від того, чи вони пропонуються безкоштовно, або платно, використовуючи відповідні пристрої за своїм вибором — отже, на недискримінаційній основі. Зазначений принцип, що отримав назву «мережева нейтральність» (*network neutrality*), визнається стрижневим для розвитку інфраструктури і доступу до неї користувачів і постачальників послуг, контенту або програм.

Разом з тим, адміністрування трафіку, що є технічно необхідним для надання послуг з його передачі, не виключає можливість застосування певних обмежувальних заходів. У Декларації наголошується на необхідності оцінювання таких заходів на відповідність критеріям пропорційності, доречності і періодичного перегляду, аби уникати невиправданої дискримінації. Крім того, повинні бути впровадженні механізми інформування користувачів і постачальників послуг про будь-які заходи управління мережею, які впливають значним чином на доступ до контенту, програм або послуг. Зазначається про необхідність процедурних гарантій, з врахуванням вимог закону, для оскарження рішень мережевого управління і, при необхідності, для стягнення відшкодування.

Третя із Декларацій, ухвалених Комітетом Міністрів Ради Європи 29 вересня 2010 року, присвячується питанням *управління ресурсами ІР-адрес* ²⁰⁸. Знову посилаючись на застосування основних прав, а також стандартів й цінностей Ради Європи в онлайн-середовищах, і, зокрема, в Інтернеті, так само, як в реальному світі (без розрізнення он-лайн /офлайн), Комітет міністрів закликав держави-члени, у співпраці з відповідними зацікавленими сторонами (приватним сектором та громадянським суспільством), пропагувати суспільну цінність Інтернету. Цей поклик виходить з розуміння, що громадяни у значній мірі покладаються на Інтернет, що є найважливішим інструментом у повсякденній діяльності, та закономірно очікують в результаті, що інтернет-послуги будуть доступними і недорогими, безпечними, надійними і безперервними. Держави-країни повинні, зокрема, заохочувати приватний сектор зробити внесок у пропагування суспільної цінності Інтернету для всіх, і розробити державну політику для доповнення ринкових сил там, де їх недостатньо. Йдеться про ІР-адреси, що використовуються в системі доменних імен (DNS), та є важливими для функціонування Інтернету.

Серед потенційних ризиків для права на повагу до приватного життя (*respect for private life*), гарантованого статтею 8 Європейської Конвенції про захист прав людини та основоположних свобод, а також права на справедливе поводження з персональними даними (*personal data protection*), закріпленого в Конвенції Ради Європи про захист особи у зв'язку з автоматичною обробкою персональних даних (ETS № 108), у Декларації наводяться приклади використання ідентифікаційних ознаки, які входять до ІР-адреси пристроїв, що використовуються для підключення до Інтернету, і надають можливість профілювання діяльності користувачів і комунікацій. Наявна можливість зловживань або необґрунтованого стеження за даними трафіку, генерованого в результаті використання мобільних пристроїв та інших приладів, підключених через інтернет-протоколи.

208. Declaration of the Committee of Ministers on the management of the Internet protocol address resources in the public interest (Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies) – [Електронний ресурс]. – Режим доступу: https://wcd.coe.int/ViewDoc.jsp?id=1678299#P10_731

А отже інформація про діяльність і зв'язки користувачів, а також дані трафіку, є персональними даними, з якими слід поводитися у відповідності з стандартами Ради Європи.

Рада Європи знову звернула увагу на специфічні проблеми, пов'язані із захистом прав людини та адмініструванням системи доменних імен у 2011 році. *Декларація Комітету Міністрів про захист свободи слова та інформації і свободи зібрань та об'єднань стосовно доменних імен та доменних стрінгів в Інтернеті*²⁰⁹, прийнята Комітетом Міністрів 21 вересня 2011 року посилається на резолюцію про управління Інтернетом та критичними ресурсами мережі Інтернет, прийнятту міністрами держав, що беруть участь в першій конференції міністрів Ради Європи, відповідальних за ЗМІ і нові комунікаційні послуги, що відбулася в Рейк'явіку 28 і 29 травня 2009 року та запрошує компетентні органи Ради Європи до взаємодії з відповідними корпораціями, установами та іншими організаціями, які управляють або роблять внесок в управління простором доменних імен, з метою належного врахування у рішеннях вимог міжнародного права, включаючи міжнародне право захисту прав людини. Комітет Міністрів висловив підтримку визнання державами-членами необхідності застосування фундаментальних гарантій прав на управління доменними іменами; попередив про ризик надмірного регулювання простору доменних імен та строк доменних імен для реалізації свободи вираження думок і права на отримання та поширення інформації та свободи зібрань і об'єднань, як форми втручання, наголосивши, що будь-яке регулювання має відповідати умовам статей 10 і 11 Європейської конвенції про захист прав людини і відповідного прецедентного права Європейського суду з прав людини.

З огляду на те, що нова медійна екосистема заснована на приватноправових відносинах, учасниками яких виступають користувачі

209. Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings (Adopted by the Committee of Ministers on 21 September 2011). – [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?id=1835805&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>

(споживачі) інформаційних і комунікаційних послуг та постачальники цих послуг, Комітет Міністрів Ради Європи не міг оминати своєю увагою питання захисту свободи вираження думок і свободу зібрань у цій сфері. *Декларація про захист свободи вираження думок і свободу зібрань та об'єднань у сфері приватних інтернет-платформ та інтернет-провайдерів*²¹⁰, прийнята Комітетом Міністрів 7 грудня 2011 року, наголошує на важливості приватних платформ, які перебуваючи в приватному управлінні, становлять значну частину публічної сфери, оскільки сприяють дискусіям з питань, що викликають суспільний інтерес; в деяких випадках, вони можуть виконувати, аналогічно традиційним ЗМІ, роль соціального «сторожового пса», і продемонстрували свою корисність для позитивних змін в реальному житті. Представники громадянського суспільства, правдошукачі та правозахисники, все більше покладаються на соціальні мережі, блоги, веб-сайти та інші засоби масової комунікації в цілому, для отримання та обміну інформацією, публікації контенту, взаємодії, спілкування та об'єднання один з одним. Зважаючи на зазначене, Комітет Міністрів застеріг держави-члени від вчинення політично мотивованого тиску на приватні інтернет-платформи та інтернет-провайдерів, атак на сайти незалежних ЗМІ, правозахисників, дисидентів, правдошукачів і нових суб'єктів ЗМІ.

У квітні 2012 року Комітет Міністрів зважив на загрози правам людини, що можуть спричинитися в соціальних мережах. *Рекомендація про захист прав людини у сфері соціальних мережесвих сервісів*²¹¹ визнає, що соціальні мережі є рушійними силами прав людини та каталізаторами демократії. Однак право на приватність та повагу до людської гідності можуть також опинитись під загрозою в соціальних

210. Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers (Adopted by the Committee of Ministers on 7 December 2011 at the 1129th meeting of the Ministers' Deputies). – [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?id=1883671>

211. Рекомендація CM/Rec(2012)4 Комітету міністрів державам-членам про захист прав людини у сфері соціальних мережесвих сервісів, прийнята Комітетом міністрів 4 квітня 2012 року на 1139-му засіданні заступників міністрів. – [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>

мережах, які практикують дискримінацію. Загрози виникають через відсутність правових та процедурних заходів безпеки, недостатній захист дітей та молоді від шкідливого контенту або поведінки; відсутність поваги до прав інших людей, відсутність налаштувань конфіденційності за замовчуванням для користувачів; відсутність прозорості цілей, для яких збираються і обробляються особисті дані.

Звертаючись до держав-членів, Комітет міністрів наголошує на необхідності: співробітництва з приватним сектором, вироблення підходів саморегулювання і спільного регулювання поведінки та стандартів для використання соціальних мереж; розвитку і просування послідовних стратегій стосовно захисту і заохоченню поваги прав людини в сфері соціальних мереж, відповідно до положень Конвенції про захист прав людини та основоположних свобод (зокрема, до статті 8 (право на повагу до приватного і сімейного життя), статті 10 (свобода вираження думок) і статті 11 (свобода зборів і об'єднань)) і Конвенції про захист стосовно автоматизованої обробки персональних даних (ETS № 108).

Серед завдань, до яких повинні залучатися провайдери соціальних мереж у партнерстві з урядами та громадянським суспільством, значаться такі:

- забезпечити середовище для користувачів соціальних мереж, що дозволить їм надалі реалізовувати свої права і свободи;
- підвищити обізнаність користувачів, за допомогою чіткої і зрозумілої мови, про можливі проблеми стосовно прав людини і способів уникнути негативного впливу на права інших людей при використанні цих послуг;
- захищати користувачів від шкоди, не обмежуючи свободу слова і доступ до інформації;
- підвищувати прозорість обробки даних, і утримуватися від незаконної обробки персональних даних;
- впроваджувати механізми самоперевірки і спільного регулювання в разі необхідності, для сприяння цілям, викладених в додатку до цієї рекомендації;

- забезпечувати доступ до їх послуг для людей з обмеженими можливостями, підсилюючи таким чином їх інтеграцію та повноцінну участь в житті суспільства.

Підсумковим документом, прийнятим Радою Європи за результатами узагальнення накопиченого досвіду захисту прав людини он-лайн в державах-членах, тлумачення цих прав і свобод у практиці Європейського суду з прав людини і відповідних правових інструментах Ради Європи, стали *Керівні принципи з прав людини для користувачів Інтернету* (далі – «*Керівні принципи*»), ухвалені 16 квітня 2014 року у формі Рекомендації Комітету Міністрів державам-членам²¹².

Рада Європи поширила всі існуючі в неї інструменти захист прав людини на сферу користування Інтернетом. Не обмежившись лише Конвенцією про захист прав людини та основоположних свобод, у цій сфері діятимуть інші конвенції та інструменти Ради Європи, якими передбачається захист права на свободу слова, доступ до інформації²¹³, право на свободу зібрань, захист від кіберзлочинності²¹⁴, право на приватне життя та захист персональних даних²¹⁵.

Рекомендація пропонує державам-членам наступне:

- активно поширювати *Керівні принципи* серед громадян, державних органів, суб'єктів приватного сектору та здійснювати конкретні заходи, спрямовані на їх застосування, з метою забезпечення реалізації користувачами в повному обсязі своїх прав і основоположних свобод у мережі;

212. Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо «Керівних принципів з прав людини для Інтернет-користувачів», ухвалена Комітетом міністрів 16 квітня 2014 року на 1197 засіданні заступників міністрів. – [Електронний ресурс]. – Режим доступу: <https://wcd.coe.int/ViewDoc.jsp?id=2184807&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>

213. Конвенція про доступ до офіційних документів, м. Тромс, 18 дня червня 2009 року – [Електронний ресурс]. – Режим доступу: http://crimecor.rada.gov.ua/komzloch/control/uk/publish/article;jsessionid=C75D14A4396DDB62F4F196E8FD76B58E?art_id=49046&cat_id=46352

214. Конвенція про кіберзлочинність, м. Будапешт, 23 листопада 2001 року, ETS No. 185. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575

215. Конвенція про захист осіб стосовно автоматизованої обробки персональних даних, Страсбург, 28 січня 1981 року, ETS No. 108. -- [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_326

- оцінювати, періодично переглядати та усувати в установленому порядку обмеження стосовно реалізації прав та свобод в Інтернеті, зокрема у тих випадках, коли вони не відповідають вимогам Конвенції у світлі відповідної практики Європейського суду з прав людини. Будь-яке обмеження повинне бути передбачене законом, бути необхідним у демократичному суспільстві для переслідування законної мети і пропорційним переслідуваній меті;
- забезпечувати доступ користувачів Інтернету до ефективних механізмів правового захисту у разі обмеження їхніх прав і свобод або в тому разі, коли вони вважають, що їхні права були порушені. Це вимагає поглиблення координації та співпраці між відповідними установами, структурами та спільнотами. Це також створює необхідність у залученні та ефективній співпраці з суб'єктами приватного сектору та організаціями громадянського суспільства. Залежно від національного контексту, цей пункт може передбачати механізми відшкодування, подібні до тих, що забезпечуються органами, відповідальними за захист даних, національними правозахисними органами (наприклад, омбудсманами), судові процедури, гарячі лінії;
- сприяти координації з іншими державними і недержавними структурами в межах Ради Європи та поза її межами у сфері стандартів і процедур, які мають вплив на захист прав людини і основоположних свобод в Інтернеті; заохочувати приватний сектор до повноцінного діалогу з відповідними державними органами і громадянським суспільством з метою забезпечення їх відповідальності перед суспільством за свою діяльність і зокрема, прозорості та підзвітності згідно з вимогами документу «Керівні принципи у сфері підприємницької діяльності та прав людини: реалізація курсу ООН на «захист, повагу, забезпечення механізмів правового захисту». Приватний сектор потрібно заохочувати до участі в поширенні *Керівних принципів*;
- заохочувати громадянське суспільство до підтримки поширення і застосування довідника, який має стати ефективним інструментом для користувачів Інтернету.

Керівні принципи не запроваджують нових прав людини і основоположних свободи, натомість спрямовані на захист і забезпечення існуючих прав людини в он-лайнному середовищі. У документі структурно виділені підрозділи, що відображають ті чи інші сфери практичного застосування прав людини в Інтернеті:

- доступ і недискримінація;
- свобода вираження думок та інформації;
- зібрання, об'єднання та участь;
- приватне життя та захист даних;
- освіта та грамотність;
- діти та молодь;
- ефективні механізми правового захисту.

Ключове місце в Керівних принципах відведено забезпеченню правового захисту у разі обмеження або порушення прав у сфері користування Інтернетом. Насамперед, такі засоби мають бути відомими, доступними, поміркованими з точки зору витрат і такими, що реально забезпечать відповідне відновлення обмежених або порушених прав. Ефективні механізми захисту можна отримати безпосередньо від провайдерів Інтернет послуг, державних органів та (або) національних правозахисних структур. Залежно від порушення, ефективні механізми правового захисту можуть передбачати надання довідки, роз'яснення, відповіді, виправлення, вибачення, поновлення в правах, повторного підключення та компенсацію.

Отже, Україна має розробити та впровадити національні механізми реалізації прав і свобод користувачів Інтернету, зробити їх доступними для загалу, а правові інструменти захисту порушених прав — зрозумілими і ефективними. Свою роль в цьому процесі, окрім органів державної влади, мають відігравати громадянське суспільство та приватний сектор, зокрема, інтернет-індустрія.

12. Розвиток правового регулювання суспільних відносин у сфері використання Інтернету в Європейському Союзі[©]

Представляється доцільним дослідити правове регулювання суспільних відносин у сфері використання Інтернету в ЄС не тільки як приклад успішного правового регулювання інформаційних відносин на регіональному рівні, але й з огляду на підписання Угоди про асоціацію між Україною та ЄС. Подальша інтеграція України до Євросоюзу вимагатиме вдосконалення правових засад, включаючи засади правового регулювання Інтернету, які мають забезпечити реалізацію Україною своїх міжнародно-правових зобов'язань щодо співробітництва з ЄС: «Це дозволить створити дієвий національний механізм імплементації норм міжнародного права, який приведе Україну до досягнення її стратегічної мети – інтеграції у Євросоюз»²¹⁶.

Інтернет є найважливішим елементом інформаційної інфраструктури світового співтовариства. Але Європейське Співтовариство і США по-різному бачать перспективи розвитку системи правового регулювання суспільних відносин в Інтернеті: в Америці приділено увагу інфраструктурі – «інформаційній супермагістралі», а в Європі основна увага приділяється соціальній стороні розвитку інформаційно-комунікаційних технологій, включаючи Інтернет. Нормативні акти і рекомендаційні норми ЄС, присвячені різним аспектам становлення європейського сегмента інформаційного суспільства, мають на меті сприяння формуванню національної політики в цій галузі, причому це завдання сприймається як імператив, невиконання якого потягне втрату конкурентоздатності всієї країни, зниження рівня життя, втрату темпів розвитку та позицій в економіці й торгівлі.

216. Висновок Комітету ВР на проект Закону про Загальнодержавну програму «Електронна Україна на 2005-2012 роки» [Електронний ресурс]. – Режим доступу: www.rada.gov.ua.

Європа звертає особливу увагу на правове регулювання Інтернету і визнає його новим і одним з найважливіших соціальних, політичних та економічних факторів сучасного світу. Розробка концепцій і наступних програм їх реалізації супроводжується загальною демократизацією європейського ринку телекомунікацій. Мережа Інтернет в цих документах привертає значну увагу, оскільки конвергенція технологій та індустрій (телекомунікаційних, комп'ютерної, телевізійної, ЗМІ) найбільш очевидно виражається саме в цих нововведеннях, а тому й ставить нові завдання перед національними урядовими органами, що регулюють інформаційну сферу.

Інтернет визнаний одним з наріжних каменів глобальної інформаційної інфраструктури і найважливішим елементом інформаційного суспільства в Європі. Значне місце в офіційних документах ЄС приділяється правовим проблемам, пов'язаним з діяльністю громадськості в мережі Інтернет. Ці проблеми включають:

- регулювання змісту ресурсів (шкідливий і незаконний зміст) в Інтернеті;
- дотримання авторських і суміжних прав в умовах технічно легкого копіювання будь-якої інформації, що представлена в цифровому вигляді;
- питання формування «кібереконіміки» (електронні гроші, оподаткування, електронні контракти, реклама, маркетинг, електронні публікації);
- інформаційна безпека (безпека життєво важливих для суспільства систем керування, яке можна здійснювати і за допомогою комп'ютерних технологій).

Національне регулювання суспільних відносин у сфері Інтернету в державах — членах ЄС розпочалося в 90-х роках. Тоді робилися спроби створити правовий базис для регулювання діяльності учасників інтернет-ринку в країнах Європи на внутрішньодержавному рівні. Особлива увага приділялася необхідності саморегулювання інтернет-індустрії.

У Франції після приватизації державного оператора *France Telecom* намітилося стрімке зростання мережі. Це змусило уряд контролювати зазначений сегмент ринку, і спроби ввести жорстку політику регламентації доступу громадян до певних видів інформації були неефективні.

У Нідерландах проводиться політика залучення користувачів до виявлення нелегального контенту, зокрема дитячої порнографії. Існує в Нідерландах своя Асоціація інтернет-провайдерів – NLIP. Вона ініціювала впровадження «гарячих ліній» щодо дитячої порнографії, расизму та іншого образливого контенту.

У Великобританії до Інтернету застосовується законодавство у галузі ЗМІ. Крім того, існує кілька законодавчих актів, що безпосередньо регулюють Інтернет, зокрема про захист інформації в електронному вигляді, про відповідальність перед законом за наклепи, про покарання за сексуальну образу в мережі Інтернет, в яких чітко визначена межа між незаконною інформацією (дитяча порнографія, наклепи, шахрайство) та небажаною інформацією (расизм, екстремізм, антисемітизм, релігійні розбрати, пропаганда наркотиків). У 1996 р. створено фундацію нагляду за Інтернетом, мета якої попереджати та запобігати поширенню протиправної інформації в Інтернеті.

В Італії законодавство у сфері Інтернету обмежується лише кількома додатками до існуючих законів, норми в яких сформульовані загально. Впровадження нових законів здійснюється повільно і лише під тиском ЄС.

Розробка законодавства в галузі Інтернету на рівні ЄС. Одну з перших спроб правового регулювання сфери комп'ютерних технологій у Європейському Співтоваристві було здійснено в 1991 році, коли розроблявся проект «Директиви про приватність», яка була прийнята Радою Міністрів ЄС у 1995 як Директива про захист персональних даних (*Directive on the Protection of Personal Data*)²¹⁷. Директива

217. Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data // Official Journal of the European Communities, L 281. – 1995. - P. 31.

обмежувала збирання даних лише для визначених і легітимних цілей і надавала індивідам право доступу до їх особистих записів. На додаток визначалося потенційне зловживання при передачі інформації через національні кордони, у тому числі і в Інтернеті. Директива мала запобігти порушенням права ЄС з боку країн, що не входили до ЄС.

З 1991 року ЄС здійснив значний прогрес у правовому регулюванні Інтернету, хоча спеціальне законодавство ще не встигло сформуватися. 19 липня 1994 р. Європейська комісія прийняла документ під назвою «Шлях Європи до інформаційного суспільства: план дій»²¹⁸. У документі зазначалась регулятивна роль ЄС, а приватний сектор не заохочувався до саморегулювання в галузі інформаційних технологій. Комісія запропонувала «широку регулятивну рамкову програму», яка стосувалася доступу до відповідного ринку, сумісності мереж, права інтелектуальної власності й захисту даних. Комісія зазначала в документі, що головною метою регулювання ЄС у галузі Інтернету стане створення «галузі відповідного рівня».

У вересні 1996 року Європейська Комісія (ЄК) і Європарламент опублікували Документ щодо основних напрямків політики із впливу інформаційних технологій на формування політики ЄС²¹⁹, у якому зазначалось, що ЄК зацікавлена у підвищенні ефективності загального законодавства різних галузей права з тим, щоб створити структуроване й об'єктивне середовище. ЄК висловила занепокоєність з приводу того, що за відсутності такого регулювання Інтернет розвинеться в середовище, в якому прогалини в праві швидко отримують негативні наслідки. У документі було зазначено, що «без відповідної регулятивної політики на рівні Спільнот і національної та регіональної політики позитивні аспекти інформаційного суспільства можуть бути втрачені, беручи до уваги ризик того, що некваліфіковані чи недостатньо кваліфіковані особи, мігранти, люди похилого віку, люди з обмеженими можливостями, мешканці периферійних районів будуть ізольовані від доступу до інформаційних

218. Action Plan: Europe's Way to the Information Society: (COM (94) 347 final) [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.echo.lu/eudocs/en/com-asc.html>.

219. EU: The Implications of the Information Society for EU Policies, Policy Paper – 24 July 1996 [Електронний ресурс]. – Режим доступу до ресурсу: <http://europa.eu.int/idabc/en/document/3624/375>.

технологій». Саме тому Документ закликав до розбудови «суворої регулятивної рамкової структури» для досягнення «максимального суспільного захисту».

У документі також визначалась необхідність проведення досліджень щодо встановлення податку ЄС на інтернет-трафік. На підтвердження позиції ЄС щодо суворого регулювання Інтернету в Документі зазначено, що слід приділити окрему увагу необхідності відповідного і вчасного створення регулятивної і законодавчої системи для інформаційного суспільства, що постійно розвивається. Інформаційне суспільство має регулюватися на наднаціональному рівні. В Документі також наголошувалась потреба в міжнародному регулятивному режимі, без зазначення про саморегулювання цієї галузі.

Саме в Європі вперше було зазначено необхідність у міжнародно-правовому регулюванні мережі Інтернет. В Резолюції Європейського Парламенту 1996 року підтверджено принцип сприяння міжнародній координації правового регулювання Інтернету урядами країн - членів ЄС. Було запропоновано визначити спільні умови для координування національного правового регулювання для запобігання фрагментації законодавства у сфері Інтернету. В листопаді 1996 року в оцінці Зеленої книги Європейської Комісії Комітет з економічних і соціальних питань зазначив, що розвиток Інтернету вимагатиме від держав-членів координувати їх регулятивні рамкові системи²²⁰. А вже пізніше ЄС закликав до високого рівня внутрішньодержавного регулювання Інтернету²²¹. В документі «Європейська ініціатива щодо електронної комерції» визначалися плани щодо регулювання всіх аспектів електронної комерції. Там зазначалося, що регулятивна структура «спільного ринку» була опрацьована для інших форм бізнесу, отже «зараз вона має працювати для електронної комерції». Комісія попереджала, що без новітнього законодавства Інтернет не працюватиме в галузі комерції, оскільки не матиме довіри і впевненості споживачів і бізнесменів. Крім

220. Див. Оцінку Економічного і соціального комітету із «Зеленої книги Комісії щодо комерційних комунікацій на Внутрішньому ринку».

221. European Union Considers Regulatory Framework For Electronic Commerce [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.iwar.org.uk/e-commerce/resources/eu/src/ecomcom3.htm>.

того, Комісія відмітила, що в регулюванні Інтернету на рівні ЄС існує потреба, оскільки необхідно запобігти фрагментації європейського внутрішнього ринку. В документі також зазначалося, що Спільний ринок повинен розбудовуватись на основі законодавства і політики в галузі Інтернету, які вже були підготовлені в Співтоваристві²²².

Розвиток системи саморегулювання суспільних відносин у сфері використання Інтернету в ЄС. До 1997 року регулятивна політика ЄС у галузі Інтернету базувалась на принципі виключного урядового регулювання з метою захисту суспільства і створення неупередженого правового середовища для існування Інтернету. Разом з цим, ЄС проголосив необхідність міжнародної співпраці і гармонізації правового регулювання Інтернету на світовому рівні.

Однак, поступово в політиці регулювання Інтернету намітилися зміни: у вересні 1997 року ЄС здійснив заходи з розвитку саморегулювання цієї галузі – було створено Європейську асоціацію інтернет-провайдерів (*EuroISPA*), яка представляла інтереси близько 400 провайдерів в ЄС. При цьому, ЄС частково здійснював фінансування і заохочував спроби Асоціації розробити політику по саморегулюванню галузі.

У 1997 році член Комісії ЄС у справах телекомунікацій М. Бангеман визначив напрямок правового регулювання Інтернету таким чином: «саморегулювання цієї галузі промисловості разом із визнанням міждержавного регулювання мають стати двома основними методами, якими користуватиметься ЄС для сприяння розвитку глобальної системи Інтернет. Такий режим встановлюватиме нові вимоги до саморегулювання і стандартизації партнерства з урядами і міжнародними організаціями

222. До таких документів, що були підготовлені в рамках політики розвитку інформаційного суспільства в ЄС, зокрема, відносяться наступні: Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data 1995 O.J. L281 31; Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases, 1996 O.J. L77 20; Directive 97/7 of the European Parliament and the Council of 17 February 1997 on the protection of consumers in respect of distance contracts; Commission Green Paper «Legal Protection of Encrypted Services in the Internal Market» COM (96) 76 final, 1996 O.J. 76 final; Communication from the Commission «Follow-Up to the Green Paper on Copyright and related Rights in the Information Society» COM (96) 1996 O.J. 568 final; Green Paper on Commercial Communications in the Internal Market, COM (96) 1996 O.J. 192 final; Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, COM (96) 1996 O.J. 483. – Pp. 23-32.

з метою розбудови конструктивної й ефективної правової структури, у межах якої глобальний порядок може бути встановлено, узгоджено та імплементовано»²²³. Він також зауважив щодо обмеження ролі урядового регулювання на рівні ЄС: «Держава не матиме потреби у встановленні детальних норм, за винятком окремих випадків, де чітко існуватиме така потреба».

Як бачимо, згодом сталася значна зміна політики ЄС щодо методів правового регулювання Інтернету. Пояснюється це двома причинами. Перша причина - реакція ЄС на ключовий документ у галузі формування політики США стосовно Інтернету: Звіт Клінтона в червні 1997 р. «Рамкова політика у сфері глобальної електронної комерції» (Framework for Global Electronic Commerce). Кожна з трьох частин звіту присвячена відповідно фінансовим, правовим і ринково-економічним питанням міжнародного розвитку мережі Інтернет. У документі наголошено на необхідності створення вільної торгової зони в Інтернеті із запобіганням дискримінаційному оподаткуванню, завищеним тарифам та надмірному регулюванню. Особливо наголошувалось на необхідності саморегулювання промисловості в цій галузі²²⁴. Друга причина такої зміни політики ЄС — нова політична стратегія, спрямована на прискорення входження ЄС до світового комерційного інтернет-ринку.

Щодо першої причини, то ще раз зауважимо, що з 1991 по 1997 роки ЄС декларував майже необмежене урядове регулювання Інтернету. Клінтон оприлюднив Звіт щодо Інтернету в червні 1997 року, слідом за цим ЄС почав декларувати саморегулювання інтернет-промисловості. Відтак, ЄС намагався привести свою політику у відповідність із проголошеною політикою США як лідера інтернет-індустрії. Щодо другої причини можна зауважити, що зміни політики ЄС можуть пояснюватися потребою прискорити входження Європи до інтернет-ринку, а отже зайняти конкурентоспроможну економічну

223. European Official Pushes Global Internet Guidelines, Rep. On Electronic Com., Sept. Working Group 4-23, 1997. – UNCITRAL: UN Press 1997 [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.uncitral.org/index.html>.

224. Clinton W. A Framework for Global Electronic Commerce / W. Clinton, A. Gore [Електронний ресурс]. - Режим доступу до ресурсу: <http://www.iitf.nist.gov/eleccomm/ecom.html>.

позицію в Інтернеті. Отже, певні заходи із саморегулювання в цій галузі вважаються прийнятним вибором в регулюванні суспільних відносин у сфері Інтернету в Європі. Правознавці визначають, зокрема, такі методи саморегулювання, що застосовуються в ЄС²²⁵: рейтингові системи, скрінінгове програмне забезпечення і систему контрактного користування. У такого регулювання є свої переваги і недоліки.

До переваг саморегулювання можна віднести суворішу експертизу і повнішу обізнаність тих, хто прямо здійснює технічне регулювання мережі, менший бюрократизм і скорішу адаптацію норм права, гнучкість їх упровадження та зменшення витрат. Однак, слід відмітити і недоліки саморегулювання: упередженість з боку тих, хто відповідатиме за саморегулювання, недостатню здатність упроваджувати правозастосування, існування в суспільстві побоювань щодо загрози того, що ліберальна природа промислового саморегулювання не буде здатна запобігти проявленню негативного потенціалу Інтернету: викрадення даних в електронній формі, порушення авторських прав і прав на торговельні марки, поширення дитячої порнографії. А відтак існує можливість того, що всі ці негативні наслідки можуть переважити комерційну вигоду — стрімкий розвиток підприємництва.

Загалом стандартний підхід на рівні ЄС полягає в тому, що регулювання Інтернету відбувається на рівні специфічних аспектів таких відносин, в основному це стосується економіки — електронної комерції. Попередні регулятивні заходи не були спеціально спрямовані на врегулювання відносини у сфері Інтернету, а стосувались ІКТ загалом. Поступово ці заходи стали все більш орієнтованими на Інтернет, як приклад, прийняті у 2000 році Директиви з електронної комерції²²⁶ і цифрового підпису²²⁷.

225. Feeley M. EU Internet Regulation Policy: The Rise of Self-Regulation / M. Feeley // Boston College Industrial and Commercial Law Review. – Boston: BC LR P, 1999. – № 39 – P. 328.

226. 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) // Official Journal of the European Communities, L 178. – 2000.

227. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a

У будь-якому випадку визначення політики у сфері спільного регулювання відносин в Інтернеті як поєднання галузевого саморегулювання, державного і міжнародного регулювання — свідчить про здатність визнати необхідність оновлення правового регулювання в новому середовищі і застосовувати до них гнучкі регулятивні режими. В Європі відбувається стрімкий розвиток Інтернету, і ЄС докладає відповідних зусиль для формулювання регулятивних схем.

Так, у лютому 1998 р. Європейська комісія опублікувала два повідомлення щодо зміни національної політики держав-членів ЄС, а також закликала уряд США спільно працювати над загальною багатосторонньою основою для глобальної електронної комерції. Перший документ Комісії «Глобалізація і інформаційне суспільство» окреслив «потребу в посиленні міжнародної координації» і «міжнародної системи правозабезпечення» для посилення електронної комерції²²⁸. Другий документ — «Питання міжнародної політики, які стосуються правового регулювання Інтернету». Ці документи засвідчили, що Комісія включила Інтернет до кола питань європейської політики.

ЄС вимагав збалансувати інтереси і відповідальність «так, щоб міжнародний характер Інтернету було визнано при застосуванні відповідних юрисдикцій у світі»²²⁹. Визначалось кілька принципів правового регулювання Інтернету, серед яких були рівноправна участь міжнародного приватного сектора (включаючи представництво інтересів споживачів і користувачів) і членство у відповідних міжнародних організаціях, особливо міждержавних. ЄС визначив, що підхід до правового регулювання Інтернету з боку США є застарілим. Відповідно, існує можливість для європейських та інших країн долучитись до наступної фази розвитку Інтернету²³⁰.

Community Framework for Electronic Signatures (Electronic Signatures Directive) // Official Journal of the European Communities, L 13. — 1993. — P. 12.

228. European Commission, 1998. Globalisation and the Information Society: The Need for Strengthened International Coordination. COM(98)50 [Електронний ресурс]. — Режим доступу до ресурсу: <http://www.ispo.cec.be/eif/policy/com9850en.html>.

229. European Commission, 1998, International Policy Issues Related to Internet Governance. COM(98)111 [Електронний ресурс]. — Режим доступу до ресурсу: <http://www.ispo.cec.be/eif/policy/governance.html>.

230. European Community, 1998. Internet Governance: Reply of the European Community and its

Європейські пропозиції багатосторонньої міжнародної системи не були впроваджені. Представники ЄС зазначали, що в ICANN існує неузгодженість стосовно того, як координувати глобальну мережу Інтернет, зокрема неузгодженим є розподіл повноважень між представниками приватного і публічного секторів у ICANN. Представники ЄС зазначали: «ICANN приймає рішення, які мали приймати уряди держав у рамках роботи міжнародних організацій»²³¹. Таким чином, в ЄС визнали, що «загальна глобалізація правового регулювання Інтернету лишається невиконаною, а відтак існує необхідність залучати Міжнародний союз електрозв'язку до активної участі в міжнародних ініціативах, які стосуються регулювання у сфері Інтернету»²³².

Європейські фахівці одностайні у своїй думці, що прагнення ЄС до правового регулювання Інтернету на міжнародному рівні має під собою підґрунтя. Існує широке коло заходів: від «м'якого права» до участі в міжнародних неурядових організаціях, таких, як ICANN, «Товариство Інтернету»²³³ чи поєднання таких заходів. Ще один аргумент на користь міжнародно-правового регулювання Інтернету: країни, які розвиваються, отримують можливість брати участь у цьому процесі. До того ж, це більш прийнятно для регулювання такого аспекту діяльності в Інтернеті, як захист прав людини. І, крім того, на думку європейців, міжнародний рівень регулювання мережі знизить виключний вплив США на правове регулювання відносин в Інтернеті.

Member States to the US Green Paper [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.ispo.cec.be/eif/policy/govreply.html>.

231. Communication from the Commission «Follow-Up to the Green Paper on Copyright and related Rights in the Information Society» COM (96) // Official Journal of the European Communities, COM(96) 568 final – 1996. – P. 45–47.

232. Resolution of the Council of the European Union on the Organisation and Management of the Internet, 09/28/00 [Електронний ресурс]. – Режим доступу до ресурсу: <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/InternetGovernance/ResolutionEN.html>.

233. *Internet Engineering Task Force* («Група для вирішення задач проектування Інтернету»), IETF і її робочі групи займаються розвитком протоколів Всесвітньої мережі. Організація IAB (англ. *Internet Architecture Board* — Рада з архітектури Інтернету) оголошує ці протоколи стандартами Інтернету. З 1992 року IETF, IAB та ряд інших організацій утворюють Товариство Інтернету (англ. *Internet Society*, ISOC) — організаційну основу для різноманітних дослідницьких та консультативних груп, що займаються розвитком і удосконаленням міжнародної системи функціонування Інтернету.

Таким чином, можна зробити висновок, що, на відміну від американського уряду, що пропонував ринково-орієнтоване рішення і здійснення регулювання Інтернету приватним сектором, ЄС запропонував змішаний приватно-публічний режим регулювання мережі, разом із значними повноваженнями державних органів. Більше того, побоюючись американської переваги в кіберпросторі, ЄС виробив багатосторонню міжнародну структуру для трансформації структури регулювання Інтернету. І хоча ЄС пізніше визнав лідерство США (адже головний комп'ютер в Інтернеті — кореневий сервер «А» належить Америці) і факт встановлення приватного режиму регулювання, він істотно вплинув на цей процес шляхом залучення суб'єктів публічного права до роботи в новій організації ICANN так само, як і відповідне пропорційне представлення європейців в її органах.

Формування ICANN посилило роль ЄС у регулюванні мережі. Одним з найважливіших кроків ЄС у цьому напрямку стало впровадження нового домену верхнього рівня — «.EU». Бажання Комісії ЄС запровадити домен верхнього рівня (TLD) — «.EU» означає впровадження незалежної політики стосовно Інтернету в Європі. Відтак, керування TLD.EU надало повноваження Комісії визначити норми регулювання цього домену. Отже, ЄС включив Інтернет до кола питань своєї політики, запровадив амбітний план «Електронної Європи» (рішення Ради міністрів ЄС 2003 р.)²³⁴, щоб наздогнати США. При цьому слід зазначити, що спільний інтерес у розвитку Інтернету об'єднує ЄС і США, незважаючи на суперечки стосовно інституційної структури для досягнення цих цілей.

Розглядаючи формування системи правового регулювання відносин у сфері Інтернету в ЄС, доцільно більш детально торкнутись окремих галузей законодавства, яким в ЄС приділено значну увагу, зокрема захисту персональних даних, поширенню протиправної інформації в Інтернеті та боротьбі з кіберзлочинністю.

234. Resolution of the Council of Ministers «eEurope 2005 Action Plan» (2003) [Електронний ресурс]. — Режим доступу до ресурсу: http://ec.europa.eu/information_society/europe/2005/doc/all_about/resolution.pdf.

Захист персональних даних. Директива ЄС із захисту прав людини стосовно автоматизованої обробки персональних даних є прикладом законодавства, застосування якого має прямі і досить жорсткі наслідки для третіх країн.

Директива була прийнята в жовтні 1995 р. для забезпечення права на приватність громадян ЄС. Директива вимагає від усіх держав-членів ЄС імплементувати до національного законодавства ці положення протягом трьох років після її прийняття. Документ спрямований на досягнення рівності всіх держав ЄС у забезпеченні прийняття уніфікованого національного законодавства із захисту даних. Крім того, Директива вимагає від держав-членів обмежити передачу даних лише до тих третіх країн, які продемонструють адекватний рівень захисту даних.

Хоча адекватність і не означає еквівалентність, однак це означає, що існує вимога певного рівня визнання і відповідності законодавства третіх країн законодавству ЄС. Директива є прикладом такої схеми регулювання, що поширює значний вплив далеко за межі тієї сфери, на яку спрямована. Отже, крім положень, які вимагають блокування даних, Директива також має результатом впровадження вимоги до третіх країн створити нову політику і впровадити нові технології забезпечення адекватного захисту даних. Відтак, обсяг дії Директиви виходить за межі ЄС, що спричиняє значний вплив на треті країни.

Директива не є першим кроком з боку країн Європи до впровадження захисту персональних даних. У 1981 році Рада Європи прийняла Конвенцію щодо захисту прав фізичних осіб при автоматичній обробці персональних даних²³⁵. Директива чітко визначає, що базується на цій Конвенції, і, відповідно, метою Директиви є «захист основних прав і свобод фізичних осіб, зокрема їх права на приватне життя при обробці персональних даних» (ст. 1 Директиви). Директива зобов'язує держави-члени ЄС запровадити законодавство, за допомогою якого відбудуватиметься імплементація

235. Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data, Jan. 28, 1981 // European Technology Service. - 1981. - No. 108. - P. 348.

її положень (ст. 4 Директиви). Гармонізація законодавства країн забезпечить рівний рівень захисту даних по всьому ЄС.

У листопаді 1997 року Єврокомісія прийняла нову Пропозицію щодо Плану дій з безпечного користування Інтернетом. Держави-члени ЄС вітали ініціативу Європейської комісії і прийняли підхід Комісії стосовно захисту від поширення неправомірного та шкідливого контенту в Інтернеті²³⁶. Вже у грудні 1998 року Рада ЄС ухвалила План дій щодо забезпечення безпечного користування Інтернетом²³⁷, що містив ряд заходів на період з 1999 по 2002 роки. Однак, на думку Європарламенту, не слід вважати, що цей План може зупинити поширення протизаконної і шкідливої інформації в Інтернеті. Лише міжнародні угоди, у яких братимуть участь найрозвиненіші країни, такі, як ЄС, США, Японія, сприятимуть вирішенню цієї проблеми. А «План дій» — це один із заходів на цьому шляху. Представники урядових органів ЄС, беручи до уваги глобальну природу Інтернету, відзначили користь саморегулювання для цього середовища стосовно незаконного та шкідливого контенту, а в Плані запровадили створення мережі гарячих ліній із сповіщення щодо правопорушень в Інтернеті, зокрема дитячої порнографії, та розробку моніторингових схем нагляду за контентом.

Всі ці заходи неможливо ефективно запровадити без згоди тих, хто безпосередньо здійснює підтримку функціонування Інтернету. Саме тому, Європейська Рада звернулася до держав-членів ЄС з наполегливим проханням сприяти розвитку систем саморегулювання, включаючи представницькі органи для провайдерів і користувачів Інтернету, ефективні кодекси поведінки і наявність гарячих ліній, що інформують громадськість про доступні механізми. Європейська Рада направила на адресу Комісії прохання сприяти розвитку координації органів саморегулювання і представницьких органів на рівні ЄС,

236. Наприклад, підтримку такої програми висловлено у Позичії Палати Спільнот Парламенту Великої Британії.

237. Common position (EC) No 56/98 adopted by the Council on 24 September 1998 with a view to adopting Decision No./98/EC of the European Parliament and of the Council adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks // Official Journal of the European Communities, C 360. – 1998. - P.113-115.

підтримувати і розвивати обмін інформацією про останні досягнення в цій сфері.

Запобігання поширенню протиправної інформації через Інтернет. Незважаючи на істотні переваги Інтернету, можливі негативні аспекти поширення Інтернету не слід недооцінювати. У зв'язку з цим Рада з телекомунікацій Європейської Комісії 27 вересня 1996 р. прийняла Повідомлення про запобігання поширенню через Інтернет протиправної та шкідливої інформації²³⁸, в якому зазначалося, що Комісія усвідомлює важливість цих проблем і прагне вирішити їх з урахуванням встановлення правильного балансу між вільним потоком інформації і гарантованим захистом суспільних інтересів. Хоча контент-провайдери безпосередньо не контролюють зміст, який поширюється через Інтернет, у деяких випадках їх діяльність стає об'єктом розслідування, оскільки через них здійснюється доступ до незаконної або шкідливої інформації. Так само як і провайдери хостінгових послуг, що безпосередньо надають місце для веб-ресурсів або груп новин, вони несуть відповідальність за зміст ресурсів.

У деяких європейських країнах прийняті або пропонуються до прийняття закони, що дозволяють поширити на провайдерів хостінгових послуг юридичну відповідальність за зміст ресурсів, що розташовані на їх комп'ютері (в разі, якщо ці провайдери знали, що цей зміст є незаконним, або не вжили заходів для його усунення).

Режим відповідальності провайдерів інтернет-послуг. Як зазначалося вище, в ЄС прийнято Директиву «Про електронну комерцію» від 8 червня 2000 р. № 2000/31/ЄС. Директива передбачає, що сервіс-провайдер оперативно видаляє або відключає доступ до інформації, яку він зберіг, після того, як суд чи адміністративний орган прийняв рішення про видалення такої інформації (ст.13). Аналогічно, хостінг-провайдер після отримання інформації про незаконну діяльність та пов'язані з цим вимоги про відшкодування збитків оперативно видаляє її або відключає

238. Illegal and harmful content on the Internet. Communication to the European Parliament, the Council, the economic and social committee and the committee of the regions, 1996 [Електронний ресурс]. – Режим доступу до ресурсу: <http://europa.eu.int/ISPO/infosoc/legreg/docs.html>.

доступ до неї (ст.14), при цьому процедура видалення інформації або припинення доступу до неї може визначитися у національному законодавстві держави-члена.

Розглянемо деякі норми більш детально. Так, стосовно сервіс-провайдерів, які забезпечують передачу інформації в Інтернеті або доступ до мережі, норми щодо звільнення їх від відповідальності встановлені у статті 12 Директиви. Держави-члени повинні гарантувати, що сервіс-провайдер не несе відповідальності за інформацію, що передається, за умови, що: - він не є ініціатором передачі інформації; - не вибирає отримувача інформації; - не може впливати на цілісність інформації, що передається. Разом з тим, ця норма не забороняє суду або адміністративному органу в рамках існуючої правової системи вимагати від сервіс-провайдера припинити або запобігти порушенням.

Відповідно до статті 13 Директиви сервіс-провайдер не повинен нести відповідальність також за автоматичне, проміжне і тимчасове зберігання інформації, що передається (хешування), здійснене з єдиною метою — зробити більш ефективною подальшу передачу інформації до інших одержувачів послуг за їх проханням, за умови, що: провайдер не модифікує інформацію; провайдер дотримується умов доступу до інформації; провайдер дотримується правил, що стосуються оновлення інформації, прийнятих у відповідній галузі; провайдер не заважає законному використанню технологій, які використовуються у певній галузі, для отримання даних про використання інформації; провайдер оперативно видаляє або відключає доступ до інформації, яку він зберіг після того, як дізнався, що інформація була видалена з первинного джерела передачі або доступ до нього був відключений, або суд чи адміністративний орган прийняв рішення про видалення такої інформації. Разом з тим, ця норма не забороняє суду або адміністративному органу в рамках існуючої правової системи вимагати від сервіс-провайдера припинити або запобігти порушенням.

Стосовно сервіс-провайдерів, які надають послуги хостінгу, тобто технічну можливість для зберігання інформації, норми щодо

обмеження їх відповідальності встановлені у статті 14 Директиви, відповідно до яких провайдер не несе відповідальності за інформацію, що зберігається користувачами, за умови, що: - провайдер не знає про незаконну діяльність або інформацію, що стосується позовів про відшкодування збитків, не знає про факти та обставини, з яких була виявлена незаконна діяльність або інформація; після отримання інформації про незаконну діяльність оперативно видаляє її або відключає доступ до неї. При цьому як суд, так і адміністративні органи можуть вимагати від провайдера припинити або запобігти порушенню, а також держави-члени можуть у законодавстві визначити процедуру видалення або припинення доступу до такої інформації. Отже, встановлення факту незаконної діяльності, а також видалення та відключення доступу до інформації має здійснюватися за рішенням суду або адміністративного органу у порядку, визначеному законодавством.

Стаття 15 Директиви визначає, що провайдери не повинні робити моніторинг інформації, передачу якої вони здійснюють або зберігають, а також намагатися з'ясувати обставини, що свідчать про незаконну діяльність. Таким чином, у цілому Директива встановлює щодо сервіс-провайдерів досить сприятливий правовий режим діяльності, що захищає їх від ризику збитків. При цьому, у Директиві закладена модель захисту контенту: «повідомлення та закриття». Суд або адміністративний орган держави-члена ЄС мають право вимагати від сервіс-провайдера припинення або запобігання порушенню законодавства, хоча будь-які рамкові критерії санкцій в Директиві не визначені, за винятком непрямої вказівки в статті 20 про те, що встановлені державами-учасниками міри покарання повинні бути дієвими, пропорційними і переконувати порушників дотримуватися закону.

Директива віддає пріоритет позасудовим механізмам вирішення спорів у галузі електронної комерції, припускаючи, що саме вони найбільше відповідають сутності послуг інформаційного суспільства, і встановлює такі вимоги до законодавства держав-учасників (стаття

17): 1) не повинно бути перешкод до застосування позасудових процедур для врегулювання спорів між провайдером і одержувачем послуг, включаючи використання електронних засобів; 2) органи позасудового врегулювання повинні забезпечувати адекватні процесуальні гарантії для сторін-учасниць, особливо при розгляді спорів за участю споживачів.

Крім того, встановлено низку обов'язків і для самих держав-учасниць у цій галузі (статті 17 і 19): заохочувати діяльність позасудових органів щодо надання відомостей Комісії ЄС про прийняття принципових рішень щодо послуг інформаційного суспільства, а також з розповсюдження інформації про практику, звичаї та традиції в сфері електронної комерції (такий же обов'язок держав-учасниць встановлено в статті 19 (5) стосовно судових процедур).

Якщо звернути увагу на механізми, які застосовуються до вирішення цієї проблеми в державах-членах ЄС загалом, слід зазначити, що у випадку порушення прав інтелектуальної власності в Інтернеті в рамках судового процесу використовують такі способи захисту прав суб'єктів авторського та суміжних прав, як судові заборони щодо провайдерів, покладення на провайдера обов'язку здійснювати фільтрацію порушень зобов'язань на веб-сайтах. Висловлюються також пропозиції про надання провайдерам у випадку повторних правопорушень можливості здійснювати відповідні заходи за власною ініціативою, а також про надання переваги застосуванню попереджень. В цілому, переважає позиція про застосування відповідних санкцій лише за рішенням суду, а також надання переваги застосуванню саме правових засобів²³⁹.

Запобігання вчиненню злочинів у галузі комп'ютерних технологій. Країни Європейського Союзу послідовно провадять політику співробітництва в галузі протидії комп'ютерній злочинності. Так, з метою уніфікації національних законодавств у 1989 р. Комітетом

239. Synthesis Report of European Commission on the Stakeholders' Dialogue on Illegal Up- and Downloading 2009-2010, March 2011. – P.7.

міністрів Європейської Ради був погоджений і затверджений перелік правопорушень (так званий «Мінімальний перелік порушень»), рекомендований країнам-членам ЄС для розробки єдиної стратегії. Цей список містить вісім видів комп'ютерних злочинів (комп'ютерне шахрайство, комп'ютерна підробка, пошкодження комп'ютерної інформації і програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних мереж, несанкціоноване перехоплення інформації, несанкціоноване копіювання комп'ютерних програм, незаконне виготовлення топографічних копій).

У Раді Європи вдалися до більш жорсткої правової регламентації діяльності в галузі ІКТ (зокрема в тому, що стосується скоєння комп'ютерних злочинів). В 2000 році під егідою Ради Європи було підготовлено проект міжнародного документа за участю великої кількості держав. Мета документа — розробка загальних положень про регулювання Інтернету, а також принципів співробітництва правоохоронних органів різних країн у боротьбі з кіберзлочинністю. В проекті зазначалось, що він має стати «першим міжнародним договором, присвяченим аспектам кримінального права і процедурним аспектам різного роду злочинної поведінки, спрямованої проти цілісності й недоторканності комп'ютерних систем, мереж і даних».

Кожна сторона договору повинна буде прийняти таке законодавство та інші заходи, що будуть необхідні для переслідування визначених кримінальних правопорушень. Цей договір пропонує усім країнам-членам прийняти систему покарань для хакерів, а також заборонити використання «білих» хакерських програм, що застосовуються для тестування безпеки корпоративних систем. Договір також зобов'язує Інтернет-компанії до тіснішого співробітництва з правоохоронними органами, зокрема, провайдерам можуть запропонувати тривале зберігання великих обсягів даних.

Представляючи цей проект на саміті Великої вісімки, Президент Франції Жак Ширак зазначив, що «саморегулювання, яке пропонують Інтернет-компанії замість правових норм, не може перебрати на себе

роль держави у захисті прав її громадян від правопорушень»²⁴⁰.

Зазначений проект дуже стурбував Інтернет-індустрію, що віддає перевагу саморегулюванню Інтернету. Він не отримав значної підтримки в Інтернет-спільноті, правозахисники піддали його суворій критиці: представники *Internet Alliance* і *Global Internet Project* заявили, що серйозне втручання держави в регулювання Мережі може задушити розвиток електронної комерції, оскільки у правоохоронних органів з'явиться можливість здійснювати свою діяльність за рахунок Інтернет-компаній, що будуть зобов'язані «співпрацювати». Міжнародна коаліція з 28 правозахисних груп «Кампанія за свободу в Інтернет» зробила в своєму Зверненні до РЄ²⁴¹ докладний розгляд досить спірних юридичних нововведень, запропонованих у проекті і таких, що суперечать європейській Конвенції про права людини. Вони висловили думку, що цей проект «суперечить нормам захисту особи, підриває розробку ефективних технологій мережевої безпеки і знижує підзвітність урядів у їхній правоохоронній діяльності». «Важко уявити будь-який перелік регулятивних вимог, які будуть достатньо гнучкі для регулювання широкого кола питань сучасного ринку» — зазначалось у заяві представника *Global Internet Project* Дж. Патріка (віце-президент кампанії ІВМ). Також він зазначив, що уряди мають сфокусуватись на підвищенні рівня безпеки їх власних систем та запобіганні місцевим «кіберзлочинам». Поява нових законів, що залучатимуть поліцію до «співрегулювання» Інтернету, може призвести до міжнародної міграції компаній до країн з більш сприятливою регуляторною політикою.

Однак, незважаючи на відсутність підтримки і значну критику Інтернет-спільноти, 23 листопада 2001 р. у Будапешті була підписана Міжнародна конвенція про кіберзлочинність (далі — «Конвенція»). Очевидно, що подальша протидія комп'ютерній злочинності буде

240. European Union Considers Regulatory Framework For Electronic Commerce [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.iwar.org.uk/e-commerce/resources/eu/src/ecomcom3.htm>.

241. Звернення «Кампанії за свободу Інтернет» до Ради Європи з приводу прийняття Конвенції щодо кіберзлочинності [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.gilc.org/privacy/coe-letter-1000.html>.

здійснюватися шляхом розвитку основних положень цього нормативно-правового документа. Основна мета Конвенції (ст. 39) — доповнення відповідних багатосторонніх і двосторонніх угод і домовленостей, включаючи положення Європейської конвенції про видачу (Париж, 13 грудня 1957 р.; Європейської конвенції про взаємну правову допомогу у кримінальних справах (Страсбург, 20 квітня 1959 р.); Додаткового протоколу до Європейської конвенції про взаємну правову допомогу в кримінальних справах (Страсбург, 17 березня 1978 р.). До структури Конвенції включено наступні розділи:

1. Визначення напрямків уніфікації національних кримінальних законодавств. Так, пропонується ввести на національному рівні кримінальну відповідальність за: навмисний протиправний доступ до комп'ютерної системи в цілому або будь-якої її частини; навмисне перехоплення комп'ютерних даних, переданих у комп'ютерну систему; навмисне пошкодження, видалення, погіршення якості, зміна або блокування комп'ютерних даних; навмисне створення перешкод функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, видалення, погіршення якості, зміни або блокування комп'ютерних даних; навмисне виробництво, продаж або інші форми надання в користування апаратних і програмних пристроїв, а також комп'ютерних паролів, кодів доступу, за допомогою яких можливий доступ до комп'ютерної системи в цілому або будь-якої її частини, розроблених або спеціально пристосованих для здійснення зазначених вище правопорушень; навмисне введення, знищення, зміна або блокування комп'ютерних даних, що спричинило порушення автентичності цих даних (комп'ютерна підробка); навмисне введення, зміна або блокування комп'ютерних даних, а також будь-яке втручання у функціонування комп'ютерної системи з метою неправомірного отримання економічної вигоди для себе або іншої особи (комп'ютерне шахрайство); правопорушення, пов'язані з порушенням авторських і суміжних прав. Важлива роль

- відведена установленню відповідальності за правопорушення, пов'язані з дитячою порнографією.
2. Встановлення єдиних сфер застосування кримінально-правових норм щодо:
 - а) злочинів, відповідальність за здійснення яких передбачена Конвенцією;
 - б) інших злочинів, вчинених за допомогою комп'ютерної системи.
 3. Гармонізація механізму збору доказів вчинення злочину в електронній формі.
 4. Міжнародне співробітництво.

Важливим вважається також досягнення і дотримання балансу між приватним життям осіб і потребою передачі даних, що стосуються індивідів. Принципи звичайного середовища не завжди переносяться ефективно в кіберпростір: завжди існує небезпека втручання в суверенітет інших країн у спробі регулювання Інтернету, можливого порушення норм міжнародного права. Відповідно, майбутні спроби правового регулювання для відповідності принципам міжнародного права і запобіганню конфліктам між державами мають залежати від міжнародних угод та спиратися на саморегулювання.

На рівні держав-членів ЄС немає жодних сумнівів щодо намірів якомога повнішого регулювання Інтернету. Однак, через культурне, історичне і соціо-політичне різноманіття склались різні підходи до регулювання Інтернету в різних європейських країнах. Наприклад, коли в Німеччині уряд виразив занепокоєння щодо використання Інтернету неонацистами, у Великій Британії виявлено менше хвилювання стосовно небезпеки расизму, але особлива увага приділяється неправомірному поширенню матеріалів порнографічного характеру. Отже, на думку фахівців, ЄС має у своїй політиці спробувати відповідним чином визначити і узгодити ці підходи, що різняться між собою.

Виходячи з того, що інституції ЄС зацікавлені у функціонуванні,

відкритості і розвитку внутрішнього ринку, регулювання (чи не регулювання) Інтернету на рівні окремих держав-членів може призвести до розбіжностей (наприклад, встановлення в різних державах різних норм щодо відповідальності інтернет-провайдерів) і, таким чином, порушити вільний обіг послуг, що, у свою чергу, призведе до втрати європейцями конкурентоспроможності на міжнародному рівні. «З огляду на головні принципи поваги до розбіжностей і субсидіарності не дивно, що держави Західної Європи і ЄС уникали домінування і встановлення монополістичних форм управління. Це не означає, що Інтернет є «безправним місцем», зауважив фахівець з кіберправа Дж. Р. Ройденберг²⁴² щодо політики Західної Європи. Загалом, підсумовуючи огляд законодавства ЄС у галузі інтернет-технологій, можна зазначити наступне: у кожній з держав - членів ЄС питання регулювання використання Інтернету намагаються вирішувати за допомогою спеціальних законів (правотворча робота ведеться в цьому напрямку в усіх країнах-членах ЄС). Однак, законодавці ЄС виходять з того, що не слід квапитися з цим, адже потрібен певний час для прояву результатів процесу саморегулювання.

Можна зробити наступні висновки і щодо схеми правового регулювання суспільних відносин у сфері Інтернету в ЄС: глобальні регуляторні рішення, підготовлені в рамках таких організацій, як ООН; регіональне наднаціональне законодавство на рівні ЄС; законодавство, що приймається на рівні держав чи регіональному рівні; регламенти, що відносяться до саморегулювання і приймаються інтернет-провайдерами; кодекси поведінки інтернет-користувачів тощо.

Сучасні тенденції розвитку правового регулювання Інтернету та інформаційного суспільства ЄС в цілому. Публікація Європейською комісією в 1987 році Зеленої книги з розвитку спільного ринку для телекомунікаційних послуг та обладнання ознаменувала початок процесу лібералізації телекомунікаційного сектора. Рамкова структура правового регулювання сектора телекомунікацій складається з п'яти

основних директив. ЄС завершив лібералізацію європейського ринку телекомунікацій в 1998 році, а потім двічі реформував її: в 2003 і 2009. «Пакет Телекомунікацій» 2009 р. спрямовано на забезпечення справедливої конкуренції між операторами телекомунікацій.

Таким чином, до нової нормативно-правової бази належать:

- Директива 2002/21/ЄС від 7 березня 2002 року про спільні правові рамки для електронних комунікаційних мереж та послуг (Рамкова Директива)²⁴³;
- Директива про авторизацію електронних комунікаційних мереж і послуг (*Authorisation Directive*)²⁴⁴;
- Директива про доступ до мереж електронних комунікацій та пов'язаних з ними ресурсів (*Access Directive*)²⁴⁵;
- Директива про універсальні послуги та права користувачів стосовно мереж електронних комунікацій та послуг (*Universal Service Directive*)²⁴⁶;
- Директива про обробку персональних даних та захист конфіденційності в секторі електронних засобів зв'язку (*Directive on the processing of personal data (the Privacy and Electronic Communications Directive)*)²⁴⁷.

243. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021>.

244. Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) [Електронний ресурс]. – Режим доступу до ресурсу: http://europa.eu/legislation_summaries/information_society/legislative_framework/124164_en.htm.

245. Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to and interconnection of electronic communications networks and associated facilities (Access Directive) [Електронний ресурс]. – Режим доступу до ресурсу: http://europa.eu/legislation_summaries/information_society/legislative_framework/124108i_en.htm.

246. Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) [Електронний ресурс]. – Режим доступу до ресурсу: http://europa.eu/legislation_summaries/information_society/legislative_framework/124108h_en.htm.

247. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Електронний ресурс]. – Режим доступу до ресурсу: http://europa.eu/legislation_summaries/information_society/legislative_framework/124120_en.htm.

Крім того, до пакету входить Рішення про правові рамки для радіоспектральної політики в Європейській Спільноті (Радіоспектральне Рішення) (*Radio Spectrum Decision*)²⁴⁸.

«Телеком-пакет» був розширений у 2009 році, коли до нього було додано дві Директиви — Директива 2009/140/ЄС від 25 листопада 2009 року, яка доповнює Директиву 2002/21/ЄС про спільні правові рамки для електронних комунікаційних мереж та послуг, Директиву 2002/19/ЄС про доступ і з'єднання електронних комунікаційних мереж та пов'язаного оснащення й Директиву 2002/20/ЄС про дозвіл електронних комунікаційних мереж та послуг (*Better law-making Directive*)²⁴⁹, а також — Директиву 2009/136/ЄК від 25 листопада 2009 року, яка доповнює Директиву 2002/22/ЄС про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг, Директиву 2002/58/ЄС про обробку персональних даних та захист таємниці сектора електронних комунікацій²⁵⁰ та Рішення (ЄС) № 2006/2004 про взаємодію національних органів, відповідальних за забезпечення виконання законів про захист споживачів (*Citizens' rights*), а також Регламент (ЄС) № 1211/2009 від 25 листопада 2009 року²⁵¹, що засновує Орган Європейських Регуляторів у галузі Електронних Комунікацій (BEREC, *Body of European regulators for electronic communications*). Основна мета роботи цього агентства

248. Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision) [Електронний ресурс]. – Режим доступу до ресурсу: http://europa.eu/legislation_summaries/information_society/radiofrequencies/l24218a_en.htm.

249. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to and interconnection of electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0140>.

250. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0136>.

251. Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office [Електронний ресурс]. – Режим доступу до ресурсу:

полягає в активізації співпраці між національними регулюючими органами і зміцненні внутрішнього ринку електронних комунікаційних мереж.

Регулювання функціонування мережі Інтернет, Інтернет-діяльності і стандартів у сфері ІКТ. Єврокомісія визнала, що держави-члени стикаються з різноманітними проблемами, пов'язаними із всебічним впровадженням і використанням Інтернету, такими, як надання великої кількості віртуальних адрес, розробка сумісних технічних стандартів на всій території країн-членів ЄС з тим, щоб гарантувати сумісність, приватність і доступність Інтернету.

ЄС прагне боротися з незаконною діяльністю в Інтернеті за допомогою таких заходів, як Програма «Безпечний Інтернет», Програма «Захист дітей в цифровому світі»²⁵² або «Відкритий Інтернет та мережевий нейтралітет»²⁵³.

На даний момент в ЄС ведеться законотворча робота за наступними напрямками:

Управління мережею Інтернет: наступні кроки. Управління Інтернетом являє собою серйозну проблему як для приватних, так і для державних зацікавлених сторін. Останнім рекомендується брати активнішу участь, оскільки регламентація діяльності в Інтернеті є одним з пріоритетів державної політики Європейського союзу. Повідомлення 2009/277 містить докладну інформацію про існуючі системи управління Інтернетом і майбутньою діяльністю в цій галузі²⁵⁴.

Інтернет: архітектура та експлуатація. ЄС намагається бути в авангарді обговорення управління Інтернетом, зокрема, на Всесвітньому саміті з питань інформаційного суспільства (WSIS) у 2003 і 2005. ЄС був також провідним учасником міжнародних

252. Матеріали звіту: http://europa.eu/legislation_summaries/information_society/internet/si0023_en.htm.

253. Матеріали звіту: http://europa.eu/legislation_summaries/information_society/internet/si0022_en.htm.

254. Communication from the Commission to the European Parliament and the Council of 18 June 2009 - Internet governance: the next steps [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52009DC0277>.

дискусій, які сприяли створенню Інтернет-корпорації з присвоєння імен та номерів (ICANN). Крім того, ЄС підкреслює важливість подолання «цифрового розриву» і необхідність урахування інтересів користувачів в країнах, що розвиваються, в механізмах управління мережею Інтернет.

ЄС висуває такі основні принципи, що стосуються управління Інтернетом: 1) наявна архітектура мережі має бути збережена; 2) приватний сектор повинен зберегти у цьому провідну роль; 3) до участі мають бути залучені численні зацікавлені сторони; 4) уряди повинні більш активно брати участь в управлінні Інтернетом.

Майбутні мережі та мережа Інтернет. Відповідне Повідомлення було видано в рамках підготовки до створення «Інтернету майбутнього». У ньому розглядаються базові умови для підтримки Інтернету як динамічної, конкурентоспроможної та безпечної мережі та основні завдання на майбутнє в європейському контексті, а також описуються можливі відповідні заходи з боку уряду ЄС²⁵⁵.

Регулювання творчого онлайн-контенту. Он-лайн контент є транскордонним і його обсяги постійно зростають. Контент-послуги можуть значно підвищити конкурентоспроможність європейської музичної, кіно - та ігрової індустрії, тому Комісія заохочує розвиток сильнішого внутрішнього споживчого ринку для творчого онлайн-контенту. Мета Повідомлення СОМ (2007) 836²⁵⁶ полягає в сприянні доступності в Інтернеті творчого контенту шляхом впровадження до розробки нових та інноваційних бізнес-моделей, а також забезпечення додаткового прибутку для всіх, хто залучений до його створення.

«*.EU*» Домен верхнього рівня. «*.eu*» інтернет-домен верхнього

255. Communication from the Commission of 29 September 2008: Future networks and the internet [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0594:FIN:EN:PDF>.

256. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 3 January 2008 on Creative Content Online in the Single Market [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52007DC0836>.

рівня дає Європі свою власну ідентичність в мережі. Регламент № 733/2002²⁵⁷ спрямований на розширення присутності Європейського союзу в Інтернеті, збільшення вибору для користувачів доменних імен і сприяння розвитку електронної комерції на внутрішньому ринку.

Захист Європи від масових кібератак і збоїв. Оскільки приватне і професійне життя громадян все більше й більше залежить від інформаційних і комунікаційних технологій (ІКТ), захист найважливіших інформаційних інфраструктур (СІІС) від великих кібератак і порушень є серйозною проблемою для європейського суспільства і його економіки.

Повідомлення COM (2009) 149²⁵⁸ дає докладну інформацію про головні виклики, що стоять перед найважливішими інформаційними інфраструктурами (СІІС), і пропонує «План дій по боротьбі з кібератаками».

Запобігання атакам на інформаційні системи. Рамкове рішення № 2005/222²⁵⁹ направлене на боротьбу з кіберзлочинністю та сприяння інформаційній безпеці. У світлі цієї нової форми транснаціональної злочинності основна мета Рамкового рішення полягає в зміцненні співробітництва між судовими та іншими компетентними органами через наближення норм кримінального права щодо атак на інформаційні системи. Основні види кримінальних злочинів, визначені цим Рішенням, включають атаки на інформаційні системи: піратство, віруси і провокування відмов у роботі сервісів. У Рішенні визначено перелік засобів боротьби зі злочинною діяльністю, до якої належить боротьба зі спамом, програмами-шипигунами і шкідливими

257. Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002R0733>.

258. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 30 March 2009 on Critical Information Infrastructure Protection – «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience» [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52009DC0149>.

259. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32005F0222>.

програмами. А в Повідомленні СОМ 2006/688²⁶⁰ Єврокомісія закликає регулюючі органи і зацікавлені сторони подвоїти свої зусилля по боротьбі з такою протиправною діяльністю і запровадити конкретні заходи.

Програма Співтовариства «Безпечніший Інтернет 2009-13». Програма²⁶¹ спрямована на підвищення безпеки дітей в онлайн-овому середовищі і фокусується на двох цілях: підвищення рівня знань про використання нових технологій дітьми; виявлення і боротьба з ризиками, яким вони піддаються.

Захист персональних даних установами Співтовариства. Особливу увагу приділено захисту персональних даних, які обробляються установами і органами ЄС. Регламент 45/2001²⁶² містить положення, спрямовані на забезпечення високого рівня захисту персональних даних згідно положень Директиви 95/46 / ЄС. Іншим Рішенням Комісії 2008/597/ЄС від 3 червня 2008 р. прийняті правила, що стосуються захисту даних відповідно до статті 24 (8) Регламенту (ЄС) № 45/2001 про захист фізичних осіб стосовно обробки персональних даних установами та органами ЄС та про вільне переміщення таких даних.

Європейська комісія розглядає умови для перегляду нинішнього правового режиму захисту персональних даних. Мета полягає в тому, щоб модернізувати законодавство, адаптуючи його до викликів глобалізації та використання нових технологій, забезпечуючи при цьому захист прав осіб.

260. Communication from the Commission of 15 November 2006 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0688>.

261. Decision 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008D1351>.

262. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001R0045>.

Повідомлення № 2010/609²⁶³ пропонує нову стратегію для захисту особистих даних, що спрямована на перегляд поточної законодавчої бази, зокрема Директиви, пов'язаної з захистом персональних даних та Директиви про захист даних у секторі електронних комунікацій. У рамках цього перегляду Повідомлення встановлює кілька цілей: посилення прав фізичних осіб, зміцнення внутрішнього ринку. У наш час існують розбіжності в тому, як державам-членам застосовувати Директиву про захист персональних даних. У цьому зв'язку Комісія хоче зміцнити гармонізацію норм щодо захисту даних на рівні ЄС. Також пропонується перегляд правил захисту даних у галузі поліцейського і судового співробітництва та розвиток міжнародного захисту даних (особисті дані з третіх країн можуть циркулювати через держави-члени, якщо Комісія вважає, що рівень захисту даних, гарантований третьою країною, є адекватним. Проте, критерії, які дозволяють з'ясувати рівень захисту, ще не були чітко визначені. Крім того, Комісія вважає за доцільне узгодити положення, що стосуються захисту персональних даних, що містяться в міжнародних договорах ЄС, з третіми країнами. У зв'язку з цим Комісія планує розширити свою співпрацю з третіми країнами і стежити за розробкою міжнародних технічних стандартів.

Авторське право і суміжні права в інформаційному суспільстві. Розглядаються можливі напрямки майбутніх дій відносно оцифровки творів, використання творів з невизначеним авторством та захисту прав творців онлайн-контенту. Після проведення аналізу відповідей на Зелену книгу «Авторські права в економіці на основі знань» Європейська комісія оголосила низку заходів, що будуть реалізовані у сфері захисту прав інтелектуальної власності; визначаються напрямки стратегії Комісії щодо захисту авторських прав. У цьому напрямку Комісія має намір продовжити роботу на загальноєвропейському рівні щодо роз'яснення правових наслідків масової оцифровки та пошуку рішень проблеми.

263. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 4 November 2010 - A comprehensive approach on personal data protection in the European Union [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0609>.

Після Директиви 2001/29²⁶⁴, яка спрямована на адаптацію законодавства про авторське право і суміжні права в інформаційному суспільстві, було прийнято два документи — Рекомендацію ЄС щодо сприяння оцифровці та онлайн-доступності матеріалів у галузі культури і їх збереженню та Рекомендацію щодо необхідних заходів на всій території ЄС зі спрощення видачі ліцензій на онлайн-послуги.

264. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [Електронний ресурс]. – Режим доступу до ресурсу: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0029>.

13. Здійснення особистих немайнових прав особи в Інтернеті: судова практика Європейського суду з прав людини[©]

Відповідно до ст. 9 Конституції України²⁶⁵ чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства. З ратифікацією Конвенції про захист прав і основних свобод людини 1950р. (далі – Конвенція), Першого протоколу та протоколів № 2, 4, 7 і 11 до Конвенції, Україна взяла на себе зобов'язання забезпечувати охорону прав і законних інтересів людини, закріплених у цьому документі. Практичне застосування норми Конвенції знайшли в рішеннях Європейського суду з прав людини (далі – ЄСПЛ). Судова практика ЄСПЛ має істотне значення для України, оскільки рішення цього міжнародного судового органу стосовно України є обов'язковими для виконання нашою державою. В судовій практиці застосування судового прецеденту викликає чимало заперечень. Дійсно, для країни романо-германської правової сім'ї це питання не лише юридичної техніки, але й правових традицій. Однак процеси глобалізації, що мають відображення й в юридичній професії, вимагають більш гнучкого ставлення до можливості звертатися до судової практики у пошуках істини. На це дедалі частіше звертається увага в літературі²⁶⁶. За таких обставин важливим є врахування практики ЄСПЛ в процесі тлумачення норм національного законодавства та, зокрема, положень Конвенції.

265. Про захист прав людини і основоположних свобод: Конвенція. Міжнародний документ від 04.11.1950. Ратифіковано Законом України № 475/97-ВР від 17.07.97. Офіційний вісник України. 1998 р., № 13, № 32 від 23.08.2006, с. 270.

266. Див. наприклад: Антонович М. Конвенція про захист прав людини і основних свобод у судах Європейських держав та перспективи її застосування в Україні / М. Антонович // Право України. – 2000. – №8. – С. 42 – 46; Полешко А. Імплементация норм Міжнародного права у вітчизняному законодавстві – важливий аспект правової реформи [Електронний ресурс] / А. Полешко. – Режим доступу: www.humanrights.gov.ua/.

Практика ЄСПЛ щодо захисту прав людини в сфері використання Інтернету та інших технологій охоплює такі основні аспекти як: 1) питання юрисдикції; 2) захист персональних даних; 3) Інтернет та свобода слова; 4) Інтернет та право на приватність; 5) Інтернет та право інтелектуальної власності; 6) доступ до інформації та Інтернет; 7) кримінально-правові

питання регулювання Інтернету (захист користувачів Інтернету від неправомірно розповсюдженої інформації тощо)²⁶⁷.

Найбільш цікавими для України є справи про конкуренцію права на повагу приватності особи із правом на свободу слова, правом на доступ до інформації, а також — щодо прав інтелектуальної власності та юридичної відповідальності Інтернет-провайдерів у разі вчинення правопорушень у глобальній мережі. В практиці ЄСПЛ суб'єктивні особисті немайнові права особи нерідко пов'язані між собою. Це простежується зокрема у прецедентній практиці Суду щодо права на приватність, яке є складним за своїм змістом.

Необхідно відразу зазначити, що до справ, які розглядаються ЄСПЛ стосовно використання Інтернету та інших технологій, можуть застосовуватися загальні принципи та критерії, встановлені давнішими рішеннями Суду, які стосуються інших питань. Конвенція не містить окремого посилання на права людини в Інтернеті, охоплюючи будь-яку діяльність у цифровому просторі «класичними» правами людини — правом на свободу слова, правом на приватність, на доступ до інформації, на свободу мирних зібрань тощо.

Останнім часом у наукових колах та серед правозахисників ведеться активна дискусія щодо можливості виокремлення права на доступ до Інтернету в самостійне право людини. Певним результатом цієї дискусії є формальне визнання права на доступ до Інтернету одним з прав людини на міжнародному рівні. 16 травня 2011 року на 17-й сесії Комісії з прав людини Генеральної Асамблеї ООН було представлено звіт спеціального доповідача з питань заохочення

267. Internet: case law of the European Court of Human Rights, 2011 [Електронний ресурс]. – Режим доступу: http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.

і захисту права на свободу думок і їх вираження Франка Ла Рю. В цьому звіті зазначено: «Інтернет є одним з найпотужніших інструментів у 21 столітті для покращення прозорості у здійсненні доступу до інформації, а також для сприяння активній участі громадян у будівництві демократичного суспільства. Дійсно, нещодавня хвиля демонстрацій у країнах Близького Сходу та Північної Африки засвідчила ключову роль, яку Інтернет може відігравати в мобілізації населення, щоб закликати до справедливості, рівності, підзвітності влади та поваги до прав людини. Таким чином, полегшення доступу до Інтернету для всіх людей, з мінімальним обмеженням до онлайн-контенту, наскільки це можливо, повинно бути пріоритетом для всіх держав»²⁶⁸.

Поряд з іншими базисними правами людини, такими, як право на життя, право на свободу та особисту недоторканність, право на справедливий судовий розгляд, Конвенція захищає право на повагу до приватного і сімейного життя (ст. 8). Отже, згідно зі ст. 8 Конвенції: кожен має право на повагу до його приватного і сімейного життя, до житла і до таємниці кореспонденції.

Держава не може втручатися у здійснення цього права інакше, ніж згідно із законом і коли це необхідно в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або з метою захисту прав і свобод інших осіб.

Зазначена норма містить чотири елементи права на приватне та сімейне життя:

1. право на повагу до приватного життя;
2. право на повагу до сімейного життя;
3. право на недоторканність житла;
4. право на недоторканність кореспонденції.

268. La Rue F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2011 [Електронний ресурс] / Frank La Rue. – Режим доступу: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

Вказані вище елементи значною мірою пов'язані між собою. Тому в нормативних актах як міжнародного, так і вітчизняного законодавства, зазначені поняття не завжди чітко розмежовуються. Наприклад, в ч.1 ст. 32 Конституції України зазначено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України²⁶⁹.

Право на повагу до приватного життя є найширшим та найбільш невизначеним за своєю природою. Приватне життя — дуже тонка категорія, оскільки кожен наповнює її своїм змістом, визначає згідно зі своїми звичками, моральними цінностями та інтересами. Сама сутність цього поняття полягає в приватності, індивідуалізмі та особистому характері окремих аспектів життя людини. Визнання права на повагу до приватного життя є необхідною умовою функціонування цивілізованого суспільства, в якому людина, її інтереси та індивідуальність становлять основну та найважливішу цінність держави. Саме на цій підставі ЄСПЛ принципово не дає чітко визначеного поняття терміна «приватне життя», оскільки вважає за необхідне тлумачити його залежно від кожної конкретної ситуації.

Конституційний Суд України (далі — КСУ) у своєму рішенні № 2-рп/2012 від 20.01.2012 підтримує позицію ЄСПЛ, зазначаючи, що «неможливо визначити абсолютно всі види поведінки фізичної особи у сферах особистого та сімейного життя, оскільки особисті та сімейні права є частиною природних прав людини, які не є вичерпними, і реалізуються в різноманітних і динамічних відносинах майнового та немайнового характеру, стосунках, явищах, подіях тощо. Право на приватне та сімейне життя є засадничою цінністю, необхідною для повного розквіту людини в демократичному суспільстві, та розглядається як право фізичної особи на автономне буття незалежно від держави, органів місцевого самоврядування, юридичних і фізичних осіб»²⁷⁰.

269. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

270. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої

Такий гнучкий підхід до визначення приватності має істотне значення в епоху розвитку інформаційних технологій, адже способи здійснення права на особисте життя знаходяться у постійному розвитку.

Наприклад, у своєму рішенні у справі *Niemietz v Germany (1992)* Суд вказав на розширене тлумачення поняття житла особи, включаючи до нього також робочі приміщення у відповідних випадках. Згідно з рішенням Суду, особливих підстав для вилучення з поняття «особисте життя» професійних відносин немає. Особливо у випадках, коли особа має гуманітарний профіль, і її робота стає невід’ємною частиною життя такою мірою, що може унеможливити визначення, в якій якості вона діє в конкретний момент часу²⁷¹. Цю справу також застосовують і до електронного листування та даних про пошукову активність користувачів Інтернету, що здійснюються з робочого приміщення особи²⁷². Зокрема, безпосередньо Інтернету стосується справа *Copland v. the United Kingdom (2007)*²⁷³. Заявниця була найманою працівницею в державній освітній установі (коледжі), займаючи посаду помічника директора. Протягом певного часу її телефонні розмови та діяльність у мережі піддавалися стеженню з боку директора з метою встановлення добросовісності використання цих технічних засобів. Діяльність заявниці в Інтернеті цікавила директора в аспекті адрес електронної пошти, що використовувалися для листування, адрес веб-сайтів, а також тривалості та конкретного часу їх відвідування заявницею тощо. Держава виступила відповідачем у цій справі, визнаючи свою відповідальність перед громадянами за державну освітню установу. Як зазначається в рішенні Суду, логічно, що електронні листи, відправлені з роботи, повинні бути захищені відповідно до статті 8 Конвенції, як і інформація, отримана в ході використання Інтернету в особистих цілях.

статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 [Електронний ресурс]. – Режим доступу: <http://www.ccu.gov.ua/uk/doccatalog/list?currDir=167724>.

271. *Niemietz v Germany*, judgement of 16 December 1992 [Електронний ресурс] – Режим доступу: <http://cmickp.echr.coe.int/>.

272. *Ibis*, n. 3, p. 8

273. *Copland v. the United Kingdom* [Електронний ресурс]. – Режим доступу: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996#%22itemid%22:%22001-79996%22> }

В наведеному рішенні КСУ зазначає: інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною. Тобто, будь-яка інформація, окрім пов'язаної із службовими повноваженнями представників державної влади, має захищатися правом на приватність.

ЄСПЛ також наголошує на тому, що «було б неможливо обмежити поняття приватного життя «внутрішнім колом», у якому може жити окрема людина своїм особистим життям, яке вона обирає, та цілком виключити звідти зовнішній світ, який не входить до цього кола. Повага до приватного життя повинна також включати визначений набір прав для встановлення та розвитку взаємовідносин з іншими аспектами життя людини»²⁷⁴.

Таким чином, виокремлюють два блоки зазначеного права: внутрішній та зовнішній. До внутрішнього кола відносять «сферу життєдіяльності людини, яку вона формує самостійно, без участі інших осіб, та в якій відчуває себе самодостатньою»²⁷⁵. Зовнішнє коло приватного життя — це відносини людини з суспільством та його членами.

Внутрішнє коло приватного життя складається особисто людиною, ніхто не причетний до цієї сфери її діяльності, тому єдине, що може та повинно бути врегульовано нормами права, — це *таємниця* приватного життя. Саме впевненість особи в таємниці її особистих уподобувань, інтимних, суто персональних цінностей дає їй змогу повноцінно розкривати свою сутність як індивіда. За таких обставин важливим аспектом поваги до приватного життя особи є недопустимість неправомірного збирання та використання інформації про неї.

274. *Ibis*, n. 7.

275. Серегин В.А. Право на уважение личной жизни в решениях Европейского суда по правам человека. - 2005 [Електронний ресурс] / В. А. Серегин. - Режим доступу: www.confcourt.net.

Ст. 1 Закону України «Про інформацію»²⁷⁶ визначає її як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. В ч.ч. 2, 3 ст. 32 Конституції України закріплено правило, згідно з яким не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Ця норма Основного Закону цілком відповідає положенню ч. 2 ст. 8 Конвенції, яка допускає втручання в сферу приватного життя людини тільки з надзвичайно поважних причин, необхідних для забезпечення національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або з метою захисту прав і свобод інших осіб.

Законодавство України деталізує положення зазначеної норми вітчизняної Конституції в численних спеціальних нормах різних галузей права. Так, у ст. 301 Цивільного кодексу України (далі – ЦК України) зазначено: «Фізична особа має право на особисте життя. Фізична особа сама визначає своє особисте життя і можливість ознайомлення з ним інших осіб. Фізична особа має право на збереження у таємниці обставин свого особистого життя. Обставини особистого життя фізичної особи можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що підтверджено рішенням суду»²⁷⁷.

В ч. 1 ст. 302 ЦК України зафіксоване правило, згідно з яким збирання, зберігання, використання і поширення інформації

276. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ. Відомості Верховної Ради України (ВВР), 1992 р., № 48, ст. 650.

277. Цивільний кодекс України від 16.01.2003 № 435-IV. Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356.

про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Колись, за часів зародження Інтернету та початку його широкого використання, існував міф анонімності користувачів мережі та їх будь-яких дій. Сьогодні очевидним є фактично протилежне: із потраплянням інформації про особу до мережі вона стає легкодоступною широкому колу осіб, навіть у разі обмеження доступу до неї. Це відзначається, зокрема, у звіті ЄСПЛ щодо справ стосовно Інтернету: «Як тільки приватна або особиста інформація була опублікована в Інтернеті, така, як ім'я та особистість людини, потреба у захисті її конфіденційності більше не може мати домінуюче значення. Інформація здебільшого вже практично не є конфіденційною (справа *Editions Plon v. France*)²⁷⁸.

Однак, прецедентна практика ЄСПЛ показує, що згідно з Конвенцією можна і потрібно захищати право особи на приватність, якщо це не перешкоджає здійсненню суб'єктами інших особистих прав.

Право на особисте зображення особи. За умов розповсюдженого користування електронними відео-сервісами та соціальними мережами важливою є практика ЄСПЛ щодо використання зображення фізичних осіб в Інтернеті. Цю практику можна поєднати із законодавством України. Гарантією забезпечення поваги до особистого життя особи є положення ст. 307 ЦК України, відповідно до якої фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку припускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру.

У справі *Peck v. the United Kingdom* (2003), яку розглядав ЄСПЛ, заявник, який страждав від депресії, скаржився на розповсюдження в ЗМІ кадрів із прихованої зйомки ССТV камерою, встановленою

на вулиці, яка зафіксувала, як він ішов вулицею, один, з кухонним ножом у руці (він намагався перерізати собі зап'ястя, але кадри відеоспостереження не показали цього). Це морально дуже зашкодило заявникові. Кадри були інтерпретовані як спроба скоєння злочину. Він також скаржився на відсутність ефективного засобу правового захисту у цьому зв'язку. Суд встановив, що розкриття кадрів муніципальною радою не супроводжувалося достатніми гарантіями, що було скоєно неспіврозмірне і невиправдане втручання в приватне життя заявника²⁷⁹. Цю справу можна застосовувати щодо питань «публікації матеріалів, отриманих у публічних місцях шляхом або у ступені, що не могли бути передбачені заздалегідь»²⁸⁰.

Таким чином, Закон забезпечує право особи самій визначати, які саме моменти та аспекти її життя є приватними. Навіть якщо ця особа демонструє деякі сторони своєї діяльності, все одно за нею залишається право вимагати нерозповсюдження інформації, яка становить, на її погляд, таємницю приватного життя.

Ч. 3 ст. 307 ЦК України містить правило, згідно з яким знімання фізичної особи на фото-, кіно-, теле чи відеоплівку, в тому числі таємне, без згоди особи, може бути проведене лише у випадках, встановлених законом.

Необхідно зазначити, що вказані норми поряд із захистом таємниці приватного життя особи містять гарантії захисту інших осіб від неправомірної поведінки суб'єктів, яким належить ця таємниця. Тобто, особа захищається законом тільки у випадку, якщо вона не ставить за мету заподіяти шкоду іншим людям чи інтересам держави або суспільства. Так, ст. 23 Конституції України закріплює правило, згідно з яким кожна людина має право на вільний розвиток своєї особистості, якщо при цьому не порушуються права і свободи інших людей, та має обов'язки перед суспільством, в якому забезпечується вільний і всебічний розвиток її особистості.

279. ECHR Factsheet – Right to the protection of one's image [Електронний ресурс] – Режим доступу: http://www.echr.coe.int/Documents/FS_Own_image_ENG.pdf.

280. *Ibis*, n. 3, p. 7.

Право на власне зображення як таке також охоплюється поняттям права на повагу до приватності особи. Зокрема, це простежується в рішенні ЄСПЛ у справі *Sciacca v. Italy* (2005)²⁸¹. Справа стосується розповсюдження в ЗМІ фотографії заарештованої особи у зв'язку із висвітленням процесу розслідування, що було визнано Судом втручанням у приватне життя згідно зі статтею 8 Конвенції.

І все ж, повноваження державних органів щодо втручання в особисте життя людини є досить широкими, чітко не встановленими законом, що вказує на не досить повну захищеність особи та її приватності. Держава залишає за собою право тлумачити поняття «необхідності» в кожному конкретному випадку на свій розсуд. Певною мірою це відповідає практиці ЄСПЛ. Так, Н. Раданович наголошує на важливості врахування практики ЄСПЛ в процесі тлумачення норм зазначеної Конвенції: «не виключена ситуація, коли національний суддя звернеться до Пленуму Верховного Суду України за роз'ясненням поняття «необхідний у демократичному суспільстві». І тоді Пленуму Верховного Суду стане у пригоді позиція Суду щодо цього питання. Вона простежується, наприклад, у рішенні по справі *Олсон проти Швеції* від 24 березня 1988 р. «Згідно з прецедентами Суду, поняття необхідності припускає, що втручання держави відображає гостру суспільну потребу і, зокрема, що воно співрозмірне з переслідуваною законною метою, встановлюючи, чи є втручання необхідним у демократичному суспільстві, Суд буде враховувати, що державі залишена деяка свобода «на розсуд»²⁸². «Свобода на розсуд», однак, не означає свавілля посадових осіб у здійсненні ними своїх повноважень. Рішення ЄСПЛ демонструють саме ту грань між інтересами суспільства (при здійсненні професійної діяльності правоохоронними органами і журналістами) та правом на повагу до приватності людини.

Важливо звернути увагу на особливу роль, яку відведено ЄСПЛ

281. *Sciacca v. Italy* [Електронний ресурс]. – Режим доступу: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-67930#%7B%22itemid%22:%5B%22001-67930%22%5D%7D>.

282. Раданович Н. Міжнародно-судові засоби імплементації Європейської Конвенції про захист прав людини і основних свобод [Електронний ресурс] / Н. Раданович. – Режим доступу: www.humanrights.gov.ua/.

захисту прав неповнолітніх у зв'язку із використанням Інтернету. Особливе місце в опосередкуванні відносин між користувачами мережі посідають Інтернет-провайдери. Забезпечення інтересів неповнолітніх має бути покладено на них у зв'язку з наявністю технічної можливості встановлення певних перешкод для розповсюдження інформації образливого характеру або такої, що шкодить психіці неповнолітніх осіб. Зокрема, в рішенні Суду у справі *K.U. v. Finland (2008)* наголошується на певних аспектах застосування ст. 8 Конвенції стосовно таких випадків. Справа стосується використання фотографії 12-річного хлопчика у рекламі веб-сайту знайомств, яке невідома особа розмістила в Інтернеті без відома цього хлопчика та його батьків, із зазначенням контактної інформації. Після отримання електронного листа від дорослого чоловіка на адресу хлопчика — його батько вимагав від Інтернет-провайдера надати інформацію про особу правопорушника, який розмістив наведені дані на веб-сайті. За фінським законодавством, чинним на той момент, поліція або суди не могли зобов'язувати Інтернет-провайдерів ідентифікувати особу, яка здійснювала розміщення реклами в Інтернеті. Зокрема, провайдер відмовився видати інформацію про особу, що розмістила зазначену рекламу в Інтернеті, вважаючи, що пов'язаний конфіденційністю з клієнтом телекомунікаційних послуг. Цю позицію провайдера підтримав місцевий суд. Однак ЄСПЛ дійшов висновку: хоча ст. 8 Конвенції покликана охороняти осіб від втручання в особисте життя державними органами, держава має надати гарантії для захисту прав неповнолітніх осіб при використанні Інтернету, зважаючи на їх психологічну вразливість, зумовлену малим віком²⁸³.

До складових права на приватне життя людини, його зовнішнього кола, входить поняття права на *захист честі, гідності та ділової репутації особи*.

Відповідно до ч.4 ст. 32 Конституції України кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації,

283. *K.U. v. Finland* [Електронний ресурс]. – Режим доступу: <http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/K.U.%20v.%20FINLAND%20en.pdf>.

а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації. Згідно зі ст. 297 ЦК України кожен має право на повагу до його гідності та честі. Гідність та честь фізичної особи є недоторканими. Фізична особа має право звернутися до суду з позовом про захист її гідності та честі. Згідно зі ст. 299 ЦК України фізична особа має право на недоторканність своєї ділової репутації. Фізична особа може звернутися до суду з позовом про захист своєї ділової репутації.

Закон не дає чіткого визначення честі, гідності та ділової репутації, тому в судовій практиці ці поняття тлумачаться по-різному, а іноді застосовуються як тотожні, що призводить до проблем при їх застосуванні²⁸⁴.

Стосовно питання захисту честі, гідності та ділової репутації Пленумом Верховного Суду України було прийнято Постанову «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» № 1 від 27 лютого 2009 року. Також є досі чинною Постанова ПВСУ «Про судову практику в справах про відшкодування моральної (немайнової) шкоди» № 4 від 31 березня 1995 року (в редакції від 27 лютого 2009 року).

Зважаючи на широке розповсюдження електронних ЗМІ, а також технічну можливість висловлення будь-яких особистих думок в Інтернеті, важливого значення набуває практика ЄСПЛ щодо дифамації (наклепу). Цікавим є рішення Суду у справі *Editorial Board of Pravoye Delo and Shtekel v. Ukraine (2011)*²⁸⁵. Ця справа стосується повторного опублікування анонімного тексту, що містив наклеп. Газета «Правое Дело» виходила друком в Одесі, нерідко повторно публікуючи інформацію з Інтернету, на тему місцевої

284. Луспенік Д. Д. Практика вирішення судами справ про захист честі, гідності, ділової репутації: проблемні питання та шляхи їх вирішення (за матеріалами узагальнення судової практики судів Харківської області) / Д. Д. Луспенік. // Адвокат. – 2003. – №5. – С. 2–14.

285. Editorial Board of Pravoye Delo and Shtekel v. Ukraine [Електронний ресурс]. – Режим доступу: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-104685#%7B%22item%22:%5B%22001-104685%22%5D%7D>].

політики та державного управління. Одним з таких матеріалів стала анонімна замітка про корупцію та зв'язки з кримінальними угрупованнями представників обласного управління служби безпеки. Цей текст був завантажений заявником з Інтернету, в газеті його було супроводжено посиланням на першоджерело із зазначенням непричетності редакції газети до тексту. В результаті цього повторного опублікування заявник був підданий відповідальності у вигляді штрафу та зобов'язаний опублікувати спростування наклепницької інформації.

Рішення у цій справі є першим з прецедентної практики Суду, в якому ЄСПЛ дійшов висновку, що стаття 10 Конвенції (свобода слова) має бути розтлумачена як така, що встановлює *позитивне зобов'язання* держави створити регулятивну базу для забезпечення ефективного захисту свободи журналістів на самовираження в Інтернеті. На думку Суду, українське законодавство не містило захисту для журналістів щодо повторного опублікування контенту з Інтернету. На додаток до цього, національні суди відмовилися застосовувати до цієї ситуації норми, які забезпечують захист для друкованих ЗМІ²⁸⁶.

Ця справа, поряд із іншими, демонструє послідовний захист ЄСПЛ права на свободу слова та його значимість у випадках конкуренції з правом на приватність. Як таке право на свободу слова в цьому разі потребувало захисту в зв'язку із наявністю суспільного інтересу та розширеного кола можливостей критики представників державних органів у зв'язку з їх повноваженнями. На це звертається увага, зокрема, у таких справах як *Sürek v. Turkey*²⁸⁷ та *Willem v. France*²⁸⁸.

Право на недоторканність житла.

У світлі Конвенції право на недоторканність житла охоплює насамперед право безперешкодного доступу та перебування в ньому, а також право не бути виселеним. Крім того, це право включає

286. *Ibis*, п. 3, р. 12.

287. *Sürek v. Turkey* [Електронний ресурс]. – Режим доступу: [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58279#{%22itemid%22:\[%22001-58279%22\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58279#{%22itemid%22:[%22001-58279%22]}).

288. *Willem v. France* [Електронний ресурс]. – Режим доступу: [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=003-2803253-3069793#{%22itemid%22:\[%22003-2803253-3069793%22\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=003-2803253-3069793#{%22itemid%22:[%22003-2803253-3069793%22]}).

захист від втручання з боку державних органів (арешт, обшук). У разі порушення цього права особи держава повинна мати вагомі підстави, які виправдовували б її дії²⁸⁹.

З цієї позиції можна зробити висновок, що зазначене право включає два аспекти: право на повагу до житла та право на недоторканність житла. Право на повагу до житла забезпечує реалізацію особою права на особисте життя, внутрішнього кола, коли житло особи виконує функцію «захисту» від суспільства. Право на недоторканність житла є гарантією неприпустимості неправомірного втручання в приватне та сімейне життя особи з боку державних органів. Згідно зі ст. 311 ЦК України житло фізичної особи є недоторканим. Проникнення до житла чи до іншого володіння фізичної особи, проведення в ньому огляду чи обшуку може відбутися лише за вмотивованим рішенням суду.

Конституція України гарантує кожному право на недоторканність житла в ст. 30. *Поняття житла* міститься в Цивільному кодексі в ст. 379: житлом фізичної особи є житловий будинок, квартира, інше приміщення, призначені та придатні для постійного проживання в них.

Повертаючись до справи *Niemietz v. Germany* з метою тлумачення норм Конвенції, необхідно зазначити, що термін «житло» має більш широке значення, ніж це закріплено в національному законодавстві. Так, у цій справі предметом оскарження стали дії німецьких органів влади, які здійснили обшук в офісі заявника, адвоката за фахом. Представники державних органів Німеччини заперечували проти скарги, посилаючись на те, що ст. 8 Конвенції не захищає від обшуку адвокатської контори та проводить чітку грань між приватним життям та житлом особи, з одного боку, й професійним життям та службовим приміщенням, з іншого боку. Проте, Суд у своєму рішенні зазначив, що принципівих підстав для вилучення професійних відносин з поняття «приватне життя» немає. Особливо у випадках,

289. Огляд практики Європейського Суду з прав людини. Норми та стандарти Конвенції про захист прав і основних свобод людини., 2002. – (Міністерство юстиції України). - С. 27-32.

коли особа має гуманітарний фах, її робота в такому контексті може стати невід'ємною частиною її життя настільки, що унеможливує визначення того, в якості кого вона діє на конкретний момент часу [9].

З цього приводу цікавим є рішення ЄСПЛ у справі *Nagla v. Latvia (2013)*²⁹⁰. Справа стосується обшуку, проведеного поліцією вдома у відомої журналістки, та здійснення вилучення носіїв електронної інформації. В домівці заявника був проведений обшук після трансляції нею в ефір у лютому 2010 року повідомлення про виток інформації з бази даних Служби державних доходів. Заявник скаржився, що обшук її будинку означав примус розкрити інформацію, що дозволила ідентифікувати журналістське джерело, порушивши її право на отримання і поширення інформації. Суд визнав наявність порушення права на свободу слова (стаття 10 Конвенції), поряд із пов'язаними відносинами щодо приватності особи, адже обшук було проведено в її особистій резиденції. На думку Суду, в цьому випадку слідчі органи не змогли належним чином збалансувати інтереси слідства в забезпеченні доказів у суспільному інтересі та захист свободи журналіста на самовираження.

Право на недоторканність кореспонденції. Основний Закон України гарантує кожному таємницю листування, телефонних переговорів, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинів чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо (ст. 31).

Європейський Суд з прав людини вважає, що телефонні розмови, в тому числі ділові та зроблені з робочого телефону, захищаються від неправомірного втручання статтею 8 Конвенції (як зазначалося у наведених вище справах).

Згідно з ч.1 ст. 306 ЦК України фізична особа має право на

290. Nagla v. Latvia. ECHR Factsheet – New technologies [Електронний ресурс]. – Режим доступу: http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції.

У своїх рішеннях ЄСПЛ нерідко підкреслює різний характер інформації про приватних осіб та про публічних осіб, зокрема представників влади. Це питання має вираження у рішеннях Суду про доступ громадськості до інформації. Стосовно інформаційних відносин з електронним елементом цікавою є нещодавня справа *Youth Initiative For Human Rights v. Serbia (2013)*²⁹¹. Справа стосується доступу до інформації, отриманої за допомогою електронного спостереження розвідувальним управлінням Сербії. Заявник (неприбуткова організація) скаржився, що відмова розвідувального управління забезпечити їх інформацією про те, як багато людей зазнали електронного спостереження в 2005 році, перешкоджає його можливості виконання своєї функції «сторожового пса громадськості». Суд постановив, що мало місце порушення статті 10 Конвенції (свобода слова).

У випадках необхідності доступу до інформації представниками державних органів влади, згідно з їх законними повноваженнями, особи не можуть застосовувати ст. 8 Конвенції для уникнення такого розкриття інформації. Зокрема, у справі *Bernh Larsen Holding As and Others v. Norway (2013)*²⁹² ЄСПЛ не знайшов порушення права на приватність за ст. 8 Конвенції у діях податкових органів держави. Ця справа стосувалася скарги трьох норвезьких компаній про рішення податкових органів, які на замовлення податкових аудиторів повинні були надати копії всіх даних на комп'ютері сервера, що використовувався спільно трьома компаніями. Суд постановив, що не було порушення статті 8 Конвенції. Він погодився з аргументом держави, що, з міркувань ефективності норвезькі суди не повинні обмежувати повноваження податкових органів у зв'язку із тим, що

291. *Youth Initiative For Human Rights v. Serbia* [Електронний ресурс]. – Режим доступу: [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-120955#{%22itemid%22:\[%22001-120955%22\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-120955#{%22itemid%22:[%22001-120955%22]}).

292. *Bernh Larsen Holding As and Others v. Norway* [Електронний ресурс]. – Режим доступу: [http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-117133#{%22itemid%22:\[%22001-117133%22\]}](http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-117133#{%22itemid%22:[%22001-117133%22]}).

платник податків використав «змішаний архів» (тобто спільний для трьох компаній рахунок), навіть якщо цей архів містив дані, що належать іншим платникам податків.

Захист персональних даних. До важливих подій у законодавчій площині права на приватність необхідно віднести прийняття Верховною Радою України Закону «Про захист персональних даних» від 1 червня 2010 року. Логічно пов'язаний із ратифікацією Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру (Страсбург, 28 січня 1981 року)²⁹³, цей Закон покликаний заповнити прогалину в сфері регулювання відносин, що виникають з приводу персональної інформації. Реакція фахівців на зміст зазначеного Закону є неоднозначною. Однак, не викликає сумнівів, що факт прийняття закону, за допомогою якого мають регулюватися відносини щодо персональних даних осіб в Україні, є надзвичайно важливим. Особливого значення в ракурсі розвитку підходів до адекватного захисту персональних даних в Україні набуває практика ЄСПЛ.

Зважаючи на зростання ролі електронних баз даних, у тому числі й у правоохоронній та оперативно-розшуковій діяльності, цікавою є практика ЄСПЛ щодо зберігання інформації про особу в електронному вигляді. Зокрема, у справі трьох заявників *V.V. v. France, Gardel v. France and M.V. v. France (2006)* заявниками були особи, засуджені за зґвалтування неповнолітніх особами, наділеними владними повноваженнями. Ці заявники заперечували проти включення даних про них до національної бази даних про осіб, що вчинили статеві злочини. Однак ЄСПЛ дійшов висновку про відсутність втручання в право на приватність, зазначивши, що строк зберігання таких даних протягом 30 років не був диспропорційним меті попередження нових злочинів²⁹⁴.

До права на приватне життя ще входить велика кількість елементів, які виокремлюються згідно з практикою ЄСПЛ. Так, виділяють

293. *Ibis*, п. 9.

294. ECHR Factsheet - Data protection [Електронний ресурс]. – Режим доступу: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

право на можливість особи визначати свою персональну ідентичність; право особи на моральну та фізичну цілісність; право на приватний простір; свободу інтимних стосунків та ін. Проте в національному законодавстві такий детальний підхід до цієї проблеми не знайшов свого відображення.

Право інтелектуальної власності. Зважаючи на значиму роль права інтелектуальної власності у регулюванні відносин щодо використання Інтернету, ЄСПЛ також розглядає справи, що стосуються використання результатів інтелектуальної діяльності. Однак ці справи зустрічаються рідко, адже відносини інтелектуальної власності зазвичай мають суто приватноправову або адміністративно-правову природу. Проте відносини інтелектуальної власності підпадають під дію статті 1 Протоколу № 1 до Конвенції. Згідно з цією статтею:

«Кожна фізична або юридична особа має право мирно володіти своїм майном. Ніхто не може бути позбавлений свого майна інакше як в інтересах суспільства і на умовах, передбачених законом або загальними принципами міжнародного права.

Проте попередні положення жодним чином не обмежують право держави вводити в дію такі закони, які, на її думку, є необхідними для здійснення контролю за користуванням майном відповідно до загальних інтересів або для забезпечення сплати податків чи інших зборів або штрафів».

Хоча, в законодавстві та правничій науці України домінує ставлення до прав інтелектуальної власності як до об'єктів виключних прав, а не права власності, факт ратифікації Україною зазначеного Протоколу № 1 до Конвенції дозволяє застосовувати прецедентну практику ЄСПЛ до відносин щодо результатів інтелектуальної діяльності у справах, що стосуються суспільного інтересу. Аналітики вирізняють дві групи справ щодо використання об'єктів права інтелектуальної власності в Інтернеті, що стали предметом розгляду Суду:

- 220 1) майнові права (до них, зокрема, відносять права на торговельні марки, заявки на реєстрацію торговельної марки, ліцензування

послуг Інтернет-провайдерів, виключні права використовувати та розпоряджатися зареєстрованими доменними адресами в Інтернеті);

2) особисті (немайнові) права²⁹⁵.

Досить цікавою є справа щодо доменного імені та прав на торговельну марку, розглянута ЄСПЛ на зазначених засадах забезпечення суспільного інтересу в суто комерційних відносинах. Так, справа *Raeffgen GmbH v. Germany (2007)* стосувалася претензій до компанії-заявника, яка була залучена до електронної комерції, від третіх осіб. Ці треті особи стверджували, що використання заявником зареєстрованого доменного імені порушувало їхні права інтелектуальної власності на торговельні марки. ЄСПЛ дійшов висновку про справедливість вимоги судів про скасування доменного імені заявника у зв'язку з порушенням ним прав на торговельні марки, оскільки такі вимоги (про скасування) сприяли встановленню балансу між інтересами володільців майнових прав [власності] та інтересів громадськості²⁹⁶.

Підбиваючи підсумки, можна сказати, що суб'єктивні цивільні права особи певною мірою гарантовані законодавством України. Питання можуть виникати в практиці застосування норм закону державними органами та в процесі тлумачення ними цих норм. За таких обставин важливим є врахування практики ЄСПЛ в процесі тлумачення норм національного законодавства та положень Конвенції.

Необхідно також зазначити, що з метою підвищення ефективності застосування міжнародно-правових, зокрема європейських стандартів у галузі прав людини на території України, вітчизняним суддям треба частіше посилатись на них, постійно підкреслюючи гарантованість тих чи інших прав людини. Необхідно виховувати культуру застосування норм міжнародного законодавства поряд з національними нормами закону. За таких умов рух у напрямку Європи стане більш впевненим та природним для України.

295. *Ibis*, n. 3, p. 18-19.

296. *Raeffgen GmbH v. Germany* [Електронний ресурс]. – Режим доступу: [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-82671#%22itemid%22:\[%22001-82671%22\]](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-82671#%22itemid%22:[%22001-82671%22])}.

РОЗДІЛ IV

РЕФОРМУВАННЯ СФЕРИ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

14. Організаційно-правове забезпечення національної інформаційної безпеки: шляхи вдосконалення[©]

Кінець ХХ ст. залишається в пам'яті людства добою надій на «кінець історії» (Фр. Фукуяма) і пошуків відповіді на питання, чи призначено втілитися в життя мрії про «абсолютну» безпеку сучасного світу, про вільний політико-економічний і соціокультурний обмін між його відкритими локальними складовими в єдиному інформаційно-культурному просторі.

На початку ХХІ ст. світовий розвиток характеризується структурною інтеграцією ринків і економік, функціональною уніфікацією всіх сфер людської діяльності, у результаті чого спостерігається системний перехід усього суспільства в нову якість, характеризовану в термінах «інформаційного суспільства», попри всю неоднозначність як самого терміна, так і його тлумачень²⁹⁷.

Показові науково-аналітичні концепти, що належать Е. Тофлеру (знання як підстава влади, що прийшло на зміну силі та багатству), Ф. Лорда-і-Алайсу (інформаційна влада), Б. Барнсу (влада як здатність поширювати соціальне знання) та іншим дослідниками, де інформація, знання, досвід ототожнюються із владою, а влада розглядається як комунікація. Е. Тофлер виокремлює як принципову таку фундаментальну підвалину сучасних демократій, як свобода

297. Для опису характерних особливостей сучасних соціальних реалій використано дуже поширений термін «інформаційне суспільство» (М. Кастельс, П. Хіманен). Однак, поруч із ним для опису сучасних суспільних реалій активно використовуються також такі терміни як «індустріальне суспільство» (Р. Арон), «відкрите суспільство» (К. Поппер), «суперіндустріальне суспільство» (Е. Тофлер), «технотронне» (Зб. Бжезинський) та інші. Маючи на увазі більшменш те саме, кожне з подібних визначень зазвичай висвітлює той бік складної проблеми окреслення реалій, на якому робить акцент або якому принаймні приділяє основну увагу автор такого визначення. Так, наприклад, Дж. Белл поруч із терміном «інформаційне суспільство» використовує термін «постіндустріальне суспільство».

інформації. Закритість інформації властива репресивним режимам та корумпованим суспільствам. Свобода інформації тісно пов'язана з поняттям «свобода самовираження» особистості. А регулювати ці взаємини, на думку Е. Тоффлера, мусить інформаційна етика.

Зміни, що викликаються масштабними процесами, носять глибинний характер і торкаються всіх сфер життєдіяльності, ставлять завдання приведення до відповідності соціально-політичних параметрів розвитку суспільства, вдосконалення його економіко-політичної структури, технологій державно-політичного управління саме у фокусі інформаційного виміру осмислення та опанування реалій сьогодення. Адже комп'ютери, як відзначав відомий західний дослідник Д. Несбітт, збільшують реальну владу кожного індивіда, дозволяючи йому більш ефективно стежити за діями свого уряду, навіть більше, ніж уряд може стежити за діями громадянина.

Інформаційна безпека України: політико-правова (структурна) та соціально-гуманітарна (функціональна) складові. Із проголошенням України незалежною державою в офіційних документах, науковій літературі та засобах масової інформації категорія «національна безпека» стала досить широко розповсюдженою. Було осмислено її загальні положення і принципи, сформульовано основні напрями проведення державної політики національної безпеки. Так, у ст. 17. Конституції України зазначається: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу».

Зараз особливої актуальності набуває науковий аналіз національної безпеки як складного та багатоаспектного феномена, що забезпечує ефективну діяльність соціальних інститутів національного і міжнародного рівнів щодо підтримки стабільних умов існування й розвитку українського суспільства. Ключовою складовою цього феномена є саме «національна інформаційна безпека».

Домінуючий в сучасній українській науці підхід тлумачить безпеку

як «рівень захищеності життєво важливих інтересів людини, а також суспільства, держави, довкілля від реальних або потенційних загроз, що їх створюють антропогенні чи природні чинники». При цьому «розрізняють воєнну, екологічну, економічну, інформаційну, пожежну, політичну, продовольчу, радіаційну, соціальну, технічну, транспортну, фінансову, ядерну безпеку». Крім того, «важливий чинник політики будь-якої держави — національна безпека»²⁹⁸.

Українські дослідники-безпекознавці (О. Бодрук, В. Горбулін, О. Литвиненко, Г. Перепелиця та ін.) відзначають, що, з одного боку, поняття «національна безпека» стало невід'ємним атрибутом більшості воєнно-політичних концепцій, аналітичних та прогностичних розробок довгострокового, глобального характеру. З іншого боку, їй досі немає чітких, загальновизнаних дефініцій понять «національна безпека» та «інформаційна безпека», і до того ж розбіжності між науковими школами та окремими дослідниками достатньо суттєві.

Львівська дослідниця А. Колодій аналізувала безпекові аспекти національної єдності та патріотизму, виходячи «з розуміння національної безпеки як *здатності суспільства запобігати і протидіяти внутрішнім та зовнішнім загрозам* його функціонуванню і розвитку. Така здатність визначається, окрім усього іншого, рівнем єдності суспільства, сформованості в його межах громадянської національної спільноти з загальною ідентичністю, спільними цінностями та метою»²⁹⁹.

Останнім часом методологічні підходи до визначення ключових понять і категорій основ національної безпеки відповідно до динамічних реалій багатовимірного соціально-політичного контексту змінюється. Простежується, зокрема, тенденція: «під національною безпекою... розуміти необхідний і динамічний стан відносної невразливості держави, який визначає характер взаємодії з зовнішнім

298. Енциклопедія Сучасної України. – К., 2003. – Т.2. – С.385. Пор. Шаповаленко М. Перверсії національної безпеки в умовах політичної трансформації України (деякі теоретичні припущення) // Національна безпека України. – К., 2004. – С.13-23.

299. Колодій А. Національна єдність і патріотизм як чинники національної безпеки // Національна безпека України. – К., 2004. – С.39.

середовищем і забезпечується переважно спільними зусиллями зовнішньополітичних, силових і координаційних державних органів у спосіб використання різних засобів в умовах явного чи прихованого, прямого чи опосередкованого негативного впливу внутрішніх чинників на прийняття рішень у сфері забезпечення життєдіяльності і розвитку держави, а також системи забезпечення її безпеки»³⁰⁰.

Таким чином, доцільно окреслити базову категорію «національна безпека» як ступінь (міру, рівень) захищеності життєво важливих інтересів, прав і свобод особи (громадянина), суспільства (народу, нації) і (національної) держави від зовнішніх та внутрішніх загроз або ступінь (міра, рівень) відсутності загроз правам і свободам людини, базовим інтересам та цінностям суспільства і держави. Відповідно, «національна інформаційна безпека» є однією із ключових складових національної безпеки як такої. Так, у Законі України «Про основи національної безпеки України»³⁰¹ визначено дев'ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності, однією з яких є саме інформаційна.

Відповідно до законодавства України інформаційна безпека — це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди державі через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації»³⁰².

Осмилення феномена «національної інформаційної безпеки» неможливе без відповіді на питання: чиєї безпеки? Адже навіть у найпростішому випадку, розглядаючи «вертикальну» політичну структуру суспільства, можна виділи безпеку держави, безпеку

300. Шипілова Л.М. Порівняльний аналіз ключових понять і категорій основ національної безпеки України: Автореф... к.політ.н. — К., 2007. — С.15.

301. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України (ВВР). — 2003. — № 39. — С.351.

302. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» // Відомості Верховної Ради України (ВВР). — 2007. — № 12. — С. 102.

правлячого угруповання (партії, еліти, владного істеблшменту тощо), безпеку «нації» (народу чи населення) та безпеку окремого громадянина держави. Ці «безпеки» далеко не завжди збігаються й часто суперечать одна одній. Більше того, «молоді демократії» і, зокрема Україна, які знаходяться у стадії транзиту, зазвичай соціально і політично нестабільні. Бажання забезпечити собі «максимум безпеки», які в умовах відсутності загальнонаціонального консенсусу виникають у численних «меншин» (починаючи від лінгво-конфесійних та закінчуючи етнотериторіальними), балансуючи на межі сепаратизму, ставлять під загрозу територіальну цілісність, що є викликом національній безпеці. Сталі демократії зазвичай вдаються до стратегії «преференції в обмін на лояльність» (на прикладі канадського Квебеку: політико-культурна автономія заради збереження унітарності). Натомість «молоді демократії», які, з одного боку, не мають у розпорядженні достатнього ресурсного потенціалу, аби йти на суттєві соціально-економічні поступки (починаючи від реалізації масштабних культурно-гуманітарних та інформаційно-пропагандистських програм і закінчуючи податковими пільгами), а з іншого, досить гостро сприймають соціокультурні загрози (на рівні «мовної експансії» як чинника/загрози «інформаційній безпеці» тощо), як правило, вдаються до примусових чи репресивних заходів із відповідними наслідками.

Національна безпека характеризується певним рівнем інтегрованості. Іншими словами, існує тісний подвійний (прямий та зворотній) взаємозв'язок між такими складовими національної безпеки, як інформаційна та політична чи інформаційна та воєнна. Послаблення одного (практично будь-якого) структурного компонента автоматично означатиме як послаблення національної безпеки в цілому, так і збільшення функціонального навантаження на інші компоненти. Так, наприклад, внутрішньополітична нестабільність має опосередкованим наслідком зменшення фінансово-інвестиційної привабливості держави, що в умовах глобалізації є викликом геоекономічній безпеці держави. З іншого боку, зайве посилення одного компонента (наприклад, воєнного) за рахунок інших (наприклад, інформаційного) матиме

наслідком структурний дисбаланс і, як наслідок, «системну кризу» національної безпеки.

Дещо парадоксально, але національна безпека для різних верств українського суспільства об'єктивно однакова. В її основі знаходиться державна функція захисту своїх громадян, незалежно від їхнього соціального, майнового, національного чи релігійного статусу. Тим самим вона захищає свій національний суверенітет. Однак, із суб'єктивного боку, в цілому не існує єдиного розуміння безпеки, адже кожний суб'єкт, включений у той чи інший спосіб у процеси забезпечення безпеки, відрізняється від інших відповідно до власного становища та бачення проблем безпеки.

Проблеми нормативного регулювання національної безпеки України тісно пов'язані з трансформаціями ціннісних пріоритетів українського суспільства. Реалізація інформаційних прав і свобод людини, одним з яких є своєрідне «право на інформаційну безпеку», залежить від багатьох чинників, зокрема, належних інформаційно-комунікаційних умов, рівня медіа-інформаційного розвитку суспільства, стану інформаційно-правової культури, належної поінформованості особистості.

У державі триває суперечливий процес усвідомлення та формування цілісного уявлення про національну інформаційну безпеку та об'єктивну потребу в її належному забезпеченні на рівні зрілої політичної нації та сучасної демократичної держави. Великою мірою це пов'язано з браком традицій «інформаційної відкритості» та досвіду їх ціннісної реалізації в національній культурі як такої.

Відповідно до чинних законодавчих актів політико-правового характеру базовими суб'єктами забезпечення національної безпеки можна визнати такі інститути як Верховна Рада України; Уповноважений Верховної Ради України з прав людини; Президент України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації та органи місцевого самоврядування; суди; органи прокуратури; військові формування, утворені відповідно до

законів України, та правоохоронні органи (крім тих, які віднесено до суб'єктів спеціальної компетенції).

На нашу думку, інформаційно-безпекова специфіка їх діяльності концентрується у наступному. По-перше, вони визначають засади політики інформаційної безпеки держави, наділені правом прийняття загальних нормативно-правових актів у цій сфері, здійснюють координаційні повноваження, реалізують державну політику щодо забезпечення внутрішньої безпеки у підвідомчих їм сферах. Так, Рада національної безпеки і оборони України 25 травня 2009 р. запропонувала Проект Доктрини інформаційної безпеки України, де виписала визначення поняття інформаційної безпеки, її місця в системі забезпечення національної безпеки України, принципи та способи її реалізації.

По-друге, їх діяльність регулюється багатьма нормативно-правовими актами, положення яких мають різну юридичну силу та ступінь конкретності. Так, кістяк національної нормативно-правової бази щодо забезпечення національної інформаційної безпеки складають профільні Закони України «Про інформацію», «Про захист інформації в автоматизованих інформаційних системах», «Про державну таємницю» та ін., а також ціла низка Указів Президента та Постанов Кабінету Міністрів України, які регулюють конкретні напрями діяльності в галузі забезпечення національної інформаційної безпеки.

По-третє, порядок встановлення та обсяг компетенції таких суб'єктів щодо захисту національної інформаційної безпеки та «національного інформаційного простору»³⁰³ залежать від того, до якої гілки влади належить державний орган, як наслідок їх компетенція обмежується тими стратегічними цілями і тактичними завданнями, заради яких вони створюються. Так, реалізація повноважень Верховної Ради України у сфері інформаційної безпеки здійснюється передусім через її структурні підрозділи, такі як (безпосередньо) комітет з питань свободи слова та інформації, а також (радше

303. Див. Литвиненко О.В., Бінко І.Ф., Потіха В.М. Інформаційний простір як чинник забезпечення національних інтересів України. – К: «Чорнобильінтерінформ», 1998. – 47 с.

опосередковано) комітети з питань національної безпеки і оборони, з питань законодавчого забезпечення правоохоронної діяльності, з питань боротьби з організованою злочинністю і корупцією, з питань законодавчого забезпечення правоохоронної діяльності, у закордонних справах та Уповноваженого Верховної Ради України з прав людини.

По-четверте, діяльність суб'єктів загальнодержавної компетенції щодо забезпечення національної інформаційної безпеки держави завжди ототожнюється з певною мірою самостійності та відособленості окремого органу держави в інформаційно-комунікаційній системі всього апарату держави.

По-п'яте, діяльність цих суб'єктів нормативно спрямована на те, щоб втілити в життя демократичну сутність держави, яка полягає у тому, що держава існує для громадян, а не навпаки. Тобто, держава надає громадянам державні послуги, створює умови для всебічної реалізації їх прав, свобод та законних інтересів.

Зараз існують загальні для всіх демократій базові принципи встановлення місця та ролі «силовиків» у демократичному суспільстві. «Сектор безпеки» має (1) підкорятися утвореному демократичним шляхом легітимному політичному керівництву із цивільними керівниками профільних міністерств та відомств (перш за все — міністрами оборони та внутрішніх справ); (2) додержуватися політичних вказівок керівництва; підкорятися верховенству закону; (3) діяти в рамках своїх конституційних завдань; (4) бути політично нейтральними; (5) не мати доступу до фінансової підтримки, крім державно-бюджетної; (6) контролюватися парламентом, політичним керівництвом, судовою системою та громадянським суспільством у цілому; (7) бути комунікаційно доступним та інформаційно відкритим. Незалежна судова система повинна виключати можливість створення та функціонування спеціалізованих судів поза межами своєї відповідальності на зразок органів військового правосуддя. Окремо стоять повноваження ЗМІ щодо оперативного доступу до безпекової інформації та повноваження Омбудсмена щодо контролю за ситуацією та соціально-психологічними настроями в силових структурах.

Базована на цих принципах сучасна парадигма обміну інформацією розглядає останню як продукт, яким повинен володіти і розпоряджатися аналітичний, а не розвідувальний орган. При цьому, наприклад, основна проблема для розвідників і контррозвідників полягає не в тому, як зібрати, а як знеособити дані, отримані оперативним шляхом, зашифрувати агентурні і сховати технічні джерела інформації, але при цьому зробити інформацію доступною для тих, хто її потребує для своєчасного ухвалення обґрунтованого рішення. Парадокс у тому, що чим секретнішими є дані, які добуваються розвідкою, тим менш вони є практично корисними для національної безпеки в силу обмеженого кола осіб допущених до них.

Держава та громадянське суспільство: специфіка безпекової взаємодії в інформаційному просторі. Як слушно зауважує європейський суспільствознавець Р. Дарендорф, демократичний устрій держави вимагає передусім тісної співпраці між політичними (урядовими) та суспільними (неурядовими) інституціями³⁰⁴. При цьому перші відповідають за можливість зміни влади ненасильницьким шляхом, а другі сприяють розвитку можливостей вираження інтересів, цінностей і уподобань як базових засад суспільства. Відповідно, формування громадянського суспільства можливе лише в тих демократичних державах, де відбулося політико-ідеологічне примирення між обома вищезгаданими чинниками задля втілення в життя свобод громадянина.

В інформаційно-комунікаційному полі демократичної держави (або держави, яка прагне стати демократичною) активно діють, з одного боку, органи (інституції) влади та державні діячі (посадовці), а з другого — незалежні громадські організації (структури громадянського суспільства), що керуються власними цілями та намірами. Відносини державних і недержавних (громадських) інституцій та структур розвиваються за принципом взаємодії та противаг. Як результат такого складного сплетення інституцій та їхніх спільних дій народжується нова системна якість, досягається адекватний демократичним

304. Dahrendorf R. Zagrozone społeczeństwo obywatelskie, Europa i społeczeństwo obywatelskie – rozmowy w Castel Gandolfo. – Krakow, 1994. – S.235.

державам ступінь забезпечення національної безпеки в її широкому розумінні (від безпеки держави до безпеки індивіда).

Однією з головних умов забезпечення національної інформаційної безпеки та стабільності національного інформаційного простору України є належний розвиток громадянського суспільства. Саме тому, згідно із Законом України «Про основи національної безпеки України» (2003 р.) формування громадянського суспільства віднесено до пріоритетних національних інтересів. Це означає, що розв'язання проблеми інтенсифікації процесів його становлення як одного із ключових чинників забезпечення інформаційної та суміжних складових національної безпеки залишається актуальним завданням національно-державного розвитку.

Залишаючи «за лапками» ті маніпулятивні та «технологічні» складові, які використовуються партійно-політичним істеблшментом (керуючою верхівкою) як інструменти інформаційного впливу на настрої та поведінку ключових акторів громадянського суспільства щодо безпекових питань (референдум щодо членства в НАТО тощо), а також вкрай неоднозначний зовнішній (міжнародний) чинник підтримки багатьох громадських рухів та об'єднань, — ці теми потребують окремого дослідження, яке виходить за рамки аналізованої проблематики — слід зупинитися на суто безпекових моментах цієї проблеми.

Однією з вимог до здійснення ефективної політики національної безпеки є двосторонній діалог держави та громадянського суспільства. В його інформаційно-комунікаційному вимірі ключовим є перманентний «соціальний моніторинг», що супроводжується політичними кроками та прийняттям ефективних рішень. Адже, одним із основних чинників, що містить потенційну загрозу національній безпеці України, є потенційна інформаційна не контрольованість та комунікаційна «закритість» органів державної влади або, принаймні, деяких з них³⁰⁵. Спроби державної влади зберегти та навіть посилити

механізми контролю за національним інформаційно-комунікаційним сегментом глобальної мережі, переважно нормативно-правовими механізмами та технічними засобами (в контексті т.зв. «керованої демократії»), не вирішують соціально-політичних проблем, залишаючи за користувачем право вибору моральних орієнтирів.

На окрему увагу заслуговує питання підконтрольності тих органів державної виконавчої влади, які публіцистично називають «силовими» («кістяк» національного «сектора безпеки»). Бурхливе зростання кількості та посилення ролі сучасних засобів масової інформації (медіа) з їхньою небезпідставною претензією на роль «четвертої влади» має наслідком інформаційний прорив у традиційно закриту царину «національної/державної безпеки» та відображення тенденції просування до «інформаційного суспільства». В цих умовах медіа стають повноцінними суб'єктами інформаційної безпеки, а в багатьох випадках — навіть активними акторами безпеки політичної та економічної.

Інформаційна безпека України у внутрішньому (національному) та зовнішньому (міжнародному) вимірах: тенденції взаємовпливу та перспективи розвитку. Концепція національної інформаційної безпеки є перш за все такою, що перманентно розвивається відповідно до тих базових («вічних») цінностей та стратегічних інтересів, які має нація, і які остання вважає на тому чи іншому етапі політико-економічного та/або соціально-культурного розвитку принципово важливими та пріоритетними.

У Рекомендаціях парламентських слухань з питань розвитку інформаційного суспільства в Україні констатується, що стан розбудови інформаційного суспільства в Україні порівняно зі світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України³⁰⁶. Одним з ключових завдань інформаційно-безпекового сегмента сучасного суспільствознавства залишається вимога виявлення суб'єктів, здатних впливати на спрямованість, характер і наслідки

306. Постанова Верховної Ради України «Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» // Відомості Верховної Ради. – 2014. – № 33. – С.1163.

процесу забезпечення національної інформаційної безпеки. Особливе значення в непростих умовах сучасної України набуває проблема формування т.зв. «третьої сили», тобто соціально-політичних інституцій, готових виступати інформаційно-комунікаційними посередниками між правлячою елітою та громадянським суспільством, сприяти вирішенню «класичної» проблеми роз'єднання держави/ влади та суспільства/ народу, сприяти інтеграції держави та громадян, створенню цілісного та безпечного, захищеного, але відкритого національного інформаційного та інформаційно-комунікаційного простору.

У зв'язку із цим не можна залишати поза увагою трансформацію системи відносин, у рамках якої відбулося істотне ослаблення державного домінування в інформаційній сфері взагалі та в царині інформаційної безпеки зокрема. Останнє фактично остаточно втрачає концентрований характер, розосереджується за межами інститутів влади, перетворюється на надбання різних суспільних груп і суб'єктів переважно недержавного походження. Органи державної влади та міжнародні інституції міждержавного характеру (починаючи від Ради Безпеки ООН) в умовах періодичної дестабілізації соціально-політичної обстановки проявляють нездатність забезпечити необхідний рівень національної та міжнародної безпеки, захистити інтереси людей, усунути (мінімізувати) загрози «кібертероризму» та «кіберзлочинності», сформулювати й реалізувати діючу стратегію стосовно тих інформаційних структур та каналів, які продовжують у тих або інших формах негативно впливати на перебіг соціально-політичних процесів у країні, безпеку та стабільність окремих її регіонів.

Можна стверджувати, що для України становлення незалежного від держави громадянського суспільства було одним із елементів посткомуністичної трансформації. За ступенем та ефективністю впливу на державу інститутів громадянського суспільства, до яких відносяться неурядові організації та незалежні аналітичні центри, можна оцінювати глибину перетворень, ступінь модернізації та європеїзації посткомуністичних держав.

Співпраця державних органів з неурядовими організаціями та незалежними аналітичними центрами є невід'ємним елементом інформаційної культури демократичного зразка. Наявність налагоджених ефективно діючих каналів комунікації між органами влади та «третім сектором» виступає запорукою відкритості державної політики та її підконтрольності суспільству і, в цілому, відповідності національним інтересам у сфері інформаційної безпеки.

Досвід співпраці недержавних організацій з органами влади у сфері забезпечення інформаційної безпеки та відкритості національного інформаційного простору, набутий за два десятиліття незалежності, засвідчує переважно наявність тих самих проблем, що характерні для відносин між владою та громадським сектором в Україні в цілому: традиції замкненості держапарату, непрозорість вироблення державної політики, взаємна недовіра, низька ефективність «третього сектора» у лобіюванні своїх позицій. Аналіз діяльності недержавних громадських організацій показує, що лише невелика кількість з них приділяє достатню увагу інформаційно-безпековим і суміжним з ними проблемам.

У той же час, протягом останніх років активістам недержавних організацій (насамперед, аналітичних центрів) спільно з представниками органів влади вдалося дещо розширити вікно можливостей для взаємокорисної співпраці.

В цілому розбудова системи національної інформаційної безпеки в Україні наразі є лише поступовим та неквапливим накопиченням досвіду, який, за умови оздоровлення інформаційної ситуації, може привести в майбутньому до формування нової культури взаємодії влади і суспільства, зокрема в сфері національної безпеки в якнайширшому її розумінні (т.зв. «культури безпеки»), і тим самим суттєво сприятиме успіху демократичного розвитку України.

Відносини, які зачіпають площину інформаційної безпеки, мають перейти від моделі протистояння до моделі партнерства. Вона має реалізовуватися на наступних засадах:

Перше, це розвиток громадянського суспільства та зниження ступеня відчуження між владою і громадянами (тобто, між «державною» та «національною» безпекою). Постійний експертний діалог представників владних структур і «мозкових центрів» громадянського суспільства (в т.ч. міжнародних) щодо актуальних викликів та загроз національній інформаційній безпеці. Високий рівень відповідальності влади і громадян за стан національної інформаційної безпеки та «якість» національного інформаційного простору.

Друге, це сприйняття демократії (в контексті її тлумачення через парадигму «контролю», запропоновану Г. Алмондом і Б. Пауелом) як цінності більшістю громадян, відносно високий ступінь інформаційної культури населення, який дозволяє людям робити свідомий вибір на користь того чи іншого варіанта забезпечення національної безпеки на основі належної поінформованості, отриманих знань і раціонального розрахунку.

Третє — формування інформаційно-безпекової «еліти» (т.зв. «стратегічного співтовариства»³⁰⁷), яка сповідує демократичні цінності і є відкритою до комунікації та діалогу. Вироблення серед представників еліти консенсусу стосовно основних принципів демократії. (При цьому, не можна до елітної верстви державного управління однозначно відносити співробітників «сектора безпеки», які професійно забезпечують виконання інформаційно-безпекових повноважень органів влади.)

Четверте, подолання протиріччя між демократичною формою та недемократичною сутністю інститутів забезпечення національної інформаційної безпеки. Набуття цими інститутами не тільки демократичної форми, але й демократичного змісту, продукування ними реальної демократичної політики інформаційної безпеки. В цьому контексті знаковими подіями можна вважати дедалі ширшу практику публікації профільними структурами т.зв. «Білих книг» як інформаційних видань щодо окремих аспектів безпекової діяльності

238 307. Див. Полтораков О.Ю. Стратегічне співтовариство в системі владно-політичних відносин в Україні // Сучасна українська політика. Політики і політологи про неї. – К.: Український центр політичного менеджменту, 2010. – Вип. 19. – С.74-84.

(оборонної, розвідувальної тощо). Це опосередковано сприяє покращенню як загального інформаційно-комунікаційного «клімату довіри», так і «довірі» (а отже і загальному іміджу) до безпекових структур.

Лише у випадку реалізації такої моделі вдасться подолати негативні тенденції розвитку національної безпеки і покращити стан її інформаційної складової. Адже «життя нації», як слушно зауважив ще Ж.Е. Ренан, — це «щоденний плебісцит». І інформаційно-комунікаційний простір людського буття в жодному разі не є винятком — скоріше навпаки.

15. Кібервійна як новий засіб і метод ведення війни: виклики міжнародному гуманітарному праву[©]

Міжнародне гуманітарне право (МГП) є галуззю сучасного міжнародного публічного права, яка застосовується під час збройних конфліктів і регулює захист жертв війни та застосування сторонами збройного конфлікту засобів і методів ведення війни. У зв'язку з цим міжнародне гуманітарне право часто називають правом збройних конфліктів або *jus in bello* — правом, яке застосовується під час війни. По суті, міжнародне гуманітарне право є балансом міркувань гуманності і військової необхідності. При порушенні цього балансу виникає необхідність зміни норм, що діють, або їх тлумачення³⁰⁸ з метою відновлення рівноваги. Тому абсолютно логічно, що розвиток нових засобів і методів ведення військових дій спричиняється до розробки норм, які регулюють або обмежують використання таких озброєнь і поведінки³⁰⁹. Наприклад, прийняття Санкт-Петербурзької декларації 1868 р. представляло реакцію на вживання російською армією нового вигляду куль, тоді як Женевський протокол 1925 р. послідував за використанням отруйних газів на полях Першої світової війни.

Сьогодні міжнародне гуманітарне право стикається з новими викликами безперервного технологічного прогресу. Ведення військових дій з використанням високотехнологічних комп'ютерних та інформаційних технологій (кібервійна або інформаційна війна) є важливим напрямом розвитку військових стратегій багатьох держав світу. Велика частина новітніх технологічних розробок значною

308. Michael Schmitt, "The Impact of High and Low-Tech Warfare on the Principle of Distinction," International Humanitarian Law Research Initiative Briefing Paper, Program on Humanitarian Policy and Conflict Research at Harvard University. – November 2003). - P. 1.

309. Isabelle Daoust, Robin Coupland, Rikke Ishoey. New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare. – IRRC, June 2002. – Vol.84, No.846, p.345.

мірою сприяє дотриманню принципу розрізнення і надає недосяжні раніше можливості по захисту цивільного населення під час ведення військових дій. Інформаційні технології (супутникові фотографії, системи спостереження і зондування, розвідувальні й комунікаційні технології) допомагають точно визначити місце розташування комбатантів і військових об'єктів, а також забезпечують інформованість про ситуацію, покращують оцінку нанесеної воєнної шкоди. Точність сучасних технологій (наприклад, точкової зброї) дозволяє мінімізувати ризик для цивільних осіб завдяки тому, що комбатанти нападають лише на військові об'єкти і ефект від таких нападів не поширюється на цивільне населення. Таким чином, дотримується і зміцнюється принцип розрізнення. Відзначимо, що представники Збройних сил США заявили, що «зобов'язання точності», яке є основою сучасної військової справи, є однією з найважливіших функціональних військових концепцій³¹⁰. Наведені вище технології сприяють також зміцненню принципу пропорційності, оскільки військові операції, засновані на достовірній і точній інформації, зменшують ризик нанесення випадкових пошкоджень і надмірної шкоди.

Крім того, технологічний прогрес робить військові операції менш небезпечними для їх безпосередніх учасників. Наприклад, малопомітні технології (технології «стелс»), такі як F-117 «Нічний яструб», дозволяють літакам проникати крізь ешелони протиповітряної оборони противника, зменшуючи при цьому міру ризику для екіпажу³¹¹.

Проте новітні технології можуть бути також викликом для міжнародного гуманітарного права і загрозою дотриманню його принципів і норм. Наприклад, комп'ютерні віруси легко можуть вивести з ладу системи і мережі, які виконують життєво необхідні для цивільного населення функції (водопостачання, медична допомога тощо). До питання загроз новітніх технологій, яке широко дебатується

310. Chairman, Joint Chiefs of Staff. – Joint Vision 2020. - Режим доступа: <http://www.fas.org/spp/military/docops/usspac/visbook.pdf>.

311. Michael Schmitt, "The Impact of High and Low-Tech Warfare on the Principle of Distinction," International Humanitarian Law Research Initiative Briefing Paper, Program on Humanitarian Policy and Conflict Research at Harvard University. – November 2003). - P. 4.

в наукових і професійних колах, має бути знайдений специфічний підхід з боку міжнародного гуманітарного права.

Поява нових видів озброєнь, які не приводять до летального результату (електричні, акустичні, хімічні, біологічні і так далі), породжує спірні точки зору відносно того: підпадають такі види зброї під сферу регулювання міжнародного гуманітарного права і договорів по контролю за озброєннями чи вони належать до нової категорії зброї. На жаль, відсутність чітких даних по дії на людину багатьох з таких озброєнь залишає питання відкритим³¹².

Певні аспекти сучасного ведення воєнних дій можуть мати непередбачуваний ефект відносно проведення військових операцій. Цей висновок напрошується саме сьогодні, коли люди все більше віддаляються від безпосереднього контролю за проведенням операцій і ухвалення рішень. До того ж цивільний персонал, що залучається до військової конструкторської справи, схильний підтримувати військові системи, що допускаяють ризик випадкового ушкодження.

Викладене вище представляє лише деякі з викликів новітніх технологій. Яким чином МГП реагує на появу нового виду озброєнь і нових способів ведення війни, таких як кібервійна? Абсолютно очевидно, що МГП не може регулювати використання всіх сучасних засобів і методів ведення війни, що з'являються, в спеціальних документах, воно просто «не встигає» за прогресом. У більшості випадків, залишаючись нездатним передбачати тенденції розвитку озброєнь, МГП відповідає на нові загрози шляхом застосування своїх основних принципів. Уже був наведений приклад Санкт-Петербурзької Декларації — першого міжнародного документа, який стосувався питання розвитку озброєнь. Зокрема, держави-учасники погодилися з пропозицією, що, «зважаючи на майбутнє вдосконалення, завдяки якому наука може вплинути на розвиток озброєнь і збройних сил... треба узгоджувати виклики війни з законами гуманності»³¹³.

312. David P. Fidler. The Meaning of Moscow: Non-lethal Weapons and International Law in the Early 21st Century. – IRRC, September 2005. – Vol. 87, No. 859, p.525-553.

313. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, 29 November 1868.

Як відзначає заступник голови юридичного відділу Міжнародного Комітету Червоного Хреста і авторитетний дослідник Кнут Дорманн, до новітніх типів озброєння, а також до кібератак, безумовно застосовуються положення Додаткових протоколів до Женевських конвенцій від 12 серпня 1949 року про захист жертв війни³¹⁴. Стаття 36 Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 р., що стосується захисту жертв міжнародних збройних конфліктів (ДП I), містить положення, що регулює це питання. Стаття 36 ДП I зобов'язує держави-учасниці «при вивченні, розробці, придбанні або прийнятті на озброєння нових видів зброї, засобів або методів ведення війни... вирішувати питання, чи підпадає їх вживання... під заборони, що містяться в цьому Протоколі, або в яких-небудь інших нормах міжнародного права»³¹⁵. Хоча стаття 36 ДП I не встановлює способи такого визначення, вона має на увазі прийняття на національному рівні заходів по з'ясуванню, чи підпадає вживання нових озброєнь і методів під заборону. Як правило, такі заходи називаються «національними перевітками». Результатом цих перевірок має стати дозвіл або заборона державі на використання певного виду озброєнь або методу ведення військових дій³¹⁶.

Першим етапом «перевітки» є аналіз специфічних заборон, що накладаються певними міжнародними договорами і документами³¹⁷. До договорів і документів, які можуть піддаватися аналізу, відносяться: Санкт-Петербурзька декларація 1868 р., Гаазькі декларації 1899 р., Гаазькі конвенції 1907 р., Женевський протокол 1925 р., Конвенція про заборону військового або будь-якого іншого ворожого використання засобів дії на природне середовище 1976р., Конвенція

314. Applicability of the Additional Protocols to Computer Network Attacks - Режим доступа: <http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf>.

315. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I), 12 декабря 1977 г., Женевские конвенции от 12 августа 1949 г. и Дополнительные протоколы к ним. – Москва, МККК, 1995.

316. Y. Sandoz, C. Swinarski, B. Zimmermann (eds). Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. – Geneva. - ICRC. – 1987. - P.428.

317. Isabelle Daoust, Robin Coupland, Rikke Ishoey. New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare. – IRRС, June 2002. – Vol.84, No.846, p.349.

про звичайні озброєння 1980р. і протоколи до неї, Конвенція про заборону хімічної зброї 1993 р., Конвенція про заборону протипіхотних мін 1997 р. та ін. Далі держава повинна впевнитися в тому, що використання таких озброєнь або методів ведення військових дій відповідає нормам звичаєвого міжнародного права. У своєму Консультативному висновку з приводу законності використання ядерної зброї або загрози нею Міжнародний Суд ООН визначив деякі основні принципи МГП як звичаєві принципи, тобто принципи звичаєвого міжнародного права. До таких принципів належать: принцип розрізнення, заборона використання зброї, яка нездатна розрізняти цивільні і військові цілі, заборона використання зброї, яка завдає комбатантам страждань, які не відповідають військовій необхідності, і зброї, яка заподіює або підсилює такі страждання³¹⁸. Дослідження Звичаєвих Норм Міжнародного Гуманітарного Права Міжнародного Комітету Червоного Хреста в розділі «Основні принципи використання озброєнь» посилається на заборону використання методів ведення військових дій, які заподіюють надмірні страждання або пошкодження, а також на заборону використання зброї невідборчого характеру (норми 70, 71). Заборона використання отрут і отруйних газів, біологічної зброї, хімічної зброї, куль дум-дум і вибухових куль, зброї, що наносить пошкодження осколками, які неможливо виявити, мін-пасток і засліплюючої лазерної зброї також має звичаєвий характер³¹⁹.

Держава, яка здійснює «перевірку» нових видів озброєнь, повинна також визначити, чи потрапляє певний тип озброєння під сферу регулювання положень ДП I, які відображують викладені вище основні принципи: заборона використання методів ведення військових дій, що завдають надмірної шкоди і страждань (п. 2 ст. 35), принцип розрізнення (ст. 48), захист цивільного населення і заборона не вибіркових нападів (ст. 51). Положення п. 3 ст. 35 і

318. Legality of the Threat of the use of Nuclear Weapons, Advisory Opinion of July 1996, ICJ. Reports 1996, para. 78.

319. Jean-Marie Henckaerts. Study on Customary International Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict. – IRLC, March 2005. – Vol. 87, No. 857, p.204-205.

ст. 55 ДП І встановлюють зобов'язання по захисту навколишнього природного середовища від поширеної, тривалої і сильної шкоди, а також забороняє використання методів ведення військових дій, які мають це за свою ціль або можуть заподіяти таку шкоду.

П. 2 ст. 1 ДП І містить положення, яке добре відоме як «Застереження Мартенса». Вперше це положення було включене в преамбулу II Гаазької конвенції 1899 р.³²⁰ «Застереження Мартенса» передбачає, що «у випадках, не передбачених цим Протоколом або іншими міжнародними угодами, цивільні особи і комбатанти залишаються під захистом і дією принципів міжнародного права, що витікають із сталих звичаїв, з принципів гуманності і з вимог суспільної свідомості». Міжнародний Суд ООН, поза всякими сумнівами, визнав тривале існування і використання «Застереження Мартенса» і постановив, що це застереження «довело, що воно є ефективним методом реагування на швидкі темпи еволюції військових технологій»³²¹.

Міжнародний Суд ООН також встановив, що міжнародне гуманітарне право застосовується до всіх видів озброєнь і що «новизна» якого-небудь виду не перешкоджає вживанню МГП³²². Насправді, міжнародне гуманітарне право має всі необхідні засоби упоратися з викликами технологічного прогресу. Ці засоби включають масив договірних і звичаєвих принципів та норм, велику кількість міжнародних організацій (серед яких, безумовно, Міжнародний Комітет Червоного Хреста відіграє найбільш значну роль) і механізми притягнення до відповідальності порушників норм МГП (як держав, так і індивідів). Утім, успіх вживання цих засобів залежить від готовності і бажання всіх суб'єктів міжнародного права сумлінно виконувати положення МГП.

У контексті розвитку новітніх технологій виникає питання використання комп'ютерів у ході ведення військових дій. Використання

320. Antonio Cassese. The Martens Clause: Half a Loaf or Simply Pie in the Sky? – EJIL, 2000. – Vol.11, No.1, p.187.

321. Legality of the Threat of the use..., paras. 78, 87.

322. Legality of the Threat of the use..., para. 86.

комп'ютерів в сучасних війнах почалося вже декілька десятиліть тому. Сфера їх застосування була досить широкою — від спрямування потоків військової техніки і особового складу в зони проведення операцій до обробки розвідувальних даних і підвищення точності дії зброї. У зв'язку з цим виникає необхідність коротко розглянути правові питання, що стосуються використання комп'ютерів у ході ведення класичних (кінетичних) воєнних дій.

В цілому, використання комп'ютерів для підвищення ефективності традиційних військових дій не ставить перед нами багато нових питань правового порядку. Єдиний виняток може стосуватися явища «відсутності людини». Розвиток інформаційних технологій дає можливість комп'ютерам все більшою мірою вирішувати завдання, які раніше виконувалися людиною. Безпілотний літак «Предейтор» з дистанційним управлінням, оснащений ракетами «Хеллфайр», успішно завдавав ударів по рухомих наземних цілям в Афганістані та Ємені³²³. Сьогодні прикладів застосування безпілотних літальних апаратів стає все більше і більше. Ще один приклад стосується використання комп'ютерів на етапі визначення об'єктів для удару. Наразі комп'ютери зберігають і оновлюють списки цілей, обробляють дані про цілі, визначають оптимальні методи виконання бойового завдання і види зброї, а також можливі супутні та випадкові втрати. І хоча людина залишається важливим учасником процесу ухвалення рішень (особливо, якщо вірогідні супутні та випадкові втрати), комп'ютери виконують усе більше функцій в процесі визначення і вибору цілей. Підхід до визначення цілей, заснований на результативності, який стає основним у війнах ХХІ століття, підсилює цю тенденцію, оскільки комп'ютерне моделювання є потужним знаряддям при визначенні того, що повинно стати об'єктом нападу і яким чином добитися певних результатів³²⁴.

323. У 2002 р. ЦРУ використовувало «Предейтор» з дистанційним управлінням для нанесення удару по автомобілю, в якому, відповідно до отриманої інформації, знаходився Каед Сеньян аль Хартхі, один з лідерів Аль Каїди в Ємені. – BBC News World Report, November 5, 2002.

324. Визначення цілей, засноване на результативності, ставить перед собою завдання вразити лише певні цілі і лише так, щоб добитися певних результатів, які дозволять реалізувати задум командира. Таке визначення цілей слід відрізнити від вибору цілей на виснаження. Див.: Joint Staff, Joint Doctrine for Targeting, Joint Publication 3-60, January 17, 2002. Див. також: Michael N.

Хоча деякі теоретики і практики висловлюють побоювання, що ця тенденція може понизити рівень захисту, що надається гуманітарним правом цивільним особам, цивільним об'єктам та іншим захищеним особам і об'єктам, історія свідчить про те, що гуманітарне право досить гнучко адаптується до змін у методах і засобах ведення війни. Ймовірно, що так станеться і в цьому випадку. Врешті-решт, неучасть людини в процесі визначає стандарти у ситуації, в якій нові методи і засоби ведення війни пов'язані з ризиком випадкових пошкоджень і супутніх втрат для захищених осіб і об'єктів.

Стаття 57 Додаткового протоколу I викладає відповідну норму: «ті, хто планує напад або приймає рішення про його здійснення: і) роблять все практично можливе, щоб упевнитися в тому, що об'єкти нападу не є ні цивільними особами, ні цивільними об'єктами і не підлягають особливому захисту, а є військовими об'єктами». Далі стаття вимагає, щоб приймалися «всі практично можливі запобіжні заходи при обранні засобів і методів нападу з тим, щоб уникнути випадкових втрат життя серед цивільного населення, поранення цивільних осіб та випадкового збитку цивільним об'єктам і, в усякому разі, звести їх до мінімуму». Хоча Сполучені Штати Америки і деякі інші країни (зокрема Ізраїль) не є учасниками ДП I, вважається, що більшість його положень відображають звичаєве міжнародне право і, таким чином, є обов'язковими для дотримання державами, які не є його учасниками. Якщо який-небудь метод або засіб ведення військових дій, що використовується за допомогою комп'ютерів, є більш ефективним або дешевшими, ніж той, замість якого цей метод або засіб застосовується, але наслідки, швидше за все, виявляться більш згубними для цивільного населення, тоді при його вживанні буде порушений принцип звичаєвого міжнародного права, кодифікований в статті 57 ДП I. Проте в більшості випадків комп'ютери значно підвищують надійність інформації, необхідної для процесу ухвалення рішень і здійснення нападів, що відповідає гуманітарним цілям. Можна сказати, що держава, яка має в своєму розпорядженні технологічні і

фінансові можливості для того, щоб використовувати комп'ютери для забезпечення своїх дій і роботи устаткування, повинна робити це так, щоб задовольнялася норма, в якій передбачається «все, практично можливе». До теперішнього часу міжнародне гуманітарне право не тлумачилося як таке, що вимагає від держав включати певні види техніки в свої арсенали; його вимоги стосуються лише використання наявної зброї, а саме використання має бути практичним і розумним з військової точки зору.

З правової точки зору проблемою є використанням комп'ютерів як засобу або методу ведення війни. У зв'язку з цим важливим викликом для МГП є кібервійна (інформаційна війна). Чутки про новий вид війни збуджують уяву військових стратегів ось уже більше десяти років. Війна в Косово показала, що чутки ці стали реальністю. Деякі з технологій і тактичних прийомів, що були предметом таких розмов, перетворилися на військову доктрину³²⁵. До змін, про які йде мова, зазвичай застосовується популярний термін «кібервійна» або «інформаційна війна», але в розумінні військових — це частина ширшого стратегічного нововведення, яке називається «інформаційними операціями» і «революцією у військовій справі». Але, незалежно від назви, суть цього явища одна: використання у ворожих цілях високотехнологічних комп'ютерних і телефонних систем противника як у військовій, так і в цивільній інфраструктурі.

Оскільки визначення кібервійни знаходиться все ще у стадії розробки і різні країни формулюють його по-різному, можна дати класифікацію двох видів кібервійни, обидва з яких уже не один раз використовувалися в світовій історії: кібервійна без одночасного застосування фізичної сили — в мирний час; кібервійна з застосуванням фізичної сили — під час збройного конфлікту.

Однією з перших важливих проблем кібервійни може бути питання: як співвідносяться між собою акти кібервійни і заборона на застосування сили, що міститься в Статуті ООН. Питання полягає в наступному: чи є використання кібервійни без застосування збройної сили застосуванням сили відповідно до положень Статуту ООН?

325. Уильям Черч. Информационная война, CIWARS Intelligence Report, 1998.

Стаття 2(4) Статуту Організації Об'єднаних Націй наказує утримуватися «від загрози силою або її застосування» в міжнародних відносинах. У системі Статуту існують два винятки з цього загального правила: дозволяється застосування сили згідно з мандатом, наданим Радою Безпеки відповідно до статті 42, і у випадку самооборони, про яку говориться в статті 51. Існують три теорії визначення поняття «застосування сили».

Відповідно до першої, заборона на використання сили має на меті не допустити переростання інцидентів, які не досягають певного порога насильства, в повномасштабні війни; значення має не засіб нападу, а об'єм заподіяного збитку. Не важливо, підстанція електромережі була зруйнована 2000-кілограмовою бомбою чи введенням ворожого програмного коду в головну програму управління підстанцією.

Прибічники другого підходу, що користується більшою популярністю в академічних колах, вважають, що укладачі Статуту ООН мали намір зробити все можливе, щоб перевага віддавалася вирішенню конфліктів невоєнними засобами. Відповідно до цього підходу, лише збройний напад (класичний напад із застосуванням традиційних збройних сил) становить застосування сили. Значення має саме засіб нападу.

Третій підхід, що розглядається дослідниками, пропонує аналіз кожного конкретного випадку, при якому братимуться до уваги як якісний, так і кількісний аспекти операції. При вживанні цього методу наступні критерії, які не є виключними, вказують на міру вірогідності того, що міжнародне співтовариство визнає інформаційну операцію застосуванням сили: серйозність наслідків, їх негайне настання, пряма дія, інвазивність, вимірність, передбачувана легітимність і відповідальність³²⁶. Сукупний розгляд таких чинників дає можливість передбачити, чи буде конкретна операція — традиційна, кібернетична або змішана — вважатися застосуванням сили або вона не перевищить цього порога. Крім того, цей підхід робить транспарентнішими сфери розбіжностей, що дозволить зробити норму більш чіткою.

326. Michael N. Schmitt. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. – Columbia Journal of Transnational Law, 1999. - Pp. 900-923.

Розмірковуючи над вищевикладеними проблемами, можна почати зі спроби осмислити кібервійну в категоріях сучасних уявлень про застосування сили. Оскільки кібервійна направлена значною мірою проти інфраструктури, яка використовується як цивільним населенням, так і військовими, доцільно було б розглянути це питання в рамках міжнародного гуманітарного права.

Проблеми контролю над озброєннями, що виникають в рамках кібервійни, вирішити непросто. Для ефективного ведення кібервійни досить персонального комп'ютера, телефонної лінії і хакерських програм, які легко скачуються з Інтернету. Це не означає, що світ повний потенційних «кіберсолдат» — від володіння однією «машиною», що дозволяє здійснити окремий злам комп'ютерної системи, далеко до здатності завдати координованих ударів з використанням сучасної системи управління і контролю, необхідної для ведення воєнної кампанії.

Сьогодні питання кібервійни стоїть на порядку денному ООН, яка опрацьовує різні варіанти вирішення проблеми, а також інших міжнародних організацій. Ця дискусія багато в чому виграла б, якби фахівці з міжнародного гуманітарного права розглянули також проблеми кібервійни і вирішили питання регулювання такого явища як кібервійна в рамках цієї галузі міжнародного права.

Перші спроби втілити ці ідеї в життя вже здійснюються. У березні 2013 року було опубліковано Талліннське керівництво з міжнародного права, що застосовується до кібервійни (Tallinn Manual on the International Law Applicable to Cyber Warfare)³²⁷. Це керівництво було написане міжнародною групою експертів з МГП за пропозицією Центру вдосконалення співпраці в галузі кібербезпеки НАТО (NATO Cooperative Cyber Defence Centre of Excellence). В підготовці цього керівництва брали активну участь три організації: НАТО, Міжнародний Комітет Червоного Хреста як «Хранитель МГП» і Кібервійська США (United States Cyber Command). Не

327. Tallinn Manual on the International Law Applicable to Cyber Warfare. – Режим доступа: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381

дивлячись на те, що керівництво було підготовлене на основі пропозиції і при організаційній підтримці НАТО, воно є консенсусним поглядом двадцяти міжнародних експертів на те, яким чином міжнародне право в цілому і міжнародне гуманітарне право зокрема застосовується до кібервійни. В цілому Талліннське керівництво охоплює дві широкі сфери: *jus ad bellum*, тобто, в яких випадках здійснення кібератак означатиме можливість у відповідь застосувати збройну силу і *jus in bello*, тобто застосування МГП до кібероперацій.

У Талліннському керівництві експерти прийшли до загальної думки, що МГП, безумовно, застосовується до ситуацій кібервійни, до кібероперацій, які проводяться в контексті збройного конфлікту. Керівництво складається з дев'яносто п'яти правил, підготовлених і прийнятих експертами шляхом консенсусу, які, на думку експертів, є частиною звичаєвого міжнародного права. Талліннське керівництво виходить з класичної дихотомії міжнародних і неміжнародних збройних конфліктів, але, в той же час, визнає, що самі по собі кібероперації можуть бути збройним конфліктом залежно від наявності обставин, зокрема руйнівних наслідків таких операцій. У керівництві дано визначення «кібератаки» по міжнародному гуманітарному праву як кібероперації, в рамках нападу або захисту, яка, як передбачається, спричиниться до каліцтва або смерть індивідам, завдасть шкоди, або знищить об'єкти, причому шкода в керівництві розуміється як фізична шкода або як втрата функціональності об'єкта.

Серед основних правил і принципів Талліннського керівництва слід зазначити такі: 1) держави не можуть дозволяти використовувати кіберінфраструктуру, яка знаходиться на їх території, для нанесення шкоди іншим державам; 2) заборона використання сили в міжнародному праві повністю поширюється на кібероперації; 3) держави відповідатимуть за кібероперації проти іншої держави, якщо ці операції проводилися секретними службами держави або індивідами або групою індивідів за вказівкою держави.

Однією з головних ідей керівництва є те, що кібервійна

повинна обмежуватися певними правилами, цивільні комп'ютери і кіберінфраструктура мають бути захищені від кібератак під час збройного конфлікту. На думку Міжнародного Комітету Червоного Хреста, зокрема його юридичного радника Лорана Жізеля, саме дотримання принципу розрізнення між цивільними і військовими комп'ютерами і кіберінфраструктурою в єдиному світовому кіберпросторі є найбільшим прийнятним рішенням для міжнародного гуманітарного права у цьому питанні³²⁸. Зрозуміло, що Талліннське керівництво не має обов'язкової юридичної сили, оскільки є науковим дослідженням і представляє лише загальну точку зору експертів. Втім, очікується, що Талліннське керівництво впливатиме на підходи і позиції держав відносно кібервійни.

Таким чином, останнім часом особливу увагу регламентації кібервійни приділяють фахівці з міжнародного гуманітарного права. Це дозволяє сподіватися, що ситуації кібервійни не знаходитимуться у правовому вакуумі, а все більше регулюватимуться сучасним міжнародним гуманітарним правом.

328. The law of war imposes limits on cyber attacks too – Режим доступа: <http://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm>.

АВТОРИ

Басиста Альбіна Володимирівна — аспірантка кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка (2)

Герасимчук Наталія Вікторівна — аспірантка кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка (4)

Городиський Іван Михайлович — директор Центру верховенства права Українського католицького університету, кандидат юридичних наук (6)

Жилінкова Олена В'ячеславівна — доцент кафедри цивільно-правових дисциплін юридичного факультету Харківського національного університету імені В. Н. Каразіна, кандидат юридичних наук (13)

Жиляєв Ігор Борисович — професор кафедри менеджменту Національного технічного університету України «Київський політехнічний інститут», член Експертної ради Комітету Верховної Ради України з питань інформатизації та інформаційних технологій, доктор економічних наук (7)

Кирилюк Ольга Василівна — аспірантка кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка (3)

Кориневич Антон Олександрович — асистент кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка, кандидат юридичних наук (15)

Кукіна Зінаїда Олександрівна — асистент кафедри європейського та порівняльного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка, кандидат юридичних наук (10)

Кушнір Ірина Володимирівна — представник Уповноваженого в Конституційному Суді України, Секретаріат Уповноваженого

Верховної Ради України з прав людини (8)

Пазюк Андрій Валерійович — керівник лабораторії з управління Інтернетом Української Асоціації міжнародного права, член Експертної ради Комітету Верховної Ради України з питань інформатизації та інформаційних технологій, кандидат юридичних наук (1, 5, 11)

Полтораков Олексій Юрійович — головний консультант, Громадський комітет національної безпеки України, Центр досліджень проблем громадянського суспільства, кандидат політичних наук (14)

Терехова Тетяна Андріївна — аспірантка кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка (9)

Шахбазян Карина Суренівна — старший науковий співробітник, Центр інтелектуальної власності і передачі технологій НАН України, кандидат юридичних наук (12)

Для нотаток.

Це видання опубліковано в рамках спільної програми Ради Європи та Європейського Союзу «Зміцнення інформаційного суспільства в Україні». Погляди, висловлені в публікації, належать авторам і не обов'язково відображають позицію Ради Європи.

Науково-практичне видання

ІНТЕГРАЦІЯ УКРАЇНИ В ЄВРОПЕЙСЬКЕ ІНФОРМАЦІЙНЕ
СУСПІЛЬСТВО:

ВИКЛИКИ ТА ЗАВДАННЯ

Колективна монографія

Підписано до друку 24.11.2014. Наклад 300 прим.
Формат 60x90 1/16 Папір офсетний. Друк офсетний.
Зам. 1125-2014

Видавництво:
ФОП Клименко Ю.Я.
м. Київ, вул. Котельнікова, 31