МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
ІНСТИТУТ МІЖНАРОДНИХ ВІДНОСИН

На правах рукопису

Кирилюк Ольга Василівна

УДК 341.1/8

МІЖНАРОДНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Спеціальність 12.00.11 – міжнародне право

Дисертація на здобуття наукового ступеня
кандидата юридичних наук

Науковий керівник
Пазюк Андрій Валерійович,
доктор юридичних наук, доцент

Київ – 2016

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Процес розбудови глобального інформаційного суспільства характеризується поступовим переходом від «міжнародного права співіснування» до «міжнародного права співпраці» усіх зацікавлених сторін в інформаційній сфері. Концепція глобального інформаційного суспільства піднімає питання альтернативних можливостей, у тому числі міжнародного права у контексті його трансформаційної спроможності та здатності до прогресивного розвитку. Аналіз сучасних тенденцій міжнародного нормотворення свідчить про те, що управління Інтернетом як критичним ресурсом глобального інформаційного суспільства буде найбільш ефективним за умови залучення до процесу прийняття рішень усіх зацікавлених сторін (держав, міжнародних організацій, приватного сектору, громадянського суспільства, технічної та академічної спільнот), що різняться між собою за ознакою правового статусу, переслідуваних інтересів та експертного потенціалу.

В основу дисертаційного дослідження покладено ідею про те, що аналіз природи нового правового феномену не повинен обмежуватися виключно формальними чи номінальними умовами, а має враховувати також динаміку його розвитку та перетворюючий трансформаційний вплив на систему міжнародного права в цілому та її окремі елементи. Саме тому в роботі застосовується діалектичний підхід до дослідження еволюції міжнародного права у контексті його адаптації до змін, зумовлених розвитком глобального інформаційного суспільства. Упродовж останніх десятиліть інформаційно-комунікаційні технології здійснюють суттєвий вплив на розвиток міжнародного права, що особливо помітно у сферах співробітництва держав із питань захисту прав людини онлайн, транскордонного обміну персональними даними та забезпечення кібербезпеки. Наразі прийнято окремі міжнародно-правові документи щодо зазначених питань, втім, досі відсутнє єдине розуміння ефективності міжнародного права як нормативного регулятора суспільних відносин, опосередкованих використанням Інтернету.

Інтернет став потужною глобальною інформаційною інфраструктурою, що виходить за фізичні кордони держави і тим самим обумовлює появу низки правових

проблем, пов'язаних із територіальністю міжнародно-правового регулювання в межах юрисдикції суверенних держав. Фізично окреслена територія держави перестає бути єдиним ідентифікатором застосовного правопорядку. Атериторіальність Інтернету потребує модифікації підходів до регулювання суспільних відносин, опосередкованих його використанням.

Адаптація міжнародного права до змін у суспільних відносинах, зумовлених розвитком глобального інформаційного суспільства, повинна супроводжуватися розширенням нормотворчих повноважень та представницької участі в інституційному механізмі управління Інтернетом усіх зацікавлених сторін. Фактично, розпочався новий етап удосконалення міжнародного права в частині охоплення ним суспільних відносин, опосередкованих використанням Інтернету, що супроводжується переходом від державоцентричної системи міжнародних відносин до моделі глобального управління інформаційним суспільством, заснованої на принципі багатосторонньої участі стейкхолдерів у здійсненні владної та нормотворчої функцій.

Тривалий час міжнародне право залишалося інертним по відношенню до питань розвитку глобального інформаційного суспільства. Складність пристосування класичних для міжнародного права концепцій суверенітету, територіальної юрисдикції, первинності ролі держав у процесах міжнародного нормотворення та управління були причиною того, що вивчення обраної проблематики залишалося в рамках політичних, технічних та суспільствознавчих наук. Розвиток глобального інформаційного суспільства спонукає до еволюції міжнародного права у XXI столітті. Позитивний та розширювальний вплив глобального інформаційного суспільства на розвиток регуляторного потенціалу міжнародного права та трансформація останнього відповідно до викликів технологічного прогресу й обумовили актуальність і вибір теми дисертаційного дослідження.

Теоретичною основою дисертаційного дослідження стали праці як українських учених, так і зарубіжних науковців. Окремі аспекти та теорії інформаційного суспільства досліджували у своїх працях М. Бангеманн, О. Баранов,

З. Бауман, Д. Белл, Ф. Вебстер, Е. Гідденс, М. Кастеллс, Й. Масуда, Ю. Нестеров, М. Постер, А. Ракітов, Т. Стоуньєр, Е. Тоффлер, Ю. Хабермас, Д. Черешкін, Г. Шиллер та інші.

Питання становлення глобального інформаційного суспільства розглядали М. Кривошеєв та А. Чернов, у той час як питаннями правового забезпечення цих процесів займалися Л. Єфимова, Ю. Кашлєв, Б. Кристальний, А. Новицький, А. Стрельцова та інші. Дослідження у сфері історичного розвитку концепції глобального інформаційного суспільства та її міжнародно-правового регулювання можна знайти у роботах У. Карлссон, Л. Маклагліна, К. Норденстренга, К. Падовані, В. Пікарда, М. Теграняна та К. Хамелінка.

Питання «м'якого» права у юридичній літературі досліджували К. Бекяшев, С. Білоцький, А. Бойл, М. Буроменський, М. Веліжаніна, Г. Вельямінов, М. Голдман, В. Денисов, О. Задорожній, Л. Зенден, О. Київець, Я. Клабберс, Р. Колодкін, П. Коттрелл, І. Лукашук, О. Мережко, В. Мицик, В. Муравйов, М. Поллак, К. Смирнова, Ф. Снайдер, В. Талімончик, Л. Тимченко, Ю. Тихомиров, Д. Трубек, Г. Тункін, С. Черніченко, М. Шоу, О. Шпакович та К. Якобссон.

У зарубіжній літературі питання управління Інтернетом знайшли відображення у роботах Л. Бігрейва, Дж. Бінга, М. Кіттіманна, В. Кляйнвехтера, Й. Курбалії, П. Поланскі, Д. Поста та А. Туцці. Серед українських учених інституційну основу та нормативний зміст міжнародно-правового регулювання суспільних відносин в інформаційній сфері розглядали І. Забара, А. Пазюк, К. Шахбазян.

До аналізу окремих аспектів захисту персональних даних вдавалися такі вчені, як О. Баранов, М. Бем, В. Галаган, Дж. Голдсміт, І. Городиський, К. Мельник, А. Пазюк, Дж. Райденберг, А. Тунік, І. Усенко, П. Шварц, тощо. Забезпечення захисту прав людини онлайн досліджували, зокрема, О. Жилінкова, Н. Камінська, А. Пазюк.

Окремі аспекти використання кіберпростору у військових цілях розглядали К. Бейкер, І. Забара (міжнародна інформаційна безпека), Тріша Д. Карпентер (кібероперації), Сьюзен В. Бреннер (кіберзлочинність), Дж. Карр, Франк

Дж. Кілуффо, Стефен Дж. Кімбала, Р. Кларк, Дж. Річард Кноп, М. МакКоннелл, Р. Нейк, Р. Рогожинскі, П. Розенцвайг та К. Сандвік (кібервійна), Р. Браст (кібератаки), М. Шмітт (кіберконфлікти) та інші.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконане в межах наукової теми «Правові засади співпраці України з міжнародними інтеграційними об'єднаннями: теорія і практика», яка є частиною наукової теми Інституту міжнародних відносин № 11БФ048-01: «Україна у міжнародних інтеграційних процесах», що є складовою Комплексної наукової програми Київського національного університету імені Тараса Шевченка.

Метою дисертаційного дослідження є з'ясування змісту і напрямів прогресивного розвитку міжнародного права як реакції на трансформуючий вплив глобального інформаційного суспільства та надання пропозицій щодо удосконалення регуляторної спроможності міжнародного права в умовах глобалізації та перманентного технологічного прогресу.

Завдання дослідження:

– сформулювати визначення базових категорій понятійного апарату дисертаційного дослідження;

– з'ясувати в історичній ретроспективі адаптивність міжнародного права до перманентно та динамічно еволюціонуючих суспільних відносин в інформаційній сфері;

– дослідити інституційні механізми управління глобальним інформаційним суспільством, проаналізувати їх ефективність, виявити нормотворчий потенціал та рівень взаємодії, а також надати рекомендації щодо удосконалення глобальної інституційної структури інформаційного суспільства;

– визначити рівень фрагментації міжнародного права шляхом порівняльного аналізу тенденцій до глобалізації та регіоналізації міжнародно-правового регулювання питань розвитку глобального інформаційного суспільства;

– встановити причини появи та рівень ефективності «допоміжних» наднаціональних регуляторів суспільних відносин, опосередкованих використанням Інтернету;

– здійснити аналіз міжнародно-правових питань *per se*, зокрема забезпечення прав людини онлайн, захисту і транскордонної передачі персональних даних як прикладів адаптації міжнародного права до вирішення проблем, пов'язаних із розвитком глобального інформаційного суспільства;

– з'ясувати нормотворчу спроможність міжнародних судових інституцій з питань розвитку глобального інформаційного суспільства на підставі аналізу відповідної судової практики;

– визначити особливості міжнародно-правового регулювання співробітництва держав у сфері забезпечення кібербезпеки, вирішення конфліктів, що виникають у кіберпросторі, та використання кіберпростору як специфічного середовища для завдання кібератак;

– охарактеризувати стан нормативної готовності України до інтеграції в європейське і глобальне інформаційне суспільство та надати пропозиції щодо реформування національного законодавства у сфері розбудови інформаційного суспільства.

Об'єктом дослідження є суспільні відносини, що виникають у зв'язку з формуванням глобального інформаційного суспільства та відповідні трансформаційні процеси у міжнародному праві, пов'язані з його прогресивним розвитком як нормативною реакцією на технологічний прогрес.

Предметом дослідження є прогресивний розвиток міжнародного права як нормативна реакція на трансформуючий вплив глобального інформаційного суспільства.

Гіпотезою дослідження є припущення про те, що нормативне відображення змін у суспільних відносинах, зумовлених формуванням глобального інформаційного суспільства, сприятиме прогресивному розвитку міжнародного права та призведе до поступового переходу від державоцентричної до людиноцентричної системи міжнародно-правового регулювання у досліджуваній сфері, заснованої на моделі багатосторонньої співпраці між усіма зацікавленими сторонами (державами, міжнародними організаціями, приватним сектором, громадянським суспільством, технічною та академічною спільнотами).

Методи дослідження. У дисертаційному дослідженні використовується сучасний методологічний інструментарій, що включає в себе загальнонаукові та спеціальні методи наукового пізнання.

Серед загальнонаукових методів автор використовує діалектичний та історико-логічний методи, що дозволяють розглянути процес конвергенції глобального інформаційного суспільства та міжнародного права від їх протиставлення до синергії, встановити тенденції їх подальшого розвитку та взаємодії, а також простежити еволюцію доктринальних підходів в аспекті відображення окреслених питань (підрозділи 1.1, 1.2, 1.3). За допомогою семантичного методу надано визначення ключових понять, зокрема глобального інформаційного суспільства, кіберпростору, принципу мережевої нейтральності, прав людини онлайн, тощо (підрозділи 1.1, 2.1, 3.1).

Окреме місце у ході наукового дослідження займають системно-структурний та системно-функціональний методи, широке застосування яких обумовлене вивченням трансформаційного впливу глобального інформаційного суспільства на систему міжнародного права як в аспекті її внутрішньої структури, так і розширення регуляторної спроможності (підрозділи 2.1, 2.2, 2.3). Синергетичний метод дозволяє поглянути на еволюцію міжнародного права з точки зору нелінійних процесів розвитку глобального інформаційного суспільства (підрозділи 1.2, 1.3, 2.2). Методи індукції та дедукції, аналізу та аналогії виявилися особливо доречними при дослідженні судової практики та при виявленні тенденцій її розвитку і впливу на відповідну нормотворчу діяльність на міжнародному та національному рівнях (підрозділ 2.3).

У роботі були також застосовані спеціальні методи: порівняльно-правовий та метод правового моделювання, які зробили можливим комплексний аналіз ряду національних, регіональних та універсальних режимів у контексті окремих аспектів розвитку глобального інформаційного суспільства та його інституційної структури, а також дозволили виявити відповідні прогалини у нормативному регулюванні та сформувати пропозиції щодо підвищення ефективності останнього (підрозділи 1.3, 2.2, 3.1, 3.2, 3.3). Метод аналогії дозволив виявити схожість режиму кіберпростору з

режимами, що були свого часу закріплені для відкритого моря та космічного простору. Завдяки цьому ж методу вдалося також обґрунтувати доцільність визнання Інтернету у якості об'єкту загальної спадщини людства (підрозділ 1.1). Метод класифікації застосовується при розмежуванні прав людини онлайн та офлайн (підрозділ 3.1).

Наукова новизна одержаних результатів полягає у тому, що дисертація є одним із перших різнобічних, системних досліджень особливостей перетворюючого впливу глобального інформаційного суспільства на прогресивний розвиток міжнародного права. При цьому, глобальне інформаційне суспільство визначається не як новий міжнародно-правовий феномен, а як об'єктивно існуючі правопорядок та правовідносини, трансформаційний потенціал яких окреслює тенденції еволюції сучасного міжнародного права. За результатами проведеного дослідження сформульовано наступні основні положення, в яких розкривається його наукова новизна та які винесені на захист як особистий внесок дисертантки.

Уперше:

– надано авторське визначення понять «глобальне інформаційне суспільство», «кіберпростір», «права людини онлайн», «принцип мережевої нейтральності» у контексті міжнародного права;

– розроблено авторську періодизацію адаптивності міжнародного права до розвитку глобального інформаційного суспільства;

– доведено, у тому числі на конкретних прикладах (права людини онлайн, захист і транскордонна передача персональних даних та кібербезпека), багатовекторний та системний позитивний трансформуючий вплив глобального інформаційного суспільства на прогресивний розвиток міжнародного права;

– обґрунтовано зростаючий нормотворчий та стандартоутворюючий потенціал міжнародних судових інституцій при застосуванні міжнародного права до вирішення суперечок, що виникають з питань розвитку глобального інформаційного суспільства.

Удосконалено:

– розуміння співіснування різних нормативно-правових джерел з питань розвитку глобального інформаційного суспільства з наголосом на тому, що мірою високої виконуваності норм не завжди є їх юридична обов'язковість;

– обґрунтування доцільності переходу від державоцентричної до людиноцентричної системи міжнародно-правового регулювання з питань розвитку глобального інформаційного суспільства, заснованої на моделі багатосторонньої співпраці між усіма зацікавленими сторонами (державами, міжнародними організаціями, приватним сектором, громадянським суспільством, технічною та академічною спільнотами);

– класифікацію інституційних механізмів розвитку глобального інформаційного суспільства, а також питань його розвитку, що знайшли своє відображення у відповідних міжнародно-правових актах;

– обґрунтування доцільності вироблення універсальних міжнародно-правових режимів з питань розвитку глобального інформаційного суспільства, зокрема у сферах захисту і транскордонної передачі персональних даних та кібербезпеки.

Отримали подальший розвиток:

– пропозиції щодо доцільності відмови від безумовного застосування концепцій територіальної юрисдикції та державного суверенітету у контексті кіберпростору на користь концепцій розподіленого суверенітету та багатосторонньої участі всіх зацікавлених сторін у прийнятті відповідних рішень;

– тенденції формування транснаціонального права кіберпростору, що передбачає закріплення нормотворчої функції за ширшим колом суб'єктів;

– ідея про допустимість поширення на Інтернет як глобальну інформаційно-комунікаційну інфраструктуру статусу об'єкта загальної спадщини людства;

– концепція «м'якого» права як інструмента унормування суспільних відносин в інформаційній сфері;

– пропозиції щодо визнання доступу до Інтернету у якості самостійного права людини, а також удосконалення механізмів та засобів правового захисту прав людини онлайн.

Теоретичне і практичне значення одержаних результатів. Наукове значення результатів дисертаційного дослідження полягає в тому, що сформульовані висновки та теоретичні положення можуть сприяти подальшому розвитку науки міжнародного права та бути корисними у практичній діяльності, зокрема для реформування національного законодавства України в інформаційній сфері, а також обґрунтування зовнішньополітичної позиції нашої держави з питань розвитку інформаційного суспільства. Зібраний науково-практичний матеріал і висновки можна застосовувати у подальших дослідженнях міжнародно-правового регулювання різноманітних аспектів розвитку глобального інформаційного суспільства, зокрема захисту прав людини онлайн, міжнародно-правового режиму захисту і транскордонної передачі персональних даних, протидії кіберзагрозам та гарантування кібербезпеки тощо. Положення дисертації можуть бути використані в навчальному процесі при розробці навчальних посібників, підручників і методичних матеріалів, а також при викладанні нормативних дисциплін «Міжнародне публічне право», «Права людини у міжнародному праві», «Міжнародне інформаційне право», «Міжнародно-правове регулювання глобальних комунікацій», «Міжнародно-правові аспекти управління Інтернетом».

Особистий внесок здобувача. Дисертаційне дослідження виконане дисертанткою особисто. Усі висновки, узагальнення, припущення, пропозиції зроблені автором завдяки самостійній дослідницькій роботі, аналізу джерельної бази – міжнародно-правового регулювання, судової практики та доктринальних праць, на які подано відповідні посилання, а також на основі власної практичної діяльності здобувача у сфері правового забезпечення процесів розбудови інформаційного суспільства в Україні.

Апробація результатів дисертації. Дисертацію заслухано та обговорено на засіданні кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка. Основні положення та ключові ідеї дисертаційного дослідження оприлюднені у виступах і публікаціях на десяти наукових конференціях: трьох Міжнародних науково-практичних конференціях «Шевченківська весна» (м. Київ, 3 квітня 2014 року, 2 квітня 2015 року, 7 квітня

2016 року) (тези опубліковано), двох Міжнародних науково-практичних конференціях «Актуальні проблеми міжнародних відносин» (м. Київ, 16 жовтня 2014 року, 22 жовтня 2015 року) (тези опубліковано), Міжнародній науково-практичній конференції «Геостратегічні пріоритети України в політичній, економічній, правовій та інформаційній сферах» (м. Київ, 15 жовтня 2015 року) (тези опубліковано), Міжнародній науковій конференції *«Challenging Media Landscapes Conference: Exploring Media Choice and Freedom»* (Манчестер, Великобританія, 17-18 листопада 2014 року), Міжнародній науково-практичній конференції «Конституційна реформа та модернізація в Україні на шляху до європейської інтеграції» (м. Київ, 4 липня 2014 року), Міжнародній науково-практичній конференції «Інтереси України: міжнародно-правовий захист» (м. Київ, 28 серпня 2014 року), Міжнародній науково-практичній конференції «Майбутнє політичних реформ в Україні» (м. Київ, 26 вересня 2014 року).

Автор дисертації у період з жовтня 2014 року по грудень 2015 року надавала експертну підтримку Офісу Ради Європи в Україні в рамках Спільного проекту Ради Європи та ЄС «Зміцнення інформаційного суспільства в Україні». У період із серпня по грудень 2015 року здійснювала функції менеджера проекту «Права людини та Інтернет», який був спрямований на формування знань та навичок свідомого користування Інтернетом, навчання правам людини онлайн та запуск механізмів реагування на їх порушення. У червні 2014 року брала участь у парламентських слуханнях на тему «Законодавче забезпечення розвитку інформаційного суспільства в Україні». У березні 2017 року представила результати дослідження під час участі у глобальній зустрічі ICANN58 у Копенгагені (Данія) та міжнародній конференції *RightsCon* у Брюсселі (Бельгія).

Публікації. Основні положення та висновки дисертаційного дослідження отримали відображення в семи наукових статтях у фахових виданнях, перелік яких затверджено МОН України, у двох статтях в іноземних фахових виданнях, одній статті в інших виданнях, шести опублікованих тезах доповідей у матеріалах міжнародних науково-практичних конференцій, а також у дописі в колективну

монографію та двох розділах дослідження, виконаного на замовлення Офісу Ради Європи в Україні.

Структура та обсяг дисертації обумовлені метою та задачами дослідження й дозволяють послідовно розглянути теоретичні та практичні аспекти обраної теми. Дисертаційна робота складається зі вступу, дев’яти підрозділів, об’єднаних у три розділи, висновків та списку використаних джерел.

Загальний обсяг дисертації складає 247 сторінок, з яких обсяг основного тексту становить 211 сторінок. Список використаних джерел складається з 334 найменувань, викладених на 36 сторінках.

РОЗДІЛ 1
МІЖНАРОДНО-ПРАВОВІ ОСНОВИ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

1.1. Концепція глобального інформаційного суспільства та міжнародне право

Упродовж кількох останніх десятиліть інформація перетворилася на основний продукт виробництва та стала невід'ємною характеристикою сучасного суспільства. Темпи розвитку інформаційно-комунікаційних технологій змушують людину швидко пристосовуватися до нових обставин, які постійно змінюються. Інформаційна ера зумовлює необхідність перегляду традиційного порядку організації економічних та політико-правових відносин як всередині держави, так і на міжнародній арені. Кількісне зростання інформації зумовило виникнення якісно нової соціальної системи – глобального інформаційного суспільства.

У попередні тисячоліття трансформація соціальної системи практично не зачіпала правові засади функціонування суспільства. Основні зміни стосувалися соціально-економічних взаємовідносин між людьми. Натомість поява інформаційного суспільства зумовлює необхідність перегляду таких фундаментальних правових концепцій як суверенітет, територія, кордони та юрисдикція. Потреба у якісно новому механізмі правового регулювання пояснюється, в першу чергу, швидкими темпами розвитку сучасних інформаційно-комунікаційних технологій (надалі – «ІКТ»), зростанням кількості Інтернет-користувачів, тісним переплетенням фізичного світу та кіберпростору, консервативністю та повільністю державоцентричного нормотворення.

У доктрині міжнародного права та міжнародно-правових документах доволі активно використовується поняття інформаційного суспільства, хоча його змістове

наповнення все ще залишається предметом гострих суперечок. На рівні побутового розуміння інформаційне суспільство доволі часто ототожнюють з Інтернетом. Однак, такий підхід може бути визнаний лише частково правильним, оскільки поняття інформаційного суспільства є значно ширшим та охоплює Інтернет як інфраструктурну основу свого існування і розвитку. На думку Кастеллса, інформаційне суспільство є новою формою організації суспільства, у якому виробництво, зберігання, пошук та використання інформації відіграють ключову роль. Виникають нові структурні елементи та мережі, які формують так зване «мережеве суспільство» [1, с. 13-18].

Глобальне інформаційне суспільство формується на основі взаємодії автономних груп, кожна з яких має власну кіберідентичність та добровільно співпрацює з іншими задля досягнення загального миру, безпеки та економічного добробуту. В інформаційному суспільстві ключова роль відводиться інформації, якість та доступ до якої зазнають суттєвих змін. За останні 30-40 років світ перетворився в інформаційно-орієнтований простір більше, ніж будь-коли раніше. Інформація стала важливим, життєво необхідним компонентом сучасного суспільства. І, хоча, інформація як така існувала завжди, її значимість, якість, швидкість розповсюдження ще ніколи не відгравали настільки значну роль як на теперішньому етапі розвитку людства [2, с. 12].

Концепція глобального інформаційного суспільства ґрунтується на принципі рівних можливостей. Історія міжнародного права свідчить про те, наскільки конфліктними можуть бути міждержавні відносини в силу нерівномірного розподілу природних ресурсів, що неодмінно позначається на впливовості держави в міжнародних органах та інституціях. Утилітаризм, що лежить в основі взаємодії суверенних держав, не може бути запорукою стійкого міжнародного миру. Саме тому пропонується надати Інтернету статус об’єкту загальної спадщини людства, доступ до якого надається всім і кожному без будь-якої дискримінації за умови дотримання норм та принципів його функціонування. Встановлення належності Інтернету до об’єктів загальної спадщини людства наразі носить характер *de lege ferenda* та потребує подальшого визнання з боку держав та затвердження у

міжнародних договорах. Нормативне закріплення статусу критичного ресурсу глобального інформаційного суспільства як *res communis* буде логічним продовженням політичного діалогу з питань управління Інтернетом та фактично закладе основу багатосторонньої моделі, що наразі визнана найбільш ефективною для обговорення питань розвитку суспільних відносин в інформаційній сфері. Застосування в контексті Інтернету концепції загальної спадщини людства дозволить гарантувати рівність можливостей та сталий розвиток як технологічно розвинених країн, так і країн, що розвиваються. Концепція загальної спадщини людства цілком гармонічно вписується у процес перетворення цифрового розриву у цифрові можливості. Прикладом може слугувати застосування аналогічного режиму по відношенню до відкритого моря, космічного простору та Антарктики. Крім того, дана концепція слугуватиме ще однією гарантією мирного використання кіберпростору та стримування нарощування військового кіберпотенціалу. Інтернет є глобальним ресурсом, що не може бути привласнений жодною державою, натомість повинен бути об'єктом спільного управління в інтересах та на користь всього людства, а також використовуватися виключно у мирних цілях.

На думку Тома Стоньєра, постіндустріальний світ є більш демократичним, процвітаючим, ресурсомістким та менш схильним до війни як засобу вирішення міждержавних конфліктів. Інформаційні технології розглядаються автором як такі, що допоможуть вирішити екологічні проблеми епохи індустріалізму. Використання нових ІКТ зведе до мінімуму загрозу війни за аналогією зі зникненням рабства в індустріальну еру. Демократизація суспільного життя пов'язується з автоматизацією процесів управління, доступністю інформації, безпосередньою участю Інтернет-користувачів у прийнятті рішень [3, с. 122]. Втім, розвиток ІКТ значною мірою залежить від політики держави у цій сфері. Наукові технологічні дослідження часто фінансуються державами з політичних, а не соціальних мотивів, та швидше мають за мету досягнення військової, а не економічної переваги.

Поява концепції глобального інформаційного суспільства пов'язується із соціально-політичними та технологічними трансформаціями в міжнародних відносинах. Спочатку дане поняття застосовувалося виключно користувачами,

провайдерами та профільними громадськими організаціями і лише згодом перейшло у наукову площину. Найбільшої популярності ідея формування суспільства нового типу набуває серед громадських активістів, які виступають за новий економічний і політичний порядок та багатосторонню систему глобального управління Інтернетом. Появу глобального інформаційного суспільства часто розглядають як логічний наслідок процесів глобалізації, які засвідчили неефективність державоцентричної системи міжнародних відносин у вирішенні глобальних проблем цифрової ери. А, отже, виникла потреба у якісно інших суб'єктах, здатних акумулювати та справедливо розподіляти ресурси глобальної цифрової мережі [4, с. 89].

При дослідженні процесів конвергенції глобального інформаційного суспільства та міжнародного права ми припустили, що перше виступає позитивною екстерналією (зовнішнім ефектом) по відношенню до останнього, оскільки сприяє його прогресивному розвитку. Так, Скринька Д. В. зазначає, що чимало важливих норм міжнародного права є результатом зусиль держав, спрямованих на координацію їхньої поведінки з метою вирішення проблеми зовнішніх ефектів [5, с. 103]. У даному контексті вважаємо цілком закономірним відображення питань розвитку глобального інформаційного суспільства у міжнародному праві.

Вважається, що концепція інформаційного суспільства виникла в Японії на початку 1960-х років. Серед вчених, які вперше використали дане поняття у своїх творах, називають імена М. Ігараші, Дз. Камішіми, К. Курокави, Т. Умесао. Вже у 1971 році був виданий перший японський словник інформаційних суспільств. В англомовній літературі термін вперше з'являється у 1970 році в роботі Й. Масуди. Цілком імовірно, що спроби описати зміни у суспільному житті, пов'язані зі зростанням ролі інформаційних технологій, мали місце й раніше. Втім, вони були далекими від відображення будь-яких чітких позицій та не мали характеру комплексних досліджень.

Концепція інформаційного суспільства протягом тривалого часу пов'язувалася виключно з рівнем розвитку техніки. Вважалося, що інформаційне суспільство обмежується заходами лібералізації телекомунікаційної сфери. Натомість,

інформаційне суспільство повинно розумітися, в першу чергу, як таке, що охоплює освіту, науку, інновації, нову економіку, культуру та функціонує в рамках якісно нового правового поля. З часом, коли знання почали визнаватися ключовим елементом інформаційного суспільства, з'явилися альтернативні концепції суспільства знань. Дуже часто відбувалася некоректна підміна понять, які в силу доволі суб'єктивних причин протиставлялися одне одному. Одні вчені наголошували на тому, що інформаційне суспільство є одним із компонентів суспільства знань, пояснюючи це тим, що інформація є складовою частиною знання. Інша група вчених стояла на позиції, що термін «суспільство знань» є більш прогресивним порівняно із поняттям «інформаційне суспільство» і більш вдало відображає реальний стан відносин у суспільстві. Згодом була висловлена думка про те, що протиставляти ці два поняття некоректно, оскільки фактично вони мають однакове змістове наповнення.

Наразі існує величезна кількість термінологічних визначень інформаційного суспільства, що зосереджують увагу на тому чи іншому аспекті даного феномену. Різні автори визначали інформаційне суспільство як:

– суспільство, в основі якого лежать знання, та яке покликане забезпечувати соціальний контроль та управління інноваціями і змінами… (Д. Белл);

– новий тип суспільства, у якому володіння інформацією (а не матеріальними благами) є рушійною силою для трансформацій та розвитку […] (та у якому) процвітає інтелектуальна діяльність людей (Й. Масуда);

– економічну реальність, а не лише абстрактне поняття … поширення і розповсюдження інформації призводить до поступової появи […] нових видів діяльності та продукції (Дж. Нейсбіт);

– суспільство, у якому […] інформація використовується громадою як економічний ресурс, розвивається промисловість, що виробляє необхідну інформацію… (Нік Мур);

– новий тип суспільства, у якому людству надається можливість вести новий спосіб життя, мати вищий рівень життя, більш ефективно працювати та відчувати свою значущість у суспільстві завдяки глобальному використанню інформаційно-

комунікаційних технологій (Б. Мураньї) [6, с. 30, 34].

Кожне з вищенаведених визначень має в основі певний компонент життєдіяльності людини і суспільства, що на думку того чи іншого вченого є найбільш суттєвим для розуміння сутності інформаційного суспільства. Деякі визначення формуються навколо ресурсів, продуктів чи промисловості, у той час як інші – навколо певних видів діяльності, суспільства чи людини. Хтось ставить глобальне охоплення у центр поняття, натомість інші вчені не надають цьому жодної уваги. Для того, щоб максимально повно розкрити сутність розглядуваної концепції необхідно провести комплексний аналіз самого поняття.

Американський вчений Віктор Пікард розглядає питання побудови інформаційного суспільства через призму політико-економічної концепції неолібералізму. Автор переконаний, що в умовах інформаційного суспільства мову слід вести про два ключових суб'єкти, один з яких представляє країни третього світу на чолі з громадянським суспільством та неурядовими організаціями і виступає за рівні можливості та права, а інший, в особі розвинених країн та найбільших транснаціональних корпорацій, переслідує виключно економічну вигоду та прагне встановлення контролю над менш розвиненими та досвідченими країнами і народами [7].

Деякі автори виділяють також поняття глобального громадянського суспільства. Ян Аарт Шольте визначає його як «громадянську активність, що (а) стосується спільних для всього людства питань; (б) охоплює транскордонну комунікацію; (в) має глобальну структуру; (г) ґрунтується на принципі надтериторіальної солідарності» [8, с. 6]. Річард Прайс визначає транснаціональне громадянське суспільство як «взаємодію між уявними спільнотами, спрямовану на організацію колективного життя, не обмеженого територіальними та інституційними рамками держави» [9, с. 616].

У цілях даного дисертаційного дослідження буде використовуватися комплексне поняття «глобального інформаційного суспільства», під яким пропонується розуміти не просто нову суспільну формацію, а усю повноту правовідносин (правопорядок), що виникають в інформаційній сфері, а також

унікальне поєднання демократичних інституцій, політичних режимів, сприятливого для інновацій середовища та активного і структурованого громадянського суспільства, що виникли та розвиваються в рамках глобального та інклюзивного кіберпростору, у якому відсутні фізичні кордони.

У літературі існує підхід, відповідно до якого виділяється три способи співвідношення глобального інформаційного суспільства та міжнародної системи: заміщення, протидія та співіснування [10, с. 176]. Трансформація державоцентричної системи міжнародних відносин пов'язується з формуванням універсального суспільства в дусі ідей встановлення верховенства права на глобальному рівні та забезпечення вічного миру, висловлених у свій час ще Кантом [11, с. 325]. Глобальне інформаційне суспільство у даному випадку розглядається як альтернатива державній формі устрою суспільного життя, що заснована на глобальній ідентичності безвідносно до громадянства особи. У цифрову еру глобальне управління повинне здійснюватися таким чином, щоб гарантувати максимальну безпеку кожної людини як суб'єкта правовідносин у кіберпросторі. Оскільки держави не змогли створити ефективну та дієву систему глобального управління на глобальне інформаційне суспільство покладаються великі надії як на універсальну спільноту, що буде охоплювати кожного індивіда у кожній державі світу та сприятиме утвердженню верховенства права, справедливості та єдиних демократичних цінностей [12, с. 99]. Протидія глобального інформаційного суспільства державній системі організації суспільного життя розпочинається в момент, коли транснаціональні мережеві спільноти протиставляють себе державі, яка, використовуючи потенціал своїх громадян, слугує задоволенню інтересів національних еліт. Натомість, у кіберпросторі створюються дійсно рівні умови для кожного індивіда, де він сам обирає членом якої мережевої спільноти ставати і яким нормам та принципам підкорятися. З іншого боку, цілком раціональним буде збереження суверенних прав національних держав щодо тих питань, які традиційно входили до сфери їх відання. Однак, регулювання кіберпростору як сфери взаємодії індивідів в умовах універсального середовища без кордонів повинне здійснюватися іншими ніж держави та міжнародні організації суб'єктами на основі якісно нових

принципів. Досі прерогатива перетворення ідей у правові норми належала виключно державам та міжнародним організаціям. З появою кіберпростору виникла потреба визнання нормотворчих повноважень також за іншими суб'єктами. Деякі автори у якості приклада успішності співпраці держав, міжнародних організацій та громадянського суспільства наводять міжнародні-правові акти у сфері прав людини. Вони стверджують, що держави пішли назустріч вимогам національних та транснаціональних недержавних акторів, закріпивши на міжнародному рівні широкий спектр прав та свобод людини і громадянина [13, с. 146]. При цьому соціальна спрямованість держави та гарантування прав людини змушують національні уряди суттєво обмежувати інтереси правлячої еліти.

Основою глобального інформаційного суспільства є співпраця між взаємозалежними та рівноправними спільнотами, що керуються нормами неагресивної ввічливості, виробленими в ході багатостороннього діалогу. Концепцію глобального інформаційного суспільства часто пов'язують із кризою сучасної системи міжнародних відносин та необхідністю прийняття якісно нових міжнародно-правових норм. З появою Інтернету правова природа транснаціональної взаємодії зазнала суттєвих змін. Транснаціональна співпраця впродовж тривалого часу розглядалася як частина інтеграційних процесів. Розвиток глобальної цифрової мережі зробив можливим спілкування, обмін інформацією та ідеями між індивідами та окремими спільнотами незалежно від державних кордонів [14, с. 85]. Ідеальне глобальне інформаційне суспільство можна представити у вигляді правової моделі, ключовими цінностями якої є справедливість, свобода та рівність. Однак, глобальне інформаційне суспільство не є однорідним утворенням, а тому потребують врегулювання правовідносини між самими мережевими суб'єктами.

З появою глобальних інформаційних мереж з'явилися не лише нові можливості, але й чимало викликів та загроз, з якими раніше людству не доводилося мати справу. Набули актуальності питання забезпечення прав людини онлайн, підтримання балансу між свободою вираження поглядів та приватністю, захисту прав інтелектуальної власності в Інтернеті, протидії кібератакам, зміцнення інформаційної безпеки та боротьби з кіберзлочинністю, які знайшли своє

відображення у розділі 3 дисертації. Постало також питання щодо ефективності ключової для міжнародного права концепції державного суверенітету, оскільки глобальні мережі за своєю природою є транскордонними та децентралізованими. Державам необхідно максимально оперативно пристосовуватися до взаємодії в межах нового глобального середовища в умовах розвитку технологій, що так чи інакше вимагає перегляду концепції державного суверенітету. Як слушно зазначає Франка Філхо, з інституційної точки зору глобалізація передбачає конвергенцію політичних, економічних та правових регуляторних механізмів держав, а в економічному контексті також обмеження суверенітету державних органів, відповідальних за національну економічну політику [15].

Ще одним базовим поняттям цього дисертаційного дослідження є кіберпростір, що формує технологічну основу глобального інформаційного суспільства. У Рекомендації ЮНЕСКО про розвиток і використання багатомовності та загальний доступ до кіберпростору 2003 року кіберпростір визначається як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою [16]. На нашу думку, кіберпростір має дихотомічну природу. З одного боку, він являє собою специфічну сферу, в межах якої здійснюється обіг товарів та послуг, відбувається комунікація та реалізація прав людини, ведеться боротьба за розподіл сфер впливу, що з іншого боку, стає можливим лише через використання відповідних інформаційно-комунікаційних технологій. На нормативному рівні потребують вирішення як технологічна складова, так і складова людської взаємодії в межах кіберпростору.

Перегляд концепції державного суверенітету є необхідною передумовою еволюції держави в умовах глобального інформаційного суспільства, де взаємозалежність суб'єктів стає все більш очевидною. Однак, слід чітко усвідомлювати, що глобалізація та технологічна революція не означають позбавлення держави повноти її влади. На думку Матіаса, повинен відбутися перерозподіл окремих функцій держави між міжнародними, транснаціональними та наднаціональними інституціями, оскільки з появою нової моделі глобального управління повнота влади держави як невід'ємна характеристика її суверенітету

більше не відповідає реаліям міжнародних правовідносин [17, с. 241].

Як справедливо зазначає Пінхейро, з появою кіберпростору зникають звичні нам фізичні межі, натомість з'являється нематеріальний, віртуальний світ. Кіберпростір являє собою віртуальне середовище, доступ до якого ми можемо отримати лише через комп'ютер, який виконує функцію посередника між двома світами [18, с. 62].

Кордони відігравали ключову роль у Вестфальській системі міжнародних відносин, відповідно до якої держави встановили територіальні межі та домовилися про мирне співіснування. Впродовж тривалого часу кордони слугували своєрідними бар'єрами, що захищали політичні, правові та економічні інтереси суверенних держав. Втім, глобалізація змусила по-новому подивитися на концепцію кордонів. Зростаюча кількість транскордонних транзакцій нівелює їх первинну значимість. У той же час, подібні міжнародні операції можуть мати місце лише у світі, розділеному кордонами. Інтеграційні процеси в Європі, що привели до створення Європейського Союзу, сприяли перетворенню сприйняття кордонів як фізичних бар'єрів на їх розуміння у якості географічних меж. Держави-члени ЄС, незважаючи на створення спільного ринку та значну лібералізацію, продовжують зберігати правовий та політичний контроль над внутрішніми справами з метою захисту своїх народів. Тобто, інституційні кордони виявляються необхідними навіть за умов, коли фізичні кордони втрачають свою роль [19].

На думку професорів Д. Джонсона та Д. Поста у кіберпросторі існують власні кордони у вигляді моніторів та паролів, що відокремлюють реальний світ від віртуального. Кіберпростір потребує створення спеціального правового регулювання та правових інституцій, відповідальних за підтримання правопорядку в його межах. Нові правові норми повинні будуть регулювати явища та концепції, що не мають аналогу у фізичному світі. Досі територіальні кордони між державами світу співпадали з межами правової юрисдикції останніх. Кордони чітко свідчили про те, що при їх перетині особа повинна буде дотримуватися правових норм іншої держави. Розвиток глобальної комп'ютерної мережі руйнує зв'язок між територією та повноваженнями національних урядів встановлювати контроль над онлайновою

поведінкою. Передача інформації та повідомлень у мережі не залежить від місцезнаходження конкретних суб'єктів. Значення мають лише віртуальні адреси комп'ютерів, між якими відбувається обмін. Навіть доменні імена далеко не завжди є свідченням належності комп'ютера до конкретної територіальної юрисдикції [20, с. 1373].

Сучасні суверенні держави надзвичайно стурбовані транскордонною передачею даних, що потенційно можуть завдати шкоду місцевому населенню. Вводяться невиправдані обмеження з метою захисту інформаційного суверенітету, приватного життя та власності. У дійсності ж потенціал ІКТ щодо транскордонної комунікації в рази перевищує спроможність держав створити належні правові рамки для регулювання суспільних відносин такого типу. Держави роблять спроби застосовувати захисні механізми у вигляді блокування та фільтрування контенту, заборони доступу до окремих Інтернет-ресурсів, втім їх ефективність залишається низькою. Це пояснюється тим, що завжди можна знайти технічні способи обходу накладених нормативних заборон. Розробка правових стандартів з урахуванням технологічної складової дозволила б сформувати якісно кращий масив нормативних приписів.

Як доречно зазначає А. Пазюк, інформаційна сфера розвивається на відкритій екстериторіальній основі та, відповідно, вимагає впорядкування засобами міжнародного права [21, с. 31]. При цьому вчений наголошує на рамковому характері міжнародного інформаційного права [21, с. 82] та звертає увагу на певний конфлікт із суверенним правом держав регулювати суспільні відносини в рамках національної інформаційної інфраструктури [21, с. 85].

Практично усі види людської діяльності, пов'язані з передачею інформації, як наприклад освіта, охорона здоров'я, банківське обслуговування, надання нематеріальних послуг, публікація художніх творів, можуть здійснюватися онлайн. Однак, закони, що регулюють суспільні відносини у вказаних сферах, мають виключно територіальний характер. В умовах глобального інформаційного суспільства територіальна прив'язка більше не виконує роль ідентифікатора компетентного правопорядку, якому повинні підпорядковуватися суб'єкти

інформаційних правовідносин. У класичній правовій думці глобальна мережа розглядається виключно у якості інструмента, що прискорює обмін повідомленнями, надісланими з однієї юрисдикції в іншу, кожна з яких має власні правові приписи.

Традиційно в теорії міжнародного права географічні кордони визначали межі юрисдикції держави. Відповідно, всі особи, які знаходяться на території певної держави, повинні дотримуватися її законів. Крім того, презюмується, що держава може поширювати свою юрисдикцію на випадки, коли протиправна поведінка іноземних громадян зашкоджує її інтересам чи безпеці. Разом з тим, негативні наслідки онлайнової діяльності можуть бути відчутними одночасно у кількох територіальних юрисдикціях, що піднімає питання про застосовний правопорядок.

Ключова особливість Інтернету полягає у тому, що він не належить жодному суб'єкту міжнародного права, однак зачіпає інтереси кожного з них, а відтак створює ситуацію, коли кожен заявляє права на участь у процесі створення нового світового правопорядку. Держави виявляються неспроможними захищати власні інтереси, а також права фізичних та юридичних осіб, що знаходяться під їх юрисдикцією, коли відсутня будь-яка територіальна прив'язка.

Автор погоджується з позицією професора Центру права Джорджтаунського університету Д. Поста, який наголошує на тому, що застосування територіальної прив'язки за принципом місцезнаходження веб-сервера буде абсолютно неефективним та створить практично необмежені можливості для маніпулювання з розміщенням контенту, забороненого в одних країнах, на веб-серверах в іншій країні, де законодавчі вимоги не такі суворі [20, с. 1384].

Усупереч загальнопоширеному уявленню кіберпростір не є однорідним утворенням. У його межах присутні численні групи суб'єктів, що наділені специфічними характеристиками і взаємодіють за власними правилами. Пост переконаний, що ідеальний регулівний механізм для кіберпростору повинен базуватися на принципі децентралізації правотворчого процесу та бути чимось на зразок електронного федералізму, коли повнота влади належить конкретним провайдерам доступу до мережі, а не суверенним державам. За таких умов

користувачі делегують право створювати обов'язкові до виконання норми провайдерам, а самі залишаються вільними у виборі онлайн спільноти, правилами якої вони будуть керуватися у майбутньому. Реальним наслідком такого правотворення стане поява мережевих конфедерацій, кожна з яких матиме власні принципи та норми. В основі сучасного нормотворчого процесу, на думку вченого, повинен бути суверенітет індивіда, а не держави, його вибір та згода на підпорядкування конкретним міжнародно-правовим нормам, застосовним до кіберпростору. Вважаємо, що попри певну утопічність зазначених ідей у транскордонному вимірі, подібна система уже засвідчила свою ефективність на рівні створення мережевих правил поведінки, так званого нетикету. Багаторівневість кіберпростору та багатовимірність питань, пов'язаних з його функціонуванням, потребують нормативної залученості усіх зацікавлених суб'єктів. Концепція багатосторонньої участі здійснює трансформуючий вплив на міжнародне право у контексті розподілення нормотворчих функцій з питань розвитку глобального інформаційного суспільства.

Концепція кордонів також набуває нового звучання у міжнародному праві. На зміну фіксованим географічним кордонам між суверенними державами приходить кордон між фізичним середовищем та кіберпростором. Перетин цієї межі, що відбувається через під'єднання до глобальної мережі, повинен символізувати, як і у випадку з територіальною юрисдикцією держав, перехід у сферу дії якісно іншого правового поля. Іншими словами, сучасне міжнародне право досягло тієї критичної точки, коли вироблення механізмів регулювання глобального інформаційного суспільства стало вкрай необхідним. Спроби застосування традиційних правових концепцій до онлайнових правовідносин поступово засвідчують свою неефективність.

Суто з логічної точки зору, нематеріальний та всеохоплюючий за своєю природою кіберпростір не може функціонувати за територіальними законами суверенних держав. У контексті застосування авторського права онлайн доволі цікавою є думка Джейн Гінсбург, на думку якої ключовою рисою глобальної інформаційної інфраструктури є її здатність до одночасного розповсюдження

авторських творів у кожній точці світу. У даному аспекті принцип територіальності викликає чимало труднощів, якщо його тлумачити як такий, що приводить у дію національні закони кожної держави, де стає можливим доступ до опублікованого авторського твору, адже такі закони можуть суттєво відрізнятися між собою. При цьому, виникає логічне запитання про необхідність оцінювання усіх можливих правових наслідків відповідно до законодавства кожної держави, де авторський твір буде опубліковано [22, с. 319-320]. Дійсно, складно не погодитися з вченою у тому, що існування правової територіальності неможливе без географічної прив'язки, яка, однак, зникає у глобальному інформаційному просторі. Фізичні кордони, таким чином, перестають бути константою та основою міжнародного правотворення з питань розвитку глобального інформаційного суспільства.

Суспільні відносини у цифрову еру зазнали суттєвих змін. Класичні концепції міжнародного права потребують перегляду з урахуванням технологічного прогресу та специфічних характеристик онлайнового середовища, яке все частіше стає платформою для проведення численних транзакцій. Імовірно, найбільш доступним підтвердженням раціональності утворення окремого правового механізму для кіберпростору буде його порівняння з торговельним правом. Останнє виникло у відповідь на швидкий розвиток міждержавної торгівлі, коли феодальне право з його локальним характером перестало відповідати реальним потребам торгового обороту. Сучасне міжнародне право виникло як система норм, спрямована на регулювання фізичного, матеріального простору та суспільних відносин, що виникають у його межах. Саме тому поява альтернативного, онлайнового середовища з унікальними рисами потребує перегляду існуючих регуляторних механізмів міжнародного права.

Саморегулювання у жодному випадку не повинно порушувати охоронювані державою права, свободи та інтереси тих осіб, що ніколи не перетинали кордон між фізичним світом та кіберпростором. Взаємовідносини між державою та саморегулівними онлайновими спільнотами повинні відбуватися на основі взаємної поваги та стримування.

Дуже цікаву думку у даному контексті висловлює Сандел, який вбачає у саморегулюванні спосіб перерозподілу державного суверенітету. Учений відкидає

ідею створення космополітичної спільноти на засадах солідарності всього людства в силу її ірраціональності, натомість пропонує передати частину суверенітету транснаціональним інституціям та локальним спільнотам, що відповідатиме потребам глобального ринку та інтересам користувачів [23, с. 73-74]. Такий підхід органічно переплітається з нашою позицією про необхідність переходу від державоцентристської міжнародно-правової системи з питань розвитку глобального інформаційного суспільства до моделі багатосторонньої співпраці між усіма зацікавленими сторонами.

Інтернет можна розглядати у якості нації, до якої належить кожен, хто користується онлайновими послугами та інструментами. Це, у свою чергу, піднімає питання представництва та прав Інтернет-користувачів [24]. Наразі значна частина цих прав не знаходить адекватного захисту в мережі в силу відсутності відповідних правових механізмів, на чому ми зупинимося більш детально у підрозділі 3.1.

По суті, глобальне інформаційне суспільство є формою транснаціонального громадянського суспільства, яке через використання потенціалу сучасних інформаційно-комунікаційних технологій здатне впливати на утвердження принципів демократії та свободи в системі глобального управління. Концепція національних інформаційних суспільств завдячує своєю появою колективному усвідомленню національної єдності, в основу якої покладено культурну самоідентичність та приналежність нації до певної території в рамках державних кордонів.

Традиційно існування народу пов'язувалося з приналежністю до певної суверенної держави. Концепція глобального інформаційного суспільства не оперує поняттями народу та держави, нехтуючи географічними кордонами у їх класичному розумінні. Ключовою цінністю визнається людина, яка наділяється реальною повнотою влади в рамках відкритого, інклюзивного суспільства, в основу функціонування якого покладено використання потенціалу ІКТ. Саме в такому суспільстві права та свободи людини можуть бути реалізовані найбільш повно.

Нерозуміння сутності правової природи глобального інформаційного суспільства пов'язане з виключно описовим характером існуючих наукових

досліджень у даній сфері. Фактично, глобальне інформаційне суспільство є складним феноменом, що поєднує концепції глобалізації, громадянського суспільства та використання ІКТ у цілях розвитку людства. Під глобалізацією ми розуміємо сукупність правових, політичних, економічних та культурних процесів, що стирають межу між сферами внутрішньої та зовнішньої компетенції держави тим самим зумовлюючи детериторіалізацію та денаціоналізацію суспільного життя. Процеси глобалізації передбачають якісну трансформацію сучасної системи міжнародних відносин, зумовлюють виникнення нових загроз та викликів міжнародному миру та безпеці, а також послаблюють роль держави у міжнародному нормотворчому процесі. Таким чином, виникає потреба у формуванні нової системи глобального управління.

Сутність громадянського суспільства стає зрозумілою з його визначення як підпорядкованого правовим та моральним нормам і принципам суспільства, в основі якого лежить вільна згода індивідів та завдяки приналежності до якого останні можуть впливати на законодавство та політику, що приймається суверенними державами, покликаними представляти їх інтереси. Наразі громадянське суспільство у формі різноманітних асоціацій, об'єднань, спільнот виступає активним учасником міжнародних відносин, хоча й без права голосу при прийнятті рішень. Формування поліцентричного глобального суспільства розширює межі впливовості громадянського сектору.

Сучасні ІКТ мають величезний потенціал для забезпечення розвитку, процвітання та добробуту всього людства. Вони є інфраструктурною основою мережевих спільнот, діяльність яких не знає державних кордонів. На противагу монополії держави у контексті реалізації владних повноважень концепція глобального інформаційного суспільства передбачає неієрархічну, саморегулівну та технологічно орієнтовану соціальну структуру, в рамках якої на засадах рівності взаємодіють різноманітні мережеві спільноти. Фактично, йдеться про застосування вже відомої міжнародному праву концепції громадянського суспільства в умовах нового глобалізованого світу, що характеризується поступовим відходом від державоцентризму у міжнародних відносинах та стрімким розвитком

транскордонних цифрових мереж. Наразі маємо ситуацію, коли на практиці реально сформувався і функціонує новий об'єкт міжнародно-правового регулювання – суспільні відносини, опосередковані використанням Інтернету, однак досі відсутнє саме міжнародно-правове регулювання та механізми глобального управління інформаційним суспільством. Крім того, необхідно чітко розуміти кому належатимуть представницькі функції та хто нестиме відповідальність за будь-які зловживання та порушення в умовах глобального інформаційного суспільства.

Наприкінці 1970-х років XX ст. розуміння важливості інформації перемістилося з виключно академічної до політичної площини. До того моменту, коли постіндустріальне суспільство поступилося місцем інформаційному суспільству, первинне розуміння останнього було абсолютно розмитим та заново окресленим у контексті політичної складової. Ключовим суб'єктом у структурі нового суспільства визнавався приватний сектор, у той час як уряди та глобальні інституції повинні були взяти на себе відповідальність за створення політичного та регуляторного середовища, сприятливого для процесів приватизації та лібералізації. Незважаючи на інформаційну складову, нове суспільство перш за все переслідувало економічні цілі. Поняття «інформаційне суспільство» мало ідеологічне забарвлення і тим самим відділяло інформацію від комунікаційних процесів [25, с. 205-208].

Цікавим у контексті даного дослідження є встановлення доктринальної наступності у вивченні процесу еволюції міжнародного права. Ґрунтовний аналіз взаємодії правової та економічної систем міститься в роботі Д. Скриньки, який звертає увагу на появу нових тенденцій у правовому регулюванні, пов'язаних з особливостями функціонування економічних систем, які неможливо було врахувати раніше. При цьому розвиток економічних відносин може призводити до поступової зміни підходів до правових категорій [26]. Аналогічні трансформації у міжнародному праві продовжують відбуватися й зараз, тільки тепер уже у відповідь на технологічний прогрес, пов'язаний з появою Інтернету та глобалізацією суспільних відносин в інформаційну еру.

Наразі доволі складно, якщо взагалі можливо, провести межу між індустріальним суспільством та інформаційним у контексті того, коли кожна

конкретна країна перетнула цю межу. На сьогоднішній день усі розвинені країни можна впевнено віднести до категорії інформаційних суспільств, чого не скажеш про країни, що розвиваються. Вони і досі не мають доступу до найбільш прогресивних досягнень у сфері інформаційно-комунікаційних технологій. Утім, сам доступ без попереднього належного навчання відповідним навичкам та умінням не принесе бажаного результату. Саме тому доволі гостро постають питання використання інформаційно-комунікаційних технологій у цілях розвитку та стійкого зростання.

Прийнято вважати, що США стали на шлях інформаційного суспільства на початку 1960-х років, Японія - на 10-15 років пізніше. На початку 1990-х років до них приєдналася більшість розвинених країн. Значна частина країн Африки, Азії та Латинської Америки й досі є далекими від цієї мети. Таким чином, говорити про глобальне інформаційне суспільство можна буде лише тоді, коли буде подолано найбільш очевидні диспропорції розвитку інформаційно-комунікаційних технологій, коли високі показники найбільш розвинених країн перебуватимуть у відносному балансі із наразі дуже низькими показниками країн, що розвиваються. Такий передовий процес розробки новітніх ІКТ у найбільш розвинених країнах є цілком логічним. Головний проблемний момент полягає у тому, щоб шлях поширення цих технологій до найменш розвинених країн залишався відкритим, а самі технології були для них матеріально доступними.

Одним із найбільших недоліків сучасного політичного та правового дискурсу в контексті прав людини є надмірна концентрація на питаннях доступу до Інтернету як єдиної та ключової складності. Цим пояснюється велика кількість обговорень щодо скорочення цифрового розриву, створення рівних можливостей та використання ІКТ як ідеального рішення усіх проблем країн, що розвиваються. Насправді ж, технології самі по собі не є панацеєю. Наслідки їх застосування залежать від того, в чиїх руках знаходиться управління їх використанням.

У листопаді 2015 року Бостонська консалтингова група опублікувала щорічний (з 2011 року) Індекс інтенсивності Інтернету (*BCG e-Intensity Index*), що відображає рівень зрілості 85 Інтернет-економік світу. Індекс складається з трьох

компонентів (доступність мережі, активність користувачів та об'єм продажів через Інтернет) та охоплює 28 держав-членів ЄС, більшість країн Латинської Америки та Азії, а також 14 африканських країн. З показників індексу чітко видно, що багаті країни стають багатшими, а бідніші повільно їх наздоганяють. Таїланд та Китай досягли найкращих показників. Багато країн Центральної та Східної Європи показали кращі результати, ніж можна було очікувати в силу стану їх економік, однак багато латиноамериканських держав отримали низький рейтинг [27].

У той же час, у доповіді Світового Банку розглядаються причини поширення цифрових технологій, а не цифрових дивідендів. По-перше, близько 60% населення світу не мають доступу до Інтернету та не можуть брати достатню участь у цифровій економіці. По-друге, деякі з можливих переваг цифрових технологій перекриваються появою нових ризиків. У зв'язку з цим недивно, що більш освічені, з безперешкодним доступом до Інтернету та більш здібні отримують більшість переваг, уникаючи при цьому цифрової революції [28].

За попередніми прогнозами очікується, що світ зможе досягти рівня глобального інформаційного суспільства до 2018-2020 років. Утім, і надалі буде зберігатися тенденція цифрового розриву, оскільки темпи розвитку країн світу все ще будуть різними. Тим не менше, такий розрив буде поступово скорочуватися.

Поряд із теоретичними розробками почали виникати перші міжнародно-правові ініціативи, спрямовані на нормативно-правове забезпечення процесу формування інформаційного суспільства. Так, у рамках Європейського співтовариства у 1994 році був прийнятий план дій «Європейський шлях до інформаційного суспільства» [29], який передбачав чотири основні напрямки діяльності Європейського Союзу у цій сфері: створення нормативно-правового простору; розвиток інформаційних і телекомунікаційних мереж, класифікація основних послуг, стандартизація обладнання; вивчення різноманітних соціальних і культурних аспектів інформаційного суспільства; пропаганда концепції формування інформаційного суспільства серед населення з метою отримання суспільної підтримки. План дій часто називають «Ініціативою Бангеманна» на честь одного з керівників Комісії Європейського співтовариства, який очолив групу експертів, що

підготувала рекомендації Комісії щодо вжиття термінових заходів для забезпечення входження країн ЄС до інформаційного суспільства.

У лютому 1995 року Європейська комісія заснувала Форум для обговорення загальних проблем становлення інформаційного суспільства. Члени Форуму представляють користувачів нових технологій, різноманітні соціальні групи, постачальників контенту і послуг, операторів мережі, державні та міжнародні інституції. Форум покликаний моніторити процес становлення інформаційного суспільства у шести сферах:

- вплив на економіку та зайнятість;
- основні соціальні та демократичні цінності у віртуальному просторі;
- вплив на суспільні та державні служби;
- освіта, перекваліфікація, навчання в інформаційному просторі;
- культурний вимір та майбутнє ЗМІ;
- сталий розвиток, технології та інфраструктура.

У 1996 році в ЄС була випущена Зелена книга «Життя і праця в інформаційному суспільстві: спочатку люди». У документі йдеться про створення нових робочих місць, захист прав і свобод громадян, перш за все недоторканності особистого життя [30].

У відповідь на появу «Ініціативи Бангеманна» у багатьох країнах світу (Німеччина, Франція, Великобританія, Австрія, Чехія, Японія, Індія, країни Південно-Східної Азії, тощо) розпочалася розробка і реалізація національних концепцій розвитку інформаційного суспільства. Зокрема, у 1995 році Фінляндія підготувала свою програму «Фінський шлях до інформаційного суспільства», у лютому 1996 року урядом ФРН була представлена програма дій «Шлях Німеччини до інформаційного суспільства». Азійські концепції розвитку інформаційного суспільства, як правило, базуються на утвердженні власних ціннісних орієнтирів і прагненні розробити альтернативний західному підхід до індустріалізації та соціального розвитку [31, с. 46-47].

Розбудова інформаційного суспільства є одним із зобов'язань України перед Європейським Союзом у рамках виконання Угоди про асоціацію, що була

синхронно ратифікована сторонами у вересні 2014 року (ст. 389-395). Зокрема, зазначається, що сторони зміцнюють своє співробітництво щодо 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 та надходженню інвестицій у цю галузь. Сторони сприяють поступовому наближенню до права і нормативно-правової бази ЄС у галузі регулювання інформаційного суспільства і електронних комунікацій [32]. Наразі в Україні продовжує діяти застарілий закон «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 2007 р., план дій щодо реалізації якого не було виконано повною мірою. Досі не розроблено план дій щодо реалізації національної Стратегії розвитку інформаційного суспільства в Україні на 2016-2020 роки [33].

У 2000 році країнами великої «вісімки» було прийнято Окінавську Хартію глобального інформаційного суспільства. У документі наголошується на тому, що кожна людина повинна мати можливість користуватися тими благами, які надає глобальне інформаційне суспільство. Саме тому, пріоритетним напрямком діяльності визнається скорочення розриву у доступі до інформаційних технологій між розвиненими країнами та країнами, що розвиваються. Країни повинні будувати свою взаємодію на основі просування соціального та економічного прогресу у всьому світі [34].

Таким чином, міжнародне право відіграє ключову роль у побудові глобального інформаційного суспільства. Воно покликане створити міцну нормативну основу, на базі якої стане можливим сформувати суспільство, у якому всі його члени матимуть рівний доступ до інформаційно-комунікаційних технологій та знань, отриманих з їх використанням. Наразі міжнародно-правові норми у сфері формування та розбудови глобального інформаційного суспільства мають здебільшого декларативний характер та закріплюють найважливіші положення і стандарти, які в подальшому повинні бути деталізовані у національних нормативно-правових актах.

На жаль, досі концепція глобального інформаційного суспільства не стала предметом детального правового аналізу. Це може бути пояснено двома основними причинами. По-перше, впродовж тривалого часу дана концепція розглядалася виключно у соціальній та технологічній площинах. По-друге, навіть поверхневе ознайомлення з особливостями кіберпростору та функціонуючої на його основі нової соціальної системи робить очевидною необхідніть пристосування класичних концепцій сучасного міжнародного права до вимог інформаційної ери. Зростаюча роль недержавних акторів, нівелювання значимості географічних кордонів, швидкість та універсальність поширення інформаційних потоків призводять до ситуації, коли держави та існуючі міжнародні організації виявляються не просто неготовими до перегляду діючої системи міжнародного права, але й абсолютно не бажають поступатися своїм місцем у цій системі та виключним правом міжнародного нормотворення на користь недержавних суб'єктів. Фактично, ми стаємо свідками нового перехідного періоду в історії людства. А трансформаційні процеси не бувають швидкими та безболісними, особливо коли йдеться про необхідність перегляду правових основ функціонування суспільства та перерозподілу владних повноважень між класичними суб'єктами міжнародного права і новими акторами на міжнародній арені. Держави не так скоро, якщо взагалі поступляться своїм виключним правом міжнародного нормотворення. Хоча вони й розуміють необхідність перелаштування та пристосування діючих механізмів та чинних міжнародно-правових норм для раціонального вирішення проблем та врегулювання суспільних відносин, що виникають у кіберпросторі або у зв'язку з ним. Про це свідчить зростаюча кількість форумів та зустрічей на міжнародному рівні, що проводяться за принципом багатосторонньої участі. Однак, недержавні суб'єкти маючи доступ до таких обговорень, так і не отримали право голосу при вирішенні питань глобального управління, що безпосередньо зачіпають їх інтереси. Держави та міжнародні організації визнають моральний авторитет громадянського суспільства, приватного сектору та академічної спільноти, втім не поспішають розглядати їх у якості рівноправних суб'єктів міжнародного нормотворення.

Глобальне інформаційне суспільство є складним феноменом, що існує на

стику соціології, політики і права та має в своїй основі технологічний прогрес. Імовірно, сам термін не є класичною правовою дефініцією, звичною для слуху правника, однак, поняття «глобального інформаційного суспільства» з надзвичайною точністю передає всю суть суспільних трансформацій у сучасному технологічно орієнтованому та інформаційно залежному світі. Абсолютно логічно, що поява нового суспільного феномену вимагає створення відповідних правових рамок його функціонування. Динамічність технологічного прогресу сприяла прояву індетермінізму міжнародного права з питань розвитку глобального інформаційного суспільства, продемонструвавши потребу у створенні «живого», рефлективного та ефективного механізму міжнародно-правового регулювання у досліджуваній сфері із залученням до процесу нормотворення усіх зацікавлених сторін.

Вважаємо, що переведення у нормативну площину питань становлення глобального інформаційного суспільства сприятиме прогресивному розвитку міжнародного права. Наразі правова та соціальна системи досягли того рівня синергії, коли очевидним є не лише трансформуючий вплив глобального інформаційного суспільства на міжнародне право, але й стає невідворотним нормативне закріплення правових основ та стандартів функціонування та еволюції такого суспільства. Авторське визначення глобального інформаційного суспільства містить прогресивний компонент та передбачає подальшу адаптацію міжнародного права в аспекті подолання його територіальності при регулюванні транскордонних суспільних відносин у межах глобального та інклюзивного кіберпростору. Еволюцію трансформуючого впливу глобального інформаційного суспільства на міжнародне право буде розкрито у наступному підрозділі.

1.2. Питання розвитку глобального інформаційного суспільства у міжнародному порядку денному: історичний огляд

У ході дослідження еволюції адаптації міжнародного права до процесів розвитку глобального інформаційного суспільства ми зіштовхнулися з системною нестачею класифікації ключових етапів такої еволюції. Наявні доктринальні періодизації

розмежовують історію становлення міжнародного права та глобального інформаційного суспільства, не об'єднуючи їх в рамках однієї класифікації. Втім, новизна нашого дослідження і полягає у тому, щоб показати, що розвиток глобального інформаційного суспільства став точкою біфуркації для міжнародного права та сприяв його переходу на більш високий рівень упорядкованості, з одночасним розширенням його регуляторної спроможності. Приклад періодизації етапів розвитку міжнародного інформаційного права залежно від домінуючих технологічних засобів комунікації можна знайти у дисертації А. Пазюка, який розрізняє наступні етапи: писемність (з VIII тис. до н. е.), друковане видавництво і преса (з XVI ст.), телеграф, телефон і радіо (з поч. XIX ст.), супутникове радіомовлення (з 1970-х рр. XX ст.), супутникове телебачення, комп'ютеризація і телекомунікації (з 1990-х рр. XX ст.), мультимедійні засоби (з поч. XXI ст.) [21, с. 38].

У свою чергу, І. Забара у якості класифікуючої ознаки міжнародно-правового регулювання інформаційних відносин використовує концепції розвитку таких відносин, виокремлюючи наступні періоди: 1945-1970 рр. (концепція «необмеженої свободи інформації»), 1970-1990 рр. (концепція «нового міжнародного інформаційного порядку»), 1990 - до сьогодні (концепція «інформаційного суспільства») [35, с. 39-45].

Ми ж пропонуємо авторську періодизацію, в основу якої покладено поворотні моменти в історії трансформуючого впливу глобального інформаційного суспільства на міжнародне право. На думку автора, перші відчутні результати взаємопроникнення міжнародного права та питань розвитку глобального інформаційного суспільства можна помітити у документах, прийнятих у ході обговорень з питань розбудови нового світового інформаційно-комунікаційного порядку (надалі – «НСІКП») (1970-ті – 1990-ті рр. XX ст.). Наступний етап конвергенції бере свій відлік з 2003 року та пов'язується з початком проведення Всесвітнього саміту інформаційного суспільства (надалі – «ВСІС»). Оцінка здобутків цього історичного періоду та перехід до наступного етапу відбувається наприкінці 2015 року із ухваленням Фінального документу ВСІС+10. Підведення підсумків цього етапу очікується у 2025 році. Крім того, паралельним поступом розвивається імплементація Плану дій «*Connect 2020*» та цілей сталого розвитку ООН на період до 2030 року. Для більшої наочності перейдемо до

безпосереднього аналізу еволюційних процесів.

НСІКП фактично став першою спробою відкритого та глобального обговорення цілого спектру питань, пов'язаних з ІКТ та їх значенням у процесі розбудови інформаційного суспільства. Активно відстоювали новий інформаційний порядок країни-учасниці Руху неприєднання ООН, число яких значно зросло внаслідок процесів деколонізації та появи нових незалежних держав. Це, в свою чергу, призвело до значних змін у біполярному світі, де досі уся повнота протистояння відбувалася між США та СРСР. Країни третього світу почали активно заявляти про необхідність рівномірного розподілу світових економічних ресурсів, збереження культурної ідентичності та створення нового міжнародного економічного порядку.

Інтеграція нових незалежних держав до глобальної системи зв'язку відбувалася на фоні невідповідної інфраструктури, нерівномірних потоків інформації та незбалансованої цінової політики. Переважання західних інформаційних потоків, трансформація індустрії зв'язку та зростаюча роль підконтрольних Заходу технологій створювали атмосферу вимушеної залежності країн, що розвиваються, на подолання якої і був спрямований новий світовий інформаційний порядок.

НСІКП вперше стає предметом обговорення у 1973 році в Алжирі на четвертій конференції глав держав та урядів країн, що не приєдналися. Конференція підкреслила необхідність підтвердження незалежності національних культур і усунення шкідливих наслідків колоніальної ери. Було запропоновано провести симпозіум, присвячений проблемам масової інформації та створити пул інформаційних агентств. Концепція НСІКП відігравала важливу роль у боротьбі країн, що розвиваються за деколонізацію їх інформаційного життя та запровадження нового міжнародного порядку у сфері інформації. Країни, що розвиваються були стурбовані тим, що імперіалістичні зазіхання Заходу не обмежуються виключно політичною та економічною сферами, але звернені також у бік культурного та соціального життя. Цим пояснювалася необхідність об'єднання зусиль з метою захисту сфери масових комунікацій. У тому ж 1973 році під час свого виступу на колоквіумі у Стенфордському університеті директор корпорації суспільного радіомовлення США Н. Кацман зазначив, що найновіші комунікаційні технології не лише не вирішать існуючі, але призведуть до виникнення нових

соціальних проблем, оскільки вони будуть загострювати класові протиріччя і сповільнювати самостійний розвиток технічно відсталих держав [36].

У травні 1975 року в Белграді відбулася підготовча зустріч, на якій обговорювалися питання, що повинні були увійти до порядку денного Симпозіуму з питань інформації, запланованого на березень 1976 року. У серпні 1975 року в Лімі проходить П'ята конференція міністрів закордонних справ, за результатами роботи якої було прийнято резолюцію «Співпраця у сфері поширення інформації та засоби масової інформації». Симпозіум з питань інформації відбувся в Тунісі та ознаменувався прийняттям заключної доповіді «Емансипація засобів масової інформації в країнах, що не приєдналися», в якій містилися пропозиції щодо вивчення потенціалу ЗМІ в цих країнах та створення регіональних центрів для обміну досвідом. Фактично, це була спроба вирішити проблему поширення інформаційних потоків, що формуються в країнах-учасницях Руху неприєднання. Туніський симпозіум сформулював практичні поради для поступового переходу до нового світового інформаційного порядку.

У результаті конференції в Делі, що відбулася кількома місяцями пізніше (липень 1976 року), було прийнято два документи – Декларацію міністрів інформації країн, що не приєдналися та Резолюцію про план дій для розвитку співпраці у сфері інформації та обміну масовою інформацією. Зрештою, на зустрічі на вищому рівні в Коломбо у серпні 1976 року була прийнята Політична декларація, в якій новий міжнародний порядок у сфері інформації та масових засобів зв'язку визнавався настільки ж важливим, як і новий міжнародний економічний порядок. Виділяють чотири міжрегіональні органи співпраці держав, що не приєдналися у сфері обміну інформацією: Міжурядова координаційна рада, Міжнародний комітет експертів з питань телекомунікацій, Пул інформаційних агентств та Об'єднання органів радіо- та телемовлення [37].

Новий порядок мав своєю метою об'єднання зусиль у сфері масової комунікації, однак зовсім скоро стала очевидною необхідність включення НСІКП як складової частини до більш широкої концепції політики розвитку країн третього світу. НСІКП передбачав далекосяжні реформи, які повинні були зачіпати усі види інформації (політичну, соціальну, економічну та технічну), ЗМІ (пресу, радіо, телебачення) та всі форми комунікаційних технологій.

У той самий час СРСР пропонує прийняти Декларацію про засоби масової інформації під егідою ЮНЕСКО. Дана ініціатива, спрямована на вироблення універсальних принципів щодо ролі ЗМІ у міжнародних відносинах, викликала протистояння з боку західних та північних країн, які вважали, що таким чином може бути порушений принцип «вільного потоку інформації». Переговори щодо прийняття Декларації тривали під час конференції ЮНЕСКО в Найробі у 1976 році.

У листопаді 1978 року на Генеральній конференції ЮНЕСКО було прийнято Декларацію про основні принципи щодо ролі засобів масової інформації у зміцненні миру та міжнародного взаєморозуміння, поширенні прав людини та протидії расизму, апартеїду і підбурюванню до війни [38]. Домовленість щодо Декларації про засоби масової інформації була досягнута доволі швидко завдяки взаємним поступкам, у межах яких розвинені країни запропонували інфраструктурну допомогу країнам, що розвиваються в обмін на їх готовність відмовитися від деяких суттєвих вимог щодо змісту документу. Найбільші суперечки все ж розгорнулися навколо запропонованих поправок до доктрини вільного потоку інформації, яку Західні країни відстоювали як передумову гарантування свободи комерційної преси. Зрештою, ця доктрина була видозмінена і передбачала тепер вільний потік та більш збалансоване поширення інформації, що в ідеалі повинно було призвести до якісного покращення інформаційного контенту. У відповідь на даний документ у 1981 році критиками нового інформаційного порядку була прийнята Таллуарська декларація.

Фактично, доктрина вільного потоку інформації покликана була захистити економічні інтереси США на міжнародній арені. Сформульована Комісією з питань свободи преси ще у середині 1940-х років минулого століття та покликана вирішити проблему якісного інформаційного контенту дана доктрина отримала нове дихання вже у 1970-х роках. Як зазначає Г. Шиллер, період після Другої світової війни був надзвичайно сприятливим для необмеженого поширення інформації. Він також вважав, що риторика щодо вільних потоків інформації, яка використовувалася американськими корпораціями для уникнення будь-яких регуляторних обмежень, передбачала інформаційну експансію, й аж ніяк не лібералізацію [39, с. 57]. Західні демократії наполегливо переконували світову спільноту у тому, що держава не повинна втручатися

у регулювання інформаційних потоків, порушуючи тим самим свободу преси та інформаційну відкритість.

Країни, що розвиваються активно виступали за подолання дисбалансу в інформаційному обміні. Втім, кількісне урівноважування різновекторних потоків інформації ще не означало структурних змін інформаційної системи та якісного перетворення контенту. Не існувало єдиного розуміння того наскільки негативним є вплив інформаційних потоків, що формуються в країнах Заходу, на країни, що розвиваються.

У грудні 1977 року ЮНЕСКО сформувала Міжнародну комісію незалежних експертів для вивчення інформаційних та комунікаційних проблем, яку очолив Нобелівський лауреат Шон Макбрайд. Комісія почала роботу над звітом, що мав доволі цікаву назву – «Багатоголосий, але єдиний світ» [40]. Доповідь Макбрайда була схвалена на Генеральній конференції ЮНЕСКО у 1980 році. Документ визначав новий світовий інформаційно-комунікаційний порядок як процес, а не просто як сукупність умов та дій. За своїм змістовим наповненням Доповідь була більш вагомим документом порівняно з Декларацією про засоби масової інформації. Зокрема, у Доповіді піднімаються наступні питання:

1. Зміцнення незалежності та самодостатності – невід'ємне право на краще життя, покращення комунікаційних можливостей, розвиток базових комунікаційних потреб населення. Розглядаються також перешкоди на шляху до майбутнього міжнародного розвитку;

2. Соціальні наслідки НСІКП та нові завдання – пропонується визнавати комунікацію складовою частиною процесів розвитку, розглядаються потенційні можливості та небезпеки технологічних викликів, зміцнення культурної ідентичності, сповільнення комерціалізації процесів комунікації та покращення доступу до технічної інформації;

3. Професійна єдність та стандарти: відповідальність журналістів, покращення рівня міжнародних репортажів (повне та достовірне висвітлення новин) та захист журналістів;

4. Демократизація процесів комунікації – забезпечення прав людини, усунення

перешкод для обміну інформацією, підтримання розмаїття ЗМІ та змісту інформаційних повідомлень (децентралізовані та численні ЗМІ), а також залучення широких мас населення до процесів обміну інформацією;

5. Заохочення міжнародної співпраці – сприяння партнерству у цілях розвитку, подолання економічних протиріч, зміцнення колективної самодостатності та посилення міжнародної співпраці;

6. Надання фінансового сприяння менш розвиненим країнам: нестача необхідних комунікаційних ресурсів вимагає додаткового міжнародного фінансування, джерелами якого можуть бути надлишковий прибуток від сировини, міжнародні податки на використання електромагнітного спектру та геостаціонарного орбітального простору чи податок на доходи транснаціональних корпорацій, що виробляють лінії електропередачі.

У цей період наголос робився на необхідності демократизації міжнародних відносин. Існувало чітке усвідомлення того, що переформатування інформаційно-комунікаційної сфери на міжнародному рівні дозволить провести радикальні зміни у глобальних владних відносинах [41, с. 42]. Відповідні трансформації у сфері технологій вимагали нового нормативного регулювання.

Дискусії з приводу Доповіді Макбрайда були спровоковані зростаючим протистоянням між країнами світу, що було викликане наступними факторами:

– невідповідність рівня розвитку інформаційних технологій у розвинених країнах Заходу та їх південних колоніях;
– незбалансованість руху інформації;
– існування двох протидіючих інформаційних таборів – західноєвропейського з його колоніями та СРСР з країнами соціалістичного табору;
– наявність антиколоніального руху в країнах Африки та Південно-Східної Азії.

Інформаційно-політичний поділ світу у XX ст. носив полярний і груповий характер, а в рамках кожної групи існували домінуючі держави, що формували інформаційну політику в регіоні в цілому [42, с. 241].

Генеральна конференція ЮНЕСКО, що відбулася в Белграді у 1980 році, прийняла «Міжнародну програму розвитку процесів комунікації» на виконання пункту 78 Доповіді Макбрайда. Сама ж доповідь викликала невдоволення США, що у 1984 році

вийшли зі складу ЮНЕСКО, звинувативши організацію в надмірній політизації. Прикладу США послідувало Сполучене Королівство. Така позиція впливових держав викликала фінансову неспроможність ЮНЕСКО та призвела до зникнення питань нового інформаційно-комунікаційного порядку з порядку денного цієї організації.

У 1989 році на 25-й сесії Генеральної конференції ЮНЕСКО була прийнята «Нова стратегія комунікації», яка перемістила акцент із збалансованого обміну інформацією на забезпечення свободи слова та друку. На думку ряду дослідників, містком між НСІКП та «Новою стратегією» стала Міжнародна програма розвитку комунікації. Передбачалося, що її реалізація зможе допомогти країнам, що розвиваються звільнитися від зовнішнього інформаційного та культурного панування шляхом зміцнення власних комунікаційних інфраструктур.

У 1999 році була видана колективна монографія «До справедливості в глобальній комунікації: Макбрайд сьогодні». На думку авторитетного фінського вченого К. Норденстренга, перспективи глобального інформаційного суспільства не лише поставили хрест на дебатах про НСІКТ, але й дали їм новий поштовх. Термінологія та риторика змінюються, але суть проблеми значною мірою залишається незмінною і буде доповнена новими компонентами технологічного та соціального характеру [43]. Інший автор колективної монографії М. Тегранян переконаний у тому, що НСІКТ слід визначати як сукупність інформаційних мереж між структурами, що формують громадянське суспільство на глобальному рівні, як місток, що перекинутий від державних акторів до недержавних, від периферії до центру у цілях боротьби з насиллям та бідністю [44].

Подальше зростання популярності Інтернету у різних країнах світу у 90-х роках XX ст. відновило діалог щодо створення дієвого регуляторного механізму в інформаційному середовищі. Найбільш обговорюваними виявилися питання конструювання технічної інфраструктури та розподілу доменних імен.

Діалог з питань глобального інформаційного та комунікаційного порядку в рамках Міжнародного союзу електрозв'язку (надалі – «МСЕ») розпочався із прийняття у 1998 році резолюції, у якій йшлося про проведення під егідою ООН Всесвітнього саміту інформаційного суспільства (надалі – «ВСІС») [45]. Згідно з резолюцією 56/183 ГА ООН

основною метою ВСІС було визнано 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 [46]. Ключовими питаннями, які повинні були бути розглянуті під час ВСІС визнавалися управління Інтернетом, безпека, вільне та відкрите програмне забезпечення, комунікаційні права, інтелектуальна власність, права людини та фінансування.

Під час ВСІС вперше за всю історію проведення самітів під егідою ООН право висловити свою позицію отримали представники приватного сектору та громадянського суспільства. ВСІС став важливою відповіддю на ті фундаментальні зміни, що відбувалися у суспільстві та були пов'язані з трансформацією останнього в контексті нової інформаційної ери. Саміт став поштовхом до співпраці на міжнародному рівні усіх зацікавлених суб'єктів з метою формування глобального інклюзивного інформаційного суспільства. Проведення Саміту у два етапи теж стало відмінною рисою цієї ініціативи. Такий підхід передбачав переоцінку цілей та аналіз досягнень з тим, щоб максимально повно реагувати на зміни, що відбуваються у суспільстві.

Фактично, ВСІС став першою серйозною подією міжнародного рівня, при підготовці до якої було створено реальні умови для широкого залучення громадянського суспільства до обговорення перспектив розвитку глобального інформаційного суспільства. ВСІС надав довгоочікувану можливість для колективного вирішення нагальних проблем у сфері ІКТ, вироблення взаємоприйнятних політичних рішень та формування глобального інформаційного суспільства.

Так, Марк Ребой вказує на те, що ВСІС був уже третьою спробою ООН глобально підійти до вирішення питань, пов'язаних з інформацією та комунікацією. У 1948 році з прийняттям Загальної декларації прав людини право шукати, отримувати та поширювати інформацію було визнане одним з базових прав людини. Наприкінці 1970-х років держави-члени Руху неприєднання виступили з ініціативою нового світового інформаційно-комунікаційного порядку. Показово, що 1948 рік ознаменувався консенсусом, натомість 1970-ті роки продемонстрували розрізненість світової громади та небажання йти на поступки [47, с. 225].

ВСІС 2003 та 2005 років ознаменував початок нового тисячоліття. Саміт не мав чітко окреслених цілей, однак повинен був певним чином формалізувати новий тип правовідносин, специфіка яких визначалася технологічним прогресом та зростаючою роллю інформації. ВСІС став чи не найпершим політично нейтральним форумом для обговорення ключових питань глобального значення в інформаційну еру. Застосування принципу багатосторонньої участі виявилося непростим завданням, оскільки самі представники громадянського суспільства не мали єдиної думки щодо питань, які вони хотіли б бачити на порядку денному. Так, одні з них наголошували на важливості прав людини, у той час як інші віддавали перевагу питанням сучасних медіа та комунікацій. Була й група, яку більше цікавив соціально-економічний потенціал ІКТ для країн, що розвиваються. Громадянське суспільство так само не мало єдиної позиції щодо того, яку роль слід відводити державам у механізмі глобального управління. Одні розглядали державу як ворога, інші – як ключового партнера. Громадянське суспільство під час ВСІС було настільки неоднорідним, що так і не змогло виступити єдиним фронтом та продемонструвати свою згуртованість [48].

У грудні 2003 року під час першого етапу Саміту в Женеві було прийнято Женевську декларацію принципів [49] та Женевський План дій [50], які описують загальне бачення інформаційного суспільства та кроки, які повинні бути вжиті для його побудови на глобальному рівні. У ході роботи у Тунісі учасниками цього етапу Саміту було затверджено Туніське зобов'язання [51] та Туніську програму для інформаційного суспільства [52], у яких розкривалися кроки по управлінню Інтернетом та наводилося робоче визначення управління Інтернетом. Таким чином, Женевський етап Саміту був присвячений вирішенню важливих соціальних проблем, натомість під час зустрічі у Тунісі акцент був зміщений на розгляд технічних питань, зокрема управління Інтернетом.

Женевська Декларація принципів 2003 року містить найбільш важливі цілі інформаційного суспільства, досягнення яких повинно слугувати задоволенню потреб населення у всьому світі. Найбільшої уваги заслуговують наступні принципи:

– роль урядів та усіх зацікавлених сторін у заохоченні використання інформаційно-комунікаційних технологій (ІКТ) у цілях розвитку поступово зростає та потребує

об’єднання зусиль;

– інформаційно-комунікаційна інфраструктура є необхідною основою для побудови інклюзивного інформаційного суспільства;

– надання доступу до інформації та знань усьому населенню;

– створення необхідних передумов для здобуття навичок і знань у сфері інформаційних технологій, у тому числі створення можливостей для безперервного навчання;

– зміцнення довіри і безпеки при використанні ІКТ;

– створення сприятливого середовища на національному та міжнародному рівнях є важливим елементом для забезпечення належного управління;

– удосконалення програм на базі ІКТ здатне принести суттєве покращення в усі сфери повсякденного життя;

– заохочення культурного різноманіття та ідентичності, мовного різноманіття та місцевого контенту слугують збереженню загальної спадщини людства;

– гарантування свободи ЗМІ та інформації;

– дотримання етичних норм інформаційного суспільства (солідарність, терпимість тощо);

– посилення міжнародної та регіональної співпраці [49].

Туніська програма для інформаційного суспільства 2005 року містить компромісне рішення щодо управління Інтернетом. Проблема полягає у тому, що для кожної групи зацікавлених сторін було передбачене власне місце у системі управління [53]. Так, повноваження щодо розробки державної політики залишалися за державами та міжурядовими організаціями. У віданні приватного сектору зберігалися питання розвитку Інтернету в технічній та економічній сферах [52]. Таким чином, відбулося штучне та непрактичне розподілення взаємопов’язаних політичних і технічних питань. При цьому держави опинилися на чолі механізму прийняття рішень, що абсолютно не відповідає їх ролі в інституційній структурі глобального інформаційного суспільства. Натомість нормативне закріплення функцій громадянського суспільства звелося всього лише до виконання важливої суспільної ролі.

Крім того, у фінальних документах ВСІС не було передбачено чіткого

інституційного механізму, до відання якого належали б питання, пов'язані з управлінням Інтернетом та інформаційним суспільством. Прийняття цього важливого рішення було відкладене. Своєрідним пробним механізмом став Форум з управління Інтернетом (надалі – «IGF»), що був створений як форум для багатостороннього діалогу, однак без будь-яких реальних можливостей для прийняття юридично обов'язкових рішень.

У свою чергу, Генеральний Секретар ООН повинен 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. Міжнародна спільнота досить неоднозначно відреагувала на необхідність розбудови режиму «посиленої співпраці». Більшість розвинених країн були переконані, що «посилена співпраця» уже має місце в рамках існуючих установ. Разом з тим, представники країн, що розвиваються виступали за створення нового міжнародного механізму, що повинен був стати платформою політики «посиленої співпраці».

Період між новим світовим інформаційно-комунікаційним порядком та Всесвітнім самітом інформаційного суспільства ознаменувався значними соціально-політичними трансформаціями, що призвели до структурних змін міжнародної системи. Втім, на той момент ще було зарано говорити про якісь вагомі трансформації регуляторного механізму, хоча окремі окремі нормативні зрушення вже ставали помітними.

Серед слабких сторін фінальних документів ВСІС голландський вчений К. Хамелінк [54] називає відсутність серйозного та критичного структурного аналізу політичних та економічних умов. Натомість інформаційне суспільство доволі детально розглядається у соціальній площині. Ключовими характеристиками інформаційного суспільства проголошуються його інклюзивність та відкритість, спрямованість на створення сприятливого середовища та підтримання нарощування потенціалу, сталого розвитку, культурного різноманіття та гендерної чутливості. За таких обставин складається враження, що інформаційне суспільство є ледь не ідеальною формою суспільного устрою, що спроможна вирішити усі існуючі проблеми та створити передумови для покращення життя кожної людини. Втім, фінальним документам ВСІС

вочевидь бракує дієвого механізму, здатного привести у виконання усі проголошені ідеї щодо побудови інформаційного суспільства, метою якого є благополуччя та добробут кожного.

Крім того, Хамелінк зазначає, що в ході своєї роботи ВСІС не звертається до вже існуючих міжнародних угод, що в тій чи іншій мірі регулюють питання міжнародного розвитку, зокрема, Угоди про телекомунікації 1997 року та Угоди про торговельні аспекти прав інтелектуальної власності 1993 року, прийнятих в рамках СОТ.

ВСІС залишає поза увагою також питання влади та контролю. На думку Л. Маклаглін, інституційна структура ВСІС є прикладом неокорпоративізму, що передбачає відповідні зміни в напрямку переходу до тристороннього механізму взаємодії в рамках ООН. ВСІС продемонстрував прагнення міжнародних неурядових організацій, урядів та бізнес-корпорацій до якомога більш широкого залучення громадянського суспільства до участі у різноманітних ініціативах з метою просування неоліберальних ідей [55].

Американський науковець В. Пікард проводить порівняльний аналіз між НСІКП і ВСІС та вказує на ряд відмінностей, що характеризують ці два ключові етапи у процесі формування глобального інформаційного суспільства. Так, він зазначає, що на відміну від НСІКП, який був започаткований в рамках ЮНЕСКО та носив переважно соціокультурний характер, ВСІС, проведений під егідою МСЕ, зробив більший акцент на технічних стандартах телекомунікацій. Відповідні зміни помітні й в стратегічному контексті. Якщо НСІКП був відверто політичною концепцією та відстоював інтереси держав, то у ВСІС була відсутня ідеологічна складова та передбачалося широке представництво міжнародних неурядових організацій та громадянського суспільства. Питання державного суверенітету втратило свою критичність. Об'єднання зусиль різних суб'єктів міжнародних відносин у ході роботи ВСІС для вирішення спільних соціальних проблем дозволило знизити рівень антагонізму між розвиненими країнами та країнами, що розвиваються. Порядок денний ВСІС також зазнав змін порівняно із НСІКП. Так, в рамках ВСІС вже не розглядалися питання транскордонного обміну інформацією, культурного різноманіття та регулювання змісту випусків новин. Автор переконаний, що замість того, щоб сконцентруватися на вирішенні соціальних несправедливостей та

виробленні конкретних політичних кроків, ВСІС був більше схильний підтримувати існуючу систему міжнародних відносин, звузивши коло переговорів виключно до технічних питань [7].

На думку італійської вченої К. Падовані, ВСІС надав можливість заново переглянути концептуальні питання соціальних трансформацій на початку XXI ст. Автор розглядає ВСІС у кількох ключових площинах: як комунікативну та медіа подію. У якості форуму для обміну думками Саміт сприяв виробленню міжнародно-правових документів, які, хоч і не мають юридично обов'язкового характеру, втім заклали основи так званого «світу слів». ВСІС також став платформою для ведення політичного діалогу між зацікавленими сторонами.

Характерною рисою порядку денного ВСІС була багатовекторність. Одночасно в центрі уваги учасників Саміту перебувала велика кількість важливих питань: інфраструктура, доступ, розширення можливостей, довіра та безпека, сприятливе середовище, застосування ІКТ, культурне та мовне різноманіття, етичні принципи інформаційного суспільства. Множинність прослідковується і в контексті учасників, документів, поштовхом до прийняття яких став глобальний діалог з питань інформаційного суспільства (Декларація громадянського суспільства 2003 р., Ліонська Декларація міністрів «Суспільство для всіх вікових груп: проблеми і можливості» 2007 р., Декларація прав корінних народів 2007 р. тощо), та зрештою у світлі самої ідеї побудови інформаційних суспільств в інтересах людини, закріпленої у Декларації громадянського суспільства.

Позитивною рисою у роботі ВСІС, як відмічає К. Падовані, стало об'єднання за переговорним процесом, хоч і не на рівних умовах, представників урядів, міжнародних організацій, бізнес структур, а також жінок, молодого покоління, корінних народів, громадських рухів та представників влади на місцях. Втім, досвід ВСІС продемонстрував, що над моделлю багатостороннього партнерства ще потрібно працювати з тим, щоб змусити її працювати ефективно в контексті розбудови глобального інформаційного суспільства [56].

У своїй пізнішій роботі [57] К. Падовані пише про важливість історичної наступності у вирішенні комунікаційних проблем. Натомість більшість вчених підходять

до їх розгляду як таких, що з'явилися лише у XXI ст. та стосуються переважно технологічних та інфраструктурних аспектів. Відповідно, і серед засобів реагування переважають, як правило, політичні інструменти.

У 2005 році К. Падовані публікує інтерв'ю з фінським вченим Каарле Норденстренгом, в якому піднімає питання історичної наступності між НСІКП і ВСІС, впливу ідей, висунутих ще у 70-ті роки минулого століття, на вирішення сучасних проблем, пов'язаних із розбудовою глобального інформаційного суспільства, а також наголошує на необхідності налагодження діалогу між поколіннями, активному використанні знань та досвіду тих вчених і науковців, що були свідками обох ключових етапів в історії розвитку інформаційного суспільства [58]. На нашу думку, абсолютно невиправданою в контексті історичної спадковості є позиція значної частини світової спільноти, відповідно до якої черговий етап у розвитку концепції інформаційного суспільства, який пов'язують із діяльністю ВСІС, розглядається як початкова сходинка, що не має нічого спільного із попередніми ініціативами у досліджуваній сфері. Підтвердженням цьому є хоча б той факт, що ключові питання НСІКП не втратили своєї актуальності і для ВСІС.

К. Норденстренг зазначає, що політичні обставини, за яких розгорталися НСІКП та ВСІС, були докорінно різними. У 70-х роках XX ст. світ був розділений на дві вісі – Схід-Захід та Північ-Південь. Холодна війна провела чітку межу між капіталістичними країнами Заходу та соціалістичним табором на Сході. Жодна зі сторін не відзначалася внутрішньою єдністю. Таким чином, НСІКП був не просто спрямований на вирішення тогочасних інформаційних та комунікаційних проблем, але й відображав геополітичний баланс сил на міжнародній арені. Наразі окреслені протиріччя або повністю зникли, або набули іншого окрасу. Крім того, в основі ВСІС лежить інформаційно-технологічний підхід, в той час як НСІКП був орієнтований на політичне вирішення існуючих проблем. Вважаємо, що ВСІС не просто розвинув ідеї, запропоновані ще у період НСІКП, але й запропонував якісно новий переговорний механізм, побудований за принципом багатосторонньої участі із залученням усіх зацікавлених сторін. Подібна модель інституціоналізації обговорень з питань глобального інформаційного суспільства стала вагомим кроком вперед у напрямку розвитку транскордонного співробітництва та

вироблення універсальних міжнародно-правових стандартів.

Згідно з авторською класифікацією наступним етапом розвитку глобального інформаційного суспільства пропонується вважати ВСІС+10. Так, Туніська програма для інформаційного суспільства передбачала перегляд досягнень ВСІС по завершенню 10-річного періоду з метою визначення подальших напрямків діяльності. У липні 2014 року Генеральна Асамблея ООН прийняла Резолюцію 68/302, відповідно до якої у грудні 2015 року було проведено дводенне засідання на вищому рівні у Нью-Йорку [59].

У контексті управління Інтернетом Фінальний документ ВСІС+10 не містить жодних новаційних ідей. У ньому визнається багатостороння модель управління Інтернетом, однак завжди міститься застереження про те, що зацікавлені сторони повинні діяти відповідно до своїх функцій та обов'язків. Такий стиль написання документу вкотре підтверджує верховенство держав поміж нібито рівних суб'єктів.

Так, у пункті 57 Фінального документу ВСІС+10 зазначається, що управління Інтернетом включає багатосторонні (*multilateral*), транспарентні, демократичні процеси за участі зацікавлених сторін, зокрема урядів, приватного сектору, громадянського суспільства, міжнародних організацій, технічних та академічних спільнот тощо, відповідно до їх функцій та обов'язків.

На включенні в текст документу поняття «*multilateral*» наполягав Китай, оскільки при усій своїй позитивній конотації воно передбачає керівну роль саме держав у процесі нормотворення. При цьому поняття «*multilateral*» використовується у тексті всього один раз, натомість «*multistakeholder cooperation*» з'являється втричі частіше. З одного боку, подібне поєднання протилежних за змістовим навантаженням принципів може здаватися дивним, а з іншого – є класичним прикладом компромісу та урівноважування різновекторних позицій найвпливовіших держав світу з метою вироблення єдиних загальноприйнятних норм та правил. Крім того, була визнана керівна роль держав у сфері кібербезпеки у тому, що стосується національної безпеки.

Слід також зазначити, що відповідно до Фінального документу ВСІС+10 (п. 31) державам при розбудові інформаційного суспільства рекомендується утримуватися від односторонніх дій, які б суперечили міжнародному праву та Статуту ООН. Втім, у фінальний текст не увійшли пропозиції щодо посилення звітності та підвищення

репрезентативності, особливо по відношенню до країн, що розвиваються [60].

Туніська програма для інформаційного суспільства містила положення щодо прав людини та кібербезпеки, однак ускладнення правовідносин у цих сферах зрештою зумовило визнання їх відособленої актуальності. Так, у Фінальному документі ВСІС+10 кожному з цих питань присвячено окремий розділ. Подібний ціннісний підхід було застосовано й при структуруванні третього розділу дисертації, де питанням прав людини онлайн та кібербезпеки присвячено окремі пункти, що пояснюється їх важливістю в умовах глобального інформаційного суспільства. У контексті прав людини у Фінальному документі було зроблено акцент на необхідності дотримання Загальної декларації прав людини та Міжнародного пакту про громадянські та політичні права. Втім, немає жодної згадки про Міжнародний пакт про економічні, соціальні та культурні права, що становлять особливий інтерес для країн, що розвиваються. Крім того, підтверджується, що правам людини повинен надаватися однаковий захист офлайн та онлайн. Окремий наголос робиться на таких правах, як доступ до інформації, свобода вираження поглядів та свобода об'єднань, для реалізації яких ІКТ стали сприятливим чинником.

У сфері кібербезпеки було визнано керівну роль держав з питань, що стосуються національної безпеки. Зміцнення довіри та безпеки у кіберпросторі повинно бути сумісним з дотриманням прав людини. Наголошується на необхідності посилення співпраці держав щодо боротьби з кіберзлочинністю та створення ефективних механізмів протидії.

Здобутком ВСІС+10 стало продовження мандату IGF на наступні 10 років. У документі підкреслюється ключова роль ІКТ для досягнення цілей сталого розвитку. Подолання цифрового розриву, розширення доступу до Інтернету та формування культури кібербезпеки утворюють своєрідну тріаду розвитку та продовжують залишатися на порядку денному ВСІС+10 [61].

Уцілому, мова Фінального документу ВСІС+10 витримана у компромісному дусі та обережних формулюваннях. Серед негативних моментів можна виокремити той факт, що у документі взагалі не згадується принцип мережевої нейтральності. Наступний перегляд здобутків ВСІС заплановано на 2025 рік, що в подальшому стане частиною

оціночного процесу у контексті досягнення цілей сталого розвитку у 2030 році.

Паралельно з процесами ВСІС ведеться робота по імплементації Плану дій «*Connect 2020*» - нової глобальної програми співпраці щодо розбудови інклюзивного інформаційного суспільства, що стала одним із головних здобутків Повноважної конференції МСЕ 2014 року. План дій розроблявся на основі багатостороннього діалогу та включає 4 загальні та 17 спеціальних цілей, які повинні бути досягнуті до 2020 року у контексті інклюзивності ІКТ, їх сталого розвитку, ролі інновацій та партнерства. Даний документ створює основу для посилення ролі ІКТ у досягненні цілей сталого розвитку на період до 2030 року. Зокрема, йдеться про ефективну співпрацю між зацікавленими сторонами у кіберпросторі та підвищення рівня готовності у сфері кібербезпеки на 40% до 2020 року [62].

Крім того, у вересні 2015 року держави-члени ООН погодили 17 цілей сталого розвитку на період до 2030 року. Серед зазначених цілей – суттєве підвищення доступу до ІКТ та в ідеалі забезпечення універсального та фінансово необтяжуючого доступу до Інтернету у найменш розвинених країнах до 2020 року (9c) [63].

Таким чином, розглянувши в історичній ретроспективі міру відображення питань розвитку глобального інформаційного суспільства у міжнародному праві, можна стверджувати про позитивні еволюційні зрушення. При цьому, на кожному з історичних етапів актуальними залишаються питання збалансованого розвитку, рівних можливостей, інклюзивності та поваги прав людини. Відрізняється лише термінологічний інструментарій відповідних нормативних документів. Особливе місце традиційно відводиться захисту прав людини, адже глобальне інформаційне суспільство за своєю природою є людиноцентричною системою. З метою забезпечення належних гарантій прав людини в інформаційному суспільстві повинні бути створені ефективні міжнародно-правові механізми їх захисту, про що більш детально йтиметься у підрозділі 3.1.

На наше глибоке переконання, період заперечення взаємопроникнення міжнародного права та глобального інформаційного суспільства залишився далеко позаду. Наразі не стоїть питання про визнання факту перетворюючого впливу технологічного прогресу на регуляторні механізми, оскільки хочемо ми того чи ні, такий

вплив об'єктивно має місце. Натомість, йдеться про використання потенціалу глобального інформаційного суспільства для сприяння прогресивному розвитку міжнародного права. Слід особливо відмітити, що усі окреслені вище етапи пов'язані з нормотворчими ініціативами, прийнятими в рамках ООН. Остання, будучи класичною міжнародною організацією, демонструє успішні приклади практичної реалізації моделі багатосторонньої участі та посиленої співпраці. Крім того, запропонована автором періодизація свідчить про зростання адаптивності міжнародного права до перманентно еволюціонуючих суспільних відносин в інформаційній сфері.

За фасадом будь-яких нормативних зрушень завжди знаходиться відповідний інституційний механізм, від ефективності та розвиненості якого залежить успішність та своєчасність міжнародно-правового регулювання. Так, ми вже згадували про роль ООН в еволюційних процесах міжнародного права в інформаційну еру, далі ж розглянемо її більш предметно, а також звернемося до альтернативних інституційних механізмів глобального інформаційного суспільства.

1.3. Інституційний механізм глобального інформаційного суспільства

Високий ступінь взаємозалежності усіх суб'єктів міжнародних відносин та видозміни самої міжнародної системи визначають динаміку розвитку інформаційного суспільства на локальному та універсальному рівнях. Відбувається поступовий перехід від державоцентричного до поліцентричного світу, де ключова роль належить глобальним структурам та утворенням. Наразі інформаційно-комунікаційні технології відіграють настільки вагому роль у всіх сферах життя людини та функціонування державних механізмів, що можна з впевненістю говорити про виникнення на глобальному рівні нової інформаційної парадигми. Так, М. Ребой зазначає, що Всесвітній саміт інформаційного суспільства сформував нову парадигму у глобальному управлінні, де інформація та комунікація відіграють ключову роль та спостерігається зростаюче залучення до процесів управління громадянського суспільства [64, с. 131].

Публічний вимір набуває рис транснаціональності, а суб'єкти, що взаємодіють у його межах, все частіше починають говорити про необхідність вироблення інституційних

механізмів та надання нормативних гарантій, які б дозволили їм брати повноправну участь не лише у напрацюванні норм та стратегій розвитку, але й входити до конкретних структур, відповідальних за глобальне управління [65, с. 83]. Чим більше питання розвитку інформаційного суспільства набувають глобального окрасу та чим швидше зростає роль транснаціональних суб'єктів у цих процесах, тим сильніше відчувається потреба у створенні такого масиву міжнародно-правового регулювання, що б заклав нормативну основу універсального механізму управління Інтернетом із залученням усіх зацікавлених сторін (держав, міжнародних організацій, приватного сектору, громадянського суспільства, технічної та академічної спільнот). Наразі інформація та комунікація розглядаються не просто як засоби досягнення політичних, економічних, соціальних цілей, але як самостійні питання, важливість яких з часом лише зростає.

На різних рівнях ми можемо спостерігати співіснування традиційних інституційних форм організації суспільства та нових інформаційно-комунікаційних технологій. Сучасні ІКТ перенесли взаємодію суб'єктів міжнародних відносин виключно з фізичного світу до кіберсередовища, де відсутні традиційні уявлення про простір та час. Ключовими цінностями глобального інформаційного суспільства визнаються відкритість, різноманітність, справедливість, рівність та інклюзивність.

Теоретично можна виділити дві протилежні моделі розвитку інформаційного суспільства. Одна з них захищає інтереси держав та комерційних структур і розглядає інформаційне суспільство як новий світовий порядок, що ґрунтується на єдиному технологічно-орієнтованому підході, відповідно до якого інформація та знання визнаються товарами, що можуть бути предметом купівлі-продажу на споживчому ринку. Інша модель має в основі ідею формування інформаційних суспільств на основі принципів відкритості, інклюзивності, поваги до різноманіття та плюралізму. За цією моделлю комунікація визнається базовою потребою, а знання отримують статус загального блага. Традиційно прихильниками такого підходу виступають громадські об'єднання та правозахисні групи [25, с. 215].

Основу інституційного механізму глобального інформаційного суспільства повинен становити багатосторонній діалог усіх зацікавлених суб'єктів, що передбачає участь кожного, від кого залежить прийняття рішень та на кого такі рішення мають чи потенційно

можуть мати вплив. В умовах розбудови суспільства нового типу право голосу при прийнятті суспільно важливих рішень повинно перестати бути виключно правом держав та міжурядових організацій. Громадянське суспільство, приватний сектор та технічні спільноти (напр., IETF – Цільова інженерна група Інтернету) повинні отримати реальну можливість впливати на рішення, що безпосередньо зачіпають їх інтереси та встановлюють принципи правовідносин між ними в кіберпросторі.

Наразі у багатьох міжнародно-правових документах, спрямованих на регулювання інформаційних правовідносин, держави поряд з громадянським суспільством, приватним сектором та міжнародними організаціями згадуються у їх відповідних ролях – «*in their respective roles*», тобто як суб'єкти, що, в першу чергу, покликані враховувати інтереси кожного індивіда. Цифровий світ за свою правовою природою є багатоголосим. Формування ефективних правових механізмів в умовах глобального інформаційного суспільства можливе лише при забезпеченні повноправної участі у нормотворчому процесі Інтернет-користувачів, провайдерів, бізнес-структур та самих держав як первинних суб'єктів міжнародного права.

Інституційний підхід до вивчення міжнародних відносин традиційно демонструється на прикладі взаємовідносин органів та інституцій, що входять до системи ООН, із недержавними утвореннями, як правило, неурядовими організаціями [66]. У 1998 році була оприлюднена доповідь Генерального секретаря ООН, у якій йшлося про те, що неурядові організації більше не розглядаються виключно як відповідальні за поширення інформації. Вони виступають своєрідними посередниками між суспільством та урядами [67]. У 2001 році Генеральна Асамблея ООН підтвердила необхідність активного залучення міжурядових та неурядових організацій, громадянського суспільства та приватного сектору до міжурядового підготовчого процесу Всесвітнього саміту інформаційного суспільства та участі у самому Саміті [46].

Як зазначає В. Кляйнвехтер, з наукової точки зору політика управління Інтернетом є багаторівневою за своєю структурою. Так, на найнижчому рівні управління здійснюється в односторонньому порядку, на середньому рівні – шляхом міждержавних переговорів та на найвищому рівні – на основі багатосторонньої участі зацікавлених сторін. При цьому, при застосуванні останньої моделі дві попередні вступають з нею в органічний взаємозв'язок.

Автор проводить аналогію з традиційною російською іграшкою – матрьошкою, де відбувається поступовий перехід від механізму багатосторонньої участі до міждержавної договірної системи та далі до національних юрисдикцій, що у своїй сукупності утворюють екосистему управління Інтернетом [68].

При виробленні ефективної інституційної моделі вибір не повинен поставати між безпечним та відкритим Інтернетом. Ці дві складові повинні бути взаємодоповнюючими, і в жодному разі не взаємовиключаючими. Тяжіння до будь-якої одної з означених характеристик Інтернету буде проявом або надмірного контролю та цензури з боку держави, або нехтування елементарними нормами приватності та поваги до гідності особи. При цьому, слід розуміти, що контроль та моніторинг не завжди є гарантією безпеки, а відкритість не означає вседозволеність та безконтрольність.

Нижче розглянемо спроби інституціоналізації глобального інформаційного суспільства та проведемо оцінку їх ефективності. Для зручності аналізу автором пропонується виділяти два типи інституційних моделей, в рамках яких відбувається формування політики та стандартів управління глобальним інформаційним суспільством. Перша модель ґрунтується на традиційному міждержавному механізмі, прикладом якого може бути співпраця в рамках ООН. В основі іншої моделі – принцип багатосторонньої участі, що передбачає залучення різноманітних недержавних суб'єктів. На даному принципі побудована діяльність, зокрема, ICANN та Форуму з управління Інтернетом (IGF). В основу концепції багатосторонньої участі покладена ідея про те, що кожен зацікавлений суб'єкт повинен мати право голосу при вирішенні питань, пов'язаних з розвитком інформаційного суспільства. З цією метою повинні бути передбачені відповідні процедури та створені необхідні інституційні механізми [69].

Той факт, що концепція багатосторонньої участі передбачає розширене представництво зацікавлених сторін у процесах управління Інтернетом, ще, однак, не означає, що відбулися сутнісні зміни в контексті розглядуваних питань та проблематики [70]. Фактично, спостерігається надлишкове представництво суб'єктів з боку західних високорозвинених країн у всіх категоріях учасників. У той же час країнам, що розвиваються бракує незалежних організацій громадянського суспільства та впливових приватних бізнес-структур, що могли б виступити з власними ініціативами на глобальних

форумах з питань інформаційного суспільства.

Традиційно розпочнемо інституційний аналіз із міждержавних механізмів, де інші суб'єкти подекуди можуть мати статус спостерігача, однак із вкрай обмеженими повноваженнями. Так, *Міжнародний союз електрозв'язку* (надалі – «МСЕ») є спеціалізованою установою ООН, що відповідає за розробку стандартів у сфері телекомунікацій. МСЕ здійснює свою діяльність за трьома основними напрямками – радіокомунікації, стандартизація та розвиток. Роль МСЕ у питаннях управління Інтернетом є спірною. Недостатня транспарентність та міжурядовий характер діяльності МСЕ не дозволяють говорити про розширення його мандату. Втім, наприклад, Росія послідовно відстоює ідею визнання лідируючої ролі МСЕ у сфері управління Інтернетом з огляду на те, що саме ця організація має достатні представницькі функції та засвідчила свою ефективність у регулюванні міждержавних відносин.

МСЕ долучається до обговорення питань, пов'язаних з кіберпростором, через надання платформи для проведення Повноважної конференції, Всесвітньої конференції з міжнародних телекомунікацій, Всесвітнього форуму з політики у сфері електрозв'язку та Всесвітньої конференції з розвитку електрозв'язку.

У грудні 2012 року МСЕ провів Всесвітню конференцію з міжнародних телекомунікацій у Дубаї, у ході якої планувалося переглянути Регламент міжнародного електрозв'язку у редакції 1988 року. Регламент – міжнародна угода, що закріплює принципи обміну телекомунікаційним трафіком. Найбільш дискусійним виявилося питання про доцільність поширення дії Регламенту на сферу управління Інтернетом та передачі Інтернет трафіку. Ідею зробити Інтернет підконтрольним МСЕ активно підтримували Росія, Китай, Саудівська Аравія, Алжир та Судан. США послідовно виступали проти розширення функцій МСЕ та за збереження відкритого Інтернету.

Компромісним рішенням стало включення до фінального тексту Регламенту юридично необов'язкової Резолюції № 3 «Забезпечення сприятливого середовища для більш активного розвитку Інтернету». Відповідно до Резолюції, усі держави повинні мати однакові повноваження та зобов'язання у сфері управління Інтернетом. Крім того, державам-членам пропонується виробити власну позицію щодо питань міжнародного характеру, пов'язаних з Інтернетом, зокрема технічних аспектів, напрямків розвитку та

державної політики в рамках мандату МСЕ та його форумів [71]. Ще одним контроверсійним моментом стало включення до Регламенту статті 5В, якою державам надається право вживати необхідні заходи для попередження поширення спаму та мінімізації його негативного впливу на послуги міжнародного електрозв'язку. Критики даної статті вказували на те, що вона може стати першим кроком на шляху встановлення державного контролю над контентом. І, хоча, у Регламенті прямо не йдеться про регулювання Інтернету, однак спам традиційно є характерним саме для кіберпростору.

Зазвичай рішення в рамках МСЕ приймаються консенсусом, чого не сталося цього разу. Держави пішли шляхом процедури формального голосування. Переглянутий Регламент підписали 89 із 144 держав, серед яких і Україна. Дана конференція стала яскравим прикладом протистояння між державоцентристським та багатостороннім підходами до регулювання Інтернету. Чимало держав, втім, не мали власної жорсткої позиції щодо даного питання та керувалися виключно економічними чи політичними мотивами при прийнятті рішення щодо підписання фінального тексту. Негативним моментом є те, що наразі сформувалося дві групи держав, одні з яких дотримуються положень Регламенту у редакції 2012 року, а інші користуються версією 1988 року. За результатами конференції почали говорити про початок холодної війни у кіберпросторі.

Наприкінці 2014 року у м. Пусан (Республіка Корея) відбулася 19-та Повноважна конференція МСЕ, що проходить кожні чотири роки. На конференції майже одноголосно новим Генеральним секретарем МСЕ було обрано Хулінь Чжао, що дозволило говорити про поступове утвердження ролі Китаю в глобальних процесах управління Інтернетом. З огляду на обмежувальну політику Китаю у кіберпросторі висловлювалися побоювання з приводу того, що в майбутньому МСЕ може поширити свої повноваження на Інтернет, а держави отримають право поширювати свій суверенітет на онлайнове середовище.

Однак, сама конференція пройшла доволі спокійно, було внесено лише незначні зміни до її чотирьох ключових резолюцій з питань Інтернету, зокрема Резолюції 101 «Мережі, засновані на проколі Інтернет» та Резолюції 102 «Роль МСЕ щодо міжнародної державної політики з питань, що стосуються Інтернету та управління ресурсами Інтернету, включаючи найменування доменів та адреси». Одним із найбільш обговорюваних питань стала кібербезпека та доцільність розширення мандату МСЕ у цій сфері. Переглянутий

текст Резолюції 130 «Посилення ролі МСЕ у зміцненні довіри та безпеки при використанні інформаційно-комунікаційних технологій» зазнав незначних змін. У преамбулі тепер міститься посилання на Резолюцію ГА ООН «Право на приватність у цифрову еру». Суперечливими виявилися статті про мережеву безпеку та спам. Вцілому, на МСЕ покладається завдання покращення координації між державами-членами та подальше вивчення питання кібербезпеки. Зрештою положення про необхідність прийняття універсальної угоди з кібербезпеки не увійшли також до тексту Резолюції 174 «Роль МСЕ у зв'язку з питаннями міжнародної державної політики щодо ризику незаконного використання ІКТ» [72].

Розширення мандату МСЕ можливе за рахунок розширювального тлумачення базових понять, які містяться в документах організації. Одним з таких термінів є «інформаційно-комунікаційні технології». На самій конференції не вдалося виробити загальноприйнятне визначення даного терміну, а тому було вирішено повернутися до цього питання на наступній конференції у 2018 році. Крім того, у якості експерименту було вирішено надати академічній спільноті статус постійного члена [73].

Обговорення в рамках Повноважної конференції проходили значно спокійніше, ніж у 2012 році. Держави доволі безболісно поступалися своїми вимогами там, де не знаходили підтримки й альтернативні пропозиції їх ідеологічних опонентів у контексті кіберпростору.

Іншим елементом міждержавного інституційного механізму глобального інформаційного суспільства є *ЮНЕСКО*, яка відповідно до Женевського Плану дій 2003 року визначена відповідальною за доступ до інформації та знань, е-навчання, е-науку, культурне різноманіття та ідентичність, лінгвістичне розмаїття і місцевий контент, медіа та етичний вимір інформаційного суспільства [74].

У рамках ЮНЕСКО була розроблена концепція «Універсальності Інтернету», що відображає позицію організації в межах її мандату щодо питань, пов'язаних з Інтернетом, на період до 2021 року. Вона також засвідчує роль Інтернету у розбудові суспільств знань та досягнення цілей сталого розвитку ООН. В основу даної концепції покладено чотири ключові принципи, що наразі відомі як принципи R.O.A.M. – орієнтованість на права людини, відкритість, доступність та багатостороння участь [75].

ЮНЕСКО щорічно проводить багатосторонній Форум ВСІС у партнерстві з МСЕ,

Програмою розвитку ООН та ЮНКТАД.

Комісія ООН з науки і техніки у цілях розвитку є допоміжним органом у структурі ЕКОСОР. З 2006 року вона проводить щорічну оцінку результатів імплементації здобутків ВСІС на міжнародному і регіональному рівнях та визначає рівень їх відповідності цілям ВСІС. Комісія є міжурядовим органом, а її рішення не мають обов'язкової сили. Складається з 43 членів, що обираються ЕКОСОР строком на чотири роки [76].

У березні 2013 року в рамках Комісії було створено першу *Робочу групу щодо посиленої співпраці*, на яку покладалося завдання дослідити мандат ВСІС у контексті посиленої співпраці як вона згадується у Туніській програмі для інформаційного суспільства. Робоча група була сформована за принципом участі зацікавлених сторін та складалася з 22 представників держав-членів та 5 представників від кожної групи стейкхолдерів, зокрема приватного сектору, громадянського суспільства, технічної та академічної спільнот, міжурядових та міжнародних організацій [77]. Комісії не вдалося досягнути жодних конкретних результатів.

Відповідно до Фінального документу ВСІС+10 на Комісію покладається завдання провести аналіз поняття «посилена співпраця», що вперше було використане у 2005 році для позначення компромісу між тими, хто наполягав на державному механізмі управління Інтернетом, та прихильниками статус-кво. Втім, яке саме значення вкладалося в дане поняття досі залишається невизначеним. З цією метою не пізніше липня 2016 року повинна бути створена нова робоча група щодо визначення способів реалізації посиленої співпраці. Оскільки, у Фінальному документі ВСІС+10 вперше згадується про необхідність об'єднання в механізмі управління Інтернетом міждержавного та багатостороннього підходів, результати роботи нової робочої групи можуть стати одним з ключових показників ефективності процесів ВСІС при підведенні підсумків у 2025 році.

Починаючи з 2004 року у структурі Першого комітету ГА ООН чотири рази створювалися *групи урядових експертів щодо досягнень у сфері інформації та комунікацій в контексті міжнародної безпеки*. Влітку 2015 року четверта Група урядових експертів опублікувала доповідь, в якій вперше було запропоновано конкретні рекомендаційні норми відповідальної поведінки держав у кіберпросторі [78]. Згідно з доповіддю у кіберпросторі держави повинні дотримуватися міжнародного права та, зокрема Статуту ООН і основних

принципів МП. Фактично, це означає, що держави, як і індивіди, володіють однаковими правами офлайн та онлайн. Незрозумілим залишається те, як саме положення Статуту ООН будуть застосовуватися у випадку використання чи погрози використання сили у кіберпросторі, здійснення акту агресії чи збройного нападу. У доповіді окремо виділяються такі міжнародно-правові принципи, як гуманність, необхідність, пропорційність та розрізнення. Державний суверенітет поширюється на ІКТ інфраструктуру в межах державної території. Державам забороняється здійснювати кібератаки на критичну інфраструктуру. Однак, сама класифікація об'єктів критичної інформаційної інфраструктури значно різниться залежно від країни. Держави повинні зміцнювати транскордонну співпрацю щодо допомоги у попередженні та розслідуванні кіберінцидентів. ООН повинна відігравати керівну роль у налагодженні діалогу щодо безпечного використання ІКТ з боку держав, а також сприяти виробленню спільного бачення щодо застосування міжнародного права до відповідальної поведінки держав. У самій доповіді робиться застереження про те, що імплементація її положень потребує часу, особливо для країн, що розвиваються, оскільки останні не володіють достатнім потенціалом.

Генеральна Асамблея схвалила доповідь та постановила про необхідність створення нової групи урядових експертів, що повинна провести своє перше засідання у серпні 2016 року в Нью-Йорку [79].

Всесвітня організація інтелектуальної власності (надалі – «ВОІВ»), у свою чергу, слідкує за дотриманням так званих Інтернет-договорів 1996 року – Договору про авторське право та Договору про виконання та фонограми. Так, обидва договори передбачають обов'язок держав-членів надавати належний рівень правової охорони та ефективні засоби правового захисту, які б унеможливлювали обхід технологічних обмежень, використаних для захисту об'єкту інтелектуальної власності. ВОІВ робила невдалі спроби зафіксувати на нормативному рівні положення щодо веб-мовлення та трансляції в Інтернеті, а також розширення прав телерадіокомпаній у кіберпросторі.

У 1999 році ICANN затвердив Єдину політику вирішення спорів щодо доменних імен, що початково була запропонована ВОІВ у вигляді режиму вирішення спорів щодо торговельних марок. Більшість таких спорів вирішується через Центр арбітражу та медіації ВОІВ. Свою роль організація відіграла й у створенні відкритої бази даних «WHOIS», що

викликає справедливе занепокоєння у контексті захисту приватності у кіберпросторі [80].

У 2003-2005 роках ВОІВ брала участь у ВСІС, втім її роль зводилася фактично до нагляду за тим, щоб питання інтелектуальної власності не стали предметом серйозних обговорень. У 2005 році ВОІВ увійшла до Робочої групи ООН з питань управління Інтернетом, однак її позиція з питань інтелектуальної власності не була включена до фінальної доповіді через її спірний характер.

У 2004 році неурядові організації, наукова спільнота та громадянське суспільство запропонували текст Женевської Декларації про майбутнє ВОІВ, що передбачала реформування організації з метою скасування її обмежувальних практик, розширення доступу до знань та врахування інтересів країн, що розвиваються [81]. Хоча Декларація не мала юридично обов'язкової сили, вона продемонструвала необхідність модернізації підходів до захисту прав інтелектуальної власності у кіберпросторі. У цьому ж році з ініціативи Індії та Бразилії розпочалося обговорення Плану дій ВОІВ у сфері розвитку. Формально План дій було затверджено рішенням ГА ВОІВ у 2007 році, яким також передбачалася імплементація 45 рекомендацій, згрупованих у шість кластерів, а також створення Комітету з питань розвитку та інтелектуальної власності [82]. Швидкий розвиток ІКТ вимагає лібералізації регулювання ВОІВ з метою встановлення розумного балансу між відкритим доступом до знань, інформації та захистом інтересів правоволодільців. Достатньо пасивна участь ВОІВ у розробці питань розвитку глобального інформаційного суспільства пояснюється застарілістю підходів організації до охорони об'єктів авторського автора, які виявляються несумісними із транскордонною природою кіберпростору. Це є ще одним свідченням на користь неможливості накладення трафарету з чинних міжнародно-правових норм та принципів на правовідносини, що виникають у кіберпросторі або у зв'язку з ним.

«Партнерство «Відкритий уряд» (*Open Government Partnership*) є багатосторонньою ініціативою, що була заснована у 2011 році та спрямована на забезпечення виконання зобов'язань урядів щодо підвищення транспарентності, розширення участі громадян у прийнятті рішень, боротьбу з корупцією, а також використання нових технологій для покращення управління. Щоб приєднатися до ініціативи, держава повинна підписати Декларацію відкритого уряду, представити план дій, розроблений у ході публічних

консультацій, а в подальшому звітувати про досягнуті результати. Станом на березень 2016 року до ініціативи приєдналися 69 держав. В Україні перший план дій з впровадження ініціативи було затверджено у 2012 році [83].

Коаліція за свободу онлайн (*Freedom Online Coalition*) – міжурядова організація що була створена в Гаазі у грудні 2011 року з ініціативи Міністерства закордонних справ Королівства Нідерландів та має своєю метою посилення співпраці держав щодо підтримання свободи в Інтернеті та сприяння індивідам у здійсненні ними своїх прав онлайн, зокрема свободи вираження поглядів, свободи об'єднання та права на приватність. Коаліція визнає принцип багатосторонньої участі та щорічно проводить конференції за участі зацікавлених сторін. Усі держави-члени підписали установчий документ «Свобода онлайн: спільні дії заради свободи вираження поглядів в Інтернеті», а також визнають принцип рівного захисту прав людини офлайн та онлайн. Станом на березень 2016 року до складу коаліції входить 29 держав [84]. Україна наразі не приєдналася.

Глобальна конференція з кіберпростору, що більше відома як Лондонський процес, була започаткована в Лондоні у листопаді 2011 року. Відтоді вона щорічно збирає разом представників урядів, приватного сектору, технічної спільноти та громадянського суспільства для вироблення спільного розуміння поведінки у кіберпросторі [85]. У ході другої конференції, що пройшла у Будапешті в жовтні 2012 року, обговорювалося питання взаємозв'язку між правами онлайн та кібербезпекою. Втретє конференція відбулася у жовтні 2013 року в Сеулі. Її результатом стало затвердження «Сеульського рамкового плану та зобов'язання щодо відкритого та безпечного кіберпростору», у якому закріплюються принципи універсального доступу до Інтернету, рівного захисту прав людини офлайн та онлайн [86]. Крім того, у документі міститься посилання на доповідь ООН щодо застосування міжнародного права до кіберпростору та його ключовій ролі для підтримання миру і стабільності, розвитку відкритого, безпечного, мирного та доступного онлайн середовища [87]. Під час четвертої конференції в Гаазі у квітні 2015 року обговорювалися питання практичної співпраці у кіберпросторі з метою розвитку кіберпотенціалу та вироблення норм відповідальної поведінки держав у кіберпросторі. Особливий акцент було зроблено на питаннях кібербезпеки. За результатами конференції було засновано Глобальний форум з кіберекспертизи [88].

Спроби інституціоналізації правовідносин у кіберпросторі мають місце і в азійському регіоні. Так, 16-18 грудня 2015 року в м. Учжен (Китай) відбулася друга *Всесвітня Інтернет-конференція*, що зібрала представників 120 країн світу. У своєму вступному слові під час церемонії відкриття конференції Президент КНР Сі Цзіньпін зазначив про необхідність трансформування глобальної системи управління Інтернетом, що повинна базуватися на принципах поваги до кіберсуверенітету, підтримання миру та безпеки, заохочення відкритості та співпраці, а також культивування стійкого порядку. Лідер Китаю наголосив на важливості уникнення кібергегемонії та подвійних стандартів у сфері кібербезпеки. Президент КНР порівняв безпеку та розвиток з двома крилами пташки або двома колесами возу, де безпека є передумовою розвитку, а розвиток є кінцевою метою безпеки. Сі Цзіньпін зробив наголос на прийнятті взаємоузгоджених правил поведінки у кіберпросторі та міжнародної конвенції щодо боротьби з тероризмом у кіберпросторі, а також на удосконаленні механізму правової допомоги щодо боротьби з кіберзлочинністю. Він також зазначив про важливість створення нових платформ для комунікації та співпраці, а також залучення усіх країн світу до користування перевагами інформаційної ери. У кіберпросторі повинен дотримуватися принцип верховенства права. Хоча сам кіберпростір є віртуальним, суб'єкти залишаються абсолютно реальними [89].

Фінальним документом другої конференції стала Учженська ініціатива, у якій зазначається, що Інтернет перетворив світ на глобальне село та спільноту зі спільною долею. Його швидкий розвиток створив нові виклики для державного суверенітету, безпеки та сталого розвитку. В Ініціативі містяться посилання на такі ключові документи, як Женевська Декларація принципів 2003 року, Туніська програма для інформаційного суспільства 2005 року, Заява Монтевідео про подальшу співпрацю у сфері Інтернету та доповіді Груп урядових експертів ООН щодо досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки. Схвалюються здобутки ВСІС +10.

Крім того, в Ініціативі наголошується на важливості дотримання державного суверенітету у кіберпросторі, захисту критичної інформаційної інфраструктури, забезпечення приватності та гарантування прав інтелектуальної власності, а також об'єднання зусиль з метою боротьби з кіберзлочинністю та кібертероризмом. Окремим пунктом виділено питання покращення глобального управління Інтернетом. Зазначається

про необхідність вироблення спільного підходу щодо міжнародних норм та правил, покликаних регулювати кіберпростір, захищати базові права та законні інтереси індивідів в Інтернеті, а також перетворити кіберпростір на мирне, безпечне, відкрите та універсальне середовище. Цікавим є той факт, що у тексті Ініціативи йдеться про формування багатосторонньої системи управління Інтернетом із залученням зацікавлених сторін відповідно до їх функцій [90].

Однак, критику науковців та експертів одразу викликала гра слів, яка зустрічається як у вітальному слові Президента Сі Цзіньпіна, так і у фінальній Учженській ініціативі. В українському перекладі дещо втрачається цей термінологічний шарм. Так, в обох випадках при згадуванні принципу багатосторонності вживається англійський термін «*multilateral*», а не звичний для ВСІС та IGF «*multistakeholder*». При цьому перелічуються суб'єкти, між якими повинні відбуватися відповідні консультації, зокрема уряди, міжнародні організації, Інтернет-компанії, технічні спільноти, неурядові інституції та окремі індивіди. Неоднозначність зроблених заяв пов'язана з централізацією та закритістю Інтернет-середовища в межах Китаю. Так само дискусійними виявилися призначення до складу Консультативної ради вищого рівня тодішнього Президента ICANN Ф. Шехада, члена координаційної ради Ініціативи *NETmundial*, президента компанії «Алібаба Груп» Джека Ма. На новостворену Раду покладалося завдання надання пропозицій щодо покращення проведення Інтернет-конференції та розвитку Інтернету в Китаї. Швидше за все, Китай прагне утвердити своє лідерство у глобальних процесах управління Інтернетом та створити альтернативу вже існуючим багатостороннім платформам, чим і зумовлені подібні кроки. Однак, навряд варто очікувати демократизації кіберрегулювання в КНР, що послідовно відстоює ідею кіберсуверенітету держав.

Слід згадати, що результатом першої Інтернет-конференції 2014 року стала Декларація Учжень, яку за офіційною версією не було прийнято через те, що учасники надто пізно отримали її текст для ознайомлення та коментування. Декларація містила дев'ять ключових принципів, що повинні були лягти в основу формування багатосторонньої (*multilateral*), демократичної та транспарентної

міжнародної системи управління Інтернетом. Кіберпростір визнавався середовищем, що повинен належати кожному та управлятися всіма на рівних умовах [91]. Аналогічні за змістом положення увійшли до Учженської Ініціативи 2015 року.

Крім того, у ході першої Інтернет-конференції 38 осіб підписали Заяву Учжень, яка містить чотири загальновизнані принципи, що повинні закласти базис для розвитку Інтернету в Китаї. Зокрема, йдеться про розвиток Інтернету як єдиного та нефрагментованого простору, підтримання безпеки, стабільності та стійкості Інтернету шляхом співпраці між різними зацікавленими сторонами [92].

Таким чином, сама ідея поширення суверенітету держав на кіберпростір суперечить принципу багатосторонньої участі суб'єктів в управлінні Інтернетом. Адже, в такому випадку серед нібито рівних суб'єктів, привілейованими залишаються знову ж таки держави, які володіють значно ширшими повноваженнями в межах своїх суверенних прав. Втім, Китай не єдиний у такому підході. Так, Генеральний секретар МСЕ Чжао Хулінь провів розмежування між системою управління Інтернетом, до якої повинні бути залучені всі зацікавлені сторони, та кібербезпекою, де державам слід відвести керівну роль. Така позиція є цілком зрозумілою, якщо зважати на те, що МСЕ є міждержавною інституцією. Крім того, у Фінальному документі ВСІС+10 чітко прописано, що керівна роль у сфері кібербезпеки повинна належати державам [93].

Китай наголошує на створенні такої моделі регулювання Інтернету, яка б враховувала суверенні права держав у цій сфері та дозволила б уникнути ризиків інформаційній безпеці держав. Адже безпека у кіберпросторі повинна бути абсолютною, інакше завжди існуватиме загроза кібернападу. Правда у тому, що просуваючи доволі непопулярну ідею кіберсуверенітету, Китай не втрачає своєї привабливості серед представників найбільших західних компаній. Так, *LinkedIn* погодився здійснювати цензуру контенту в обмін на доступ до китайського ринку. Той же *Facebook* не виключає можливості компромісу з китайською владою [94]. І це при тому, що у 2014 році міжнародна неурядова організація «*Amnesty International*» назвала китайську модель Інтернету найбільш контрольованою [95], а у 2015 «*Freedom House*» визнала Китай державою, що проводить найбільш

обмежувальну Інтернет політику серед 65 досліджених країн [96]. Наразі усі великі держави намагаються контролювати Інтернет. Різниця у тому, що хтось робить це під більш привабливими лозунгами.

Далі перейдемо до аналізу інституційних механізмів, в основу яких покладена класична багатостороння модель управління глобальним інформаційним суспільством. Так, *Інтернет-корпорація з присвоєння імен та номерів* (ICANN) є приватною, неприбутковою глобальною корпорацією, що управляє системою доменних імен та IP-адрес. Корпорація була створена у 1998 році в Лос-Анджелесі відповідно до законодавства штату Каліфорнія на основі Меморандуму взаєморозуміння між ICANN та Департаментом торгівлі США. Система прийняття рішень в ICANN побудована на основі класичної багатосторонньої моделі. Хоча ICANN займається виключно технічними питаннями, держави з метою посилення своєї ролі в процесах управління Інтернетом неодноразово заявляли про те, що діяльність корпорації впливає на такі важливі сфери національного регулювання як інтелектуальна власність, приватність, кібербезпека та правозастосування.

14 березня 2014 року Національне управління США з телекомунікацій та інформації (надалі – «NTIA») оголосило про передачу координуючої ролі у здійсненні функцій Агентства з розподілу номерів Інтернету (надалі – «IANA») міжнародній спільноті зацікавлених сторін. Ключовою умовою була абсолютна відмова від передачі координуючої ролі державам чи міжурядовій організації. Така передача повинна також базуватися на чотирьох основних принципах: багатостороння модель, безпека, стабільність та стійкість системи доменних імен Інтернету; відповідність потребам та очікуванням партнерів та користувачів послуг IANA у всьому світі; відкритість Інтернету. Обговорення нової моделі управління відбувається в контексті двох ключових напрямків – передачі координуючих функцій IANA та посилення підзвітності ICANN.

У серпні 2015 року NTIA заявило про продовження строку дії контракту з ICANN та перенесення кінцевої дати з 30 вересня 2015 року на 30 вересня 2016 року [97]. Усі події, що відбуваються у сфері управління Інтернетом, є надзвичайно взаємопов’язаними. Рішення, прийняті в рамках одних форумів, неминуче матимуть

вплив на договірний процес в рамках інших інституційних механізмів.

Іншим показовим прикладом є те, як світова спільнота підійшла до створення в рамках ООН нового майданчику для багатостороннього діалогу з питань формування політики у сфері Інтернету. *Форум з управління Інтернетом* (надалі – «IGF») створювався як відкрита платформа для участі усіх зацікавлених сторін, що повинні були спільно визначати формат його діяльності та 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 сектору, 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 учасниками [98].

Форуму вдалося заповнити той інституційний вакуум, що існував у сфері управління Інтернетом. Вперше вдалося створити рівні умови для участі в обговоренні актуальних питань усіх зацікавлених сторін, особливо представників громадянського суспільства, які отримали реальну можливість впливати на формування політики в Інтернет-сфері. Втім, IGF 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 необов'язкових рішень. Наразі Форум швидше нагадує платформу для обміну думками та ведення дискусій. Розвинені країни продовжують надавати перевагу випробуваним 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.

Європейським аналогом Форуму з управління Інтернетом став заснований у 2008 році щорічний *Європейський діалог з управління Інтернетом – EuroDIG.* Заключні рішення EuroDIG передаються для обговорення на IGF.

Важливим етапом еволюції інституційної системи глобального інформаційного суспільства стало проведення *Глобальної багатосторонньої*

зустрічі щодо майбутнього управління Інтернетом, що відбулася 23-24 квітня 2014 року в бразильському Сан-Паулу. Конференція зібрала 1480 учасників з 97 країн світу та стала вагомою подією в контексті формування альтернативної ООН екосистеми управління Інтернетом. Підсумковим документом стала Багатостороння декларація NETmundial, перша частина якої присвячена принципам управління Інтернетом, а друга – містить перелік заходів, які слід вжити задля того, щоб забезпечити участь усіх зацікавлених сторін відповідно до їх функцій та обов'язків.

Наприкінці червня 2015 року у тому ж Сан-Паулу відбулося установче засідання Координаційної ради *Ініціативи NETmundial*, на якому було визначено сферу повноважень останньої. Так, Ініціатива повинна стати платформою для співпраці усіх зацікавлених сторін з метою приведення в дію спільних рішень, що приймаються за принципом «знизу-догори» в рамках екосистеми розподіленого управління Інтернетом. Зокрема, було окреслено шість ключових функцій Ініціативи: сприяти імплементації Принципів *NETmundial*, бути незалежною інституційною структурою по збору та розповсюдженню інформації, слугувати платформою для співпраці, надавати допомогу експертним групам, сприяти залученості до процесу управління Інтернетом та вживати необхідні заходи для розвитку потенціалу.

Крім того, було розглянуто та схвалено два перші напрямки діяльності Ініціативи *NETmundial*. Зокрема, вдалося досягти згоди щодо пробних версій Карти рішень *NETmundial*, призначеної для полегшення співпраці щодо обміну інформацією з питань управління Інтернетом, та Платформи для співробітництва *NETmundial*, що покликана акумулювати пропозиції щодо активізації спільних зусиль у сфері управління Інтернетом. Координаційна рада зобов'язалася співпрацювати з усіма зацікавленими сторонами (урядами, приватним сектором, громадянським суспільством, технічною та академічною спільнотами) з метою імплементації концепції ВСІС щодо розбудови людиноцентричного, інклюзивного та орієнтованого на розвиток інформаційного суспільства на період після 2015 року.

Таким чином, управління Інтернетом повинно здійснюватися на основі відкритих стандартів з урахуванням індивідуальних та колективних знань і досвіду,

а також рішень, що приймаються на основі консенсусу та забезпечують функціонування унікальної, інтероперабельної, відказостійкої, стабільної, децентралізованої, безпечної та взаємопов'язаної мережі, доступної кожному [99].

Планується також запуск проекту щодо обміну кращими практиками по створенню локальних структур управління Інтернетом за принципом багатосторонньої участі. Оцінка ефективності діяльності Ініціативи *NETmundial* буде проведена наприкінці червня 2016 року. Впродовж цього першого року фінансова підтримка буде надходити від бразильського Керівного комітету з питань Інтернету, ICANN та Всесвітнього економічного форуму.

В минулому член Ради директорів ICANN Себастьян Башолє порівнює *NETmundial* з чемпіонатом світу з футболу, акцентуючи увагу на тій лише відмінності, що в умовах першого виграє кожен учасник, а останній передбачає перемогу лише найсильнішого гравця [100].

В основу розвитку Інтернету закладено принципи якості, безпеки, розвитку та мережевої нейтральності. У глобальному інформаційному суспільстві усі суб'єкти отримують право участі у процесах управління Інтернетом [60], втім модель їх взаємодії залишається невизначеною та незбалансованою. Постає питання про створення глобальних, а не міжнародних організацій. Кожен суб'єкт глобального інформаційного суспільства повинен бути відповідальним перед кінцевими Інтернет-користувачами, без яких існування самого Інтернету було б неможливим. Це свідчить про людиноцентричний характер мережевого суспільства, у якому державам відводиться другорядна роль.

У міжнародному праві чітко прослідковується еволюція від природних прав людини до прав громадянина та зрештою прав Інтернет-користувачів. Втім, у глобальній мережі користувач опиняється один на один з іншими суб'єктами. У контексті прав людини акцент традиційно робиться на забезпеченні доступу до Інтернету. При цьому кінцеві користувачі недостатньо добре обізнані з переговорними процесами та механізмами управління Інтернетом, що позбавляє їх можливості бути повноправними учасниками обговорень щодо питань структурної організації та правового регулювання глобального інформаційного суспільства.

Крім того, люди не приймають участі у тих процесах, які, як вони думають, їх не стосуються. Універсальність Інтернету не залишає сумнівів з приводу того, що управління цією глобальною мережею зачіпає права та інтереси кожного її користувача. При цьому слід враховувати, що глобальне інформаційне суспільство аж ніяк не являє собою однорідну ліберально налаштовану спільноту людей.

У зв'язку з цим виникає потреба розробки ефективної моделі глобального управління мережевим суспільством за принципом багатосторонньої участі. Управління глобальним інформаційним суспільством повинне здійснюватися за принципами відкритого членства та рівних можливостей для кожного індивіда незалежно від його громадянської приналежності. Наразі не існує жодної організації, яка б виступала у якості повноправного представника інтересів Інтернет-користувачів. Фактично, розвиток глобального інформаційного суспільства впродовж тривалого часу відбувався в умовах міжнародно-правового вакууму. Згодом виникло чимало колізій, пов'язаних зі спробами держав застосувати до Інтернету різні національні юрисдикції та обмежити його регулювання державними кордонами. Ще й досі ми стаємо свідками випадків, коли держави на законодавчому рівні закріплюють відповідальність провайдерів за передачу контенту, перехоплюють повідомлення приватних компаній, відбувається масове розповсюдження спаму та блокування поштових розсилок, мають місце зловживання, пов'язані з розподілом критичних IP-адрес та доменних імен, а поширення політичного контенту обмежується кордонами держави. Проблеми виникають також у зв'язку із захистом приватного життя онлайн та охороною об'єктів інтелектуальної власності в Інтернеті. Нові загрози з'являються настільки швидко, що держави не просто не встигають регулювати їх на нормативному рівні, але навіть своєчасно ідентифікувати їх появу. З огляду на це чимало вчених та практиків визнають потребу створення глобальної моделі управління інформаційним суспільством.

Інтернет став технологічною інновацією, що наразі потребує інноваційного підходу до інституційної та регуляторної сфер. Надмірна політизація питання управління Інтернетом та нормативних основ розвитку кіберпростору знижують

ефективність інституційних платформ, що наразі діють у цій сфері. У зв'язку з цим невирішеними залишаються питання кібершпигунства, ідентифікації суб'єктів у кіберпросторі, мережевої нейтральності, юрисдикції в Інтернеті тощо. Крім того, множинність інституційних механізмів може зрештою призвести до небажаної фрагментації екосистеми Інтернету. Останнім часом намітилася стійка тенденція до регіоналізації обговорень з питань управління Інтернетом, розвитку кіберпростору та розбудови інформаційного суспільства. Така тенденція є доволі небезпечною, оскільки може зумовити відповідні зміни на найнижчому інфраструктурному рівні та призвести до сегментації Інтернету на основі державних кордонів. Отже, проведений аналіз дає підстави стверджувати, що інституційний механізм глобального інформаційного суспільства повинен бути настільки ж універсальним, транснаціональним та відкритим до змін, як і саме суспільство, розвиток якого й повинен стати об'єктом відповідного міжнародно-правового регулювання.

ВИСНОВКИ ДО РОЗДІЛУ 1

Концепція інформаційного суспільства вперше виникла у 1960-х роках у рамках суспільних наук та лише в останні десятиліття поступово почала знаходити своє відображення у науці міжнародного права. Поняття «інформаційного суспільства» є доволі загальновживаним як у міжнародно-правовій доктрині, так і у відповідних міжнародно-правових документах. Однак, навіть при поверхневому аналізі стає зрозумілою відсутність консенсусу щодо визначення самого терміну та його концептуального наповнення. У теоретичних дослідженнях пропонувалися різні терміни для позначення досліджуваного феномену, зокрема «мережеве суспільство», «суспільство нового типу», «постіндустріальне суспільство», «суспільство знань», «інформаційне суспільство» тощо.

У дисертаційній роботі використовується комплексне поняття «глобальне інформаційне суспільство», під яким пропонується розуміти не просто нову суспільну формацію, а усю повноту правовідносин (правопорядок), що виникають в інформаційній сфері, а також унікальне поєднання демократичних інституцій,

політичних режимів, сприятливого для інновацій середовища та активного і структурованого громадянського суспільства, що виникли та розвиваються в рамках глобального та інклюзивного кіберпростору, у якому відсутні фізичні кордони.

Ще одним базовим поняттям термінологічного апарату дисертаційного дослідження є «кіберпростір», що в авторському визначенні означає специфічне середовище, в межах якого на основі використання Інтернету та відповідних інформаційно-комунікаційних технологій здійснюється обіг товарів та послуг, відбувається комунікація та реалізація прав людини, ведеться боротьба за розподіл сфер впливу та формуються власні механізми управління глобальним інформаційним суспільством. На нормативно-правовому рівні потребують врегулювання як питання використання та контролю над інформаційною інфраструктурою, так і самі суспільні відносини, що виникають у межах кіберпростору.

Стан сучасного міжнародного права означено поняттям нормативного індетермінізму, що зумовлює необхідність вдосконалення класичних міжнародно-правових концепцій суверенітету, кордонів, громадянства, територіальності та юрисдикції з метою відображення еволюційних змін, викликаних розвитком глобального інформаційного суспільства. Уявлення про кіберпростір як середовище у якому відсутні будь-які географічні кордони потребує нормативної реакції з боку міжнародного права. Однак, таке регулювання не може бути ефективним за умови застосування територіально орієнтованих правових актів до транскордонного глобального простору.

Доведено, що відображення на нормативному рівні змін у суспільних відносинах, зумовлених формуванням глобального інформаційного суспільства, сприятиме прогресивному розвитку міжнародного права. Наразі правова та соціальна системи досягли того рівня синергії , коли очевидним є не лише трансформуючий вплив глобального інформаційного суспільства на міжнародне право, але й стає невідворотним нормативне закріплення правових основ та стандартів функціонування та еволюції такого суспільства.

Розроблено авторську періодизацію еволюції адаптивності міжнародного

права до питань розвитку глобального інформаційного суспільства, що підтверджує робочу гіпотезу про позитивний трансформуючий вплив глобального інформаційного суспільства на міжнародне право. Прогресивний розвиток останнього проявляється у розширенні його регуляторної спроможності за рахунок охоплення широкого кола питань розвитку глобального інформаційного суспільства.

Пропонується розпочинати відлік взаємопроникнення міжнародного права та питань розвитку глобального інформаційного суспільства з моменту прийняття документів з питань розбудови нового світового інформаційно-комунікаційного порядку (НСІКП) (1970-ті – 1990-ті рр. XX ст.). Наступний етап конвергенції датується 2003 роком та пов'язується з початком проведення Всесвітнього саміту інформаційного суспільства (ВСІС). Оцінка здобутків цього історичного періоду та перехід до наступного етапу відбувається наприкінці 2015 року із ухваленням Фінального документу ВСІС+10. Підведення підсумків цього етапу очікується у 2025 році. Крім того, паралельним поступом розвивається імплементація Плану дій «*Connect 2020*» та цілей сталого розвитку ООН на період до 2030 року.

Примітно, що усі виділені автором етапи пов'язані з нормотворчими ініціативами, прийнятими в рамках ООН. Остання, будучи класичною міжнародною організацією, демонструє успішні приклади практичної реалізації моделі багатосторонньої участі та посиленої співпраці. Крім того, запропонована в дисертаційній роботі періодизація свідчить про поступове зростання адаптивності міжнародного права до перманентно та динамічно еволюціонуючих суспільних відносин в інформаційній сфері.

Запропоновано розрізняти два типи інституційних моделей, в рамках яких відбувається формування політики та стандартів управління глобальним інформаційним суспільством. Перша модель ґрунтується на традиційному міждержавному механізмі, прикладом якого може бути співпраця в рамках ООН. В основі іншої моделі – принцип багатосторонньої участі, що передбачає залучення різноманітних недержавних суб'єктів. На даному принципі побудована діяльність, зокрема, ICANN та Форуму з управління Інтернетом (IGF).

Комплексний аналіз універсальних та регіональних інституційних ініціатив та їх значення у процесах нормотворення з питань глобального інформаційного суспільства дозволяє зробити висновок про те, що множинність інституційних механізмів може зрештою призвести до небажаної фрагментації екосистеми Інтернету. Натомість єдина глобальна інституційна структура повинна представляти інтереси усіх країн та усіх зацікавлених сторін. Інтернет став технологічною інновацією, що наразі потребує інноваційного підходу до інституційної та регуляторної сфер.

Тривалий час кіберпростір розглядався як середовище, вільне від державного регулювання в силу його динамічної природи та розподіленої архітектури. Втім, встановлено, що уряди продовжують здійснювати свої суверенні повноваження щодо контролю над інформаційними потоками в кіберпросторі, а також щодо застосування обмежень і заборон на поширення певного контенту у межах своєї територіальної юрисдикції, яку вони автоматично поширюють на онлайнове середовище. Досі не знайшли належного відображення у міжнародному праві міжнародні та глобальні процеси і механізми, покликані вирішувати питання інституціоналізації розвитку інформаційного суспільства. Нормативне закріплення даних аспектів є вкрай важливим, оскільки держави повинні співпрацювати між собою в межах визначених нормативних рамок, а не правового вакууму.

Продемонстровано, що роль держав як суб’єктів глобального інформаційного правопорядку чи не вперше за всю історію міжнародного права перестає бути лідируючою. Обґрунтовано перехід від державоцентричної до людиноцентричної системи міжнародно-правового регулювання. Крім того, визнання концепцій розподіленого суверенітету та багатосторонньої участі повинно стати органічним відображенням відповідних трансформацій у нормотворчій активності суб’єктів, спрямованій на регулювання суспільних відносин, опосередкованих використанням Інтернету (більш розгорнута аргументація цієї тези буде наведена у розділі 2 дисертації).

Основі висновки розділу висвітлені у наукових працях автора [101-104].

РОЗДІЛ 2
ОСОБЛИВОСТІ НОРМОТВОРЕННЯ З ПИТАНЬ РОЗВИТКУ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

2.1. Характеристика джерел унормування правовідносин в інформаційній сфері

Наразі система нормативного регулювання інформаційної сфери є швидше трискладовою, аніж двоскладовою. Так, окрім традиційних систем національного та міжнародного права, де первинними та основними суб'єктами виступають суверенні держави, з'являється транснаціональне право, що визнає нормотворчу функцію також за недержавними приватними акторами [105, с. 130–145].

Нетривала історія розвитку інформаційного суспільства є однією з основних причин відсутності великого масиву договірних міжнародно-правових норм у цій сфері. Найбільш значимими договорами є Конвенція Ради Європи про кіберзлочинність 2001 року та Додатковий протокол щодо криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи 2003 року, Угода держав-членів ШОС про співпрацю у сфері забезпечення міжнародної інформаційної безпеки 2009 року, Статут та Конвенція МСЕ 1992 року з відповідними змінами.

М. Шмітт та Л. Віхул зазначають, що якщо дотримуватися підходу, згідно з яким договори загального міжнародного права можуть застосовуватися до регулювання кіберпростору, діяльність у межах останнього значно обмежується міжнародними договорами, що регулюють поведінку держав безвідносно до кіберпростору. Так, Конвенція з морського права 1982 року встановлює норми поведінки суден однієї держави у територіальному морі іншої держави. Хоча суднам надається право проходу, останній повинен бути мирним та не суперечити інтересам прибережної держави. Отже, незважаючи на те, що Конвенція 1982 року не містить положень щодо кіберпростору, здійснення

кібероперації проти прибереженої держави з борту морського судна буде порушенням права мирного проходу. Аналогічним чином, Угода про Місяць 1979 року передбачає використання Місяця та інших небесних тіл виключно у мирних цілях. А, отже, військові кібероперації не можуть бути здійснені з поверхні Місяця чи інших небесних тіл. І це при тому, що даний міжнародний договір був ухвалений задовго до появи відповідних технологій. Так само не могли передбачити усі нюанси й розробники Європейської конвенції з прав людини 1950 року, що наразі застосовується для регулювання питань приватності та захисту персональних даних у кіберпросторі [106, с. 13-14].

Однозначно, ухвалення універсального міжнародного договору з питань кіберпростору дозволило б значною мірою унормувати міждержавні відносини в інформаційній сфері. Однак, історія міжнародного права свідчить, що процес формування договірного механізму є доволі тривалим та затяжним. Так, незважаючи на тисячолітню історію морських перевезень та торгівлі, відповідний договірний режим з питань морського права з'явився лише у 1958 році з ухваленням Конвенції про територіальне море та прилеглу зону та Конвенції про відкрите море. Втім, досі відсутня міжнародна угода щодо повітряних військових операцій. В обох випадках нестача договірного регулювання доволі успішно компенсувалася зміцненням звичаєвих норм.

Міжнародні договори, ускладнені технологічною складовою, часто укладаються вже після того, як відповідні технології певний час знаходяться в обороті та виявляють прогалину у чинному міжнародно-правовому регулюванні. Прикладами можуть бути Оттавська конвенція про заборону протипіхотних мін 1997 року та Дублінська конвенція про заборону касетних боєприпасів 2008 року, що з'явилися у відповідь на неоднозначне ставлення до використання відповідних технологій у військових операціях. Ухвалення універсальних договорів з питань кіберпростору ускладнюється різним рівнем розвитку держав, а також їх небажанням обмежувати себе юридично обов'язковими рамками в контексті технологій, темпи та можливості розвитку яких не дозволяють робити довгострокові передбачення на нормативному рівні. Складним залишається питання створення ефективних контрольних механізмів, які б забезпечували дотримання відповідних договорів з питань кіберпростору. Анонімність дій у кіберпросторі значно ускладнює процес встановлення винних суб'єктів та притягнення їх до відповідальності.

Цікава позиція у контексті формування універсального режиму міжнародно-правового регулювання кіберпростору була висловлена Сполученим Королівством та представлена Генеральному Секретарю ООН. Так, Сполучене Королівство висловило сумнів щодо імовірності укладення універсальних, багатосторонніх угод, кодексів поведінки чи подібних документів, що сприяли б посиленню співпраці у сфері кібербезпеки у найближчому майбутньому. Складний та всеохоплюючий характер будь-якої юридично обов'язкової угоди з питань кіберпростору, що розвивається з надзвичайною швидкістю, потребує багаторічної роботи над нормами поведінки та заходами зміцнення довіри, покликаними забезпечити належний рівень порозуміння між державами-підписантами і гарантувати їм право розумно очікувати виконання своїх зобов'язань іншими сторонами. Досвід з укладення подібних договорів у інших сферах свідчить про те, що вони будуть ефективними лише тоді, коли являтимуть собою результат досягнення консенсусу, а не будуть метою самі по собі. Тобто, зусилля міжнародного співтовариства повинні бути спрямовані на вироблення спільного розуміння міжнародного права та окремих норм у контексті кіберпростору, на противагу веденню переговорів щодо укладення обов'язкових угод, що є передчасними та недосконалими для регулювання нової сфери [107].

Ухвалення універсальних договорів не має сенсу за умови, коли держави роблять застереження або роками не ратифікують документ, тим самим не беручи на себе жодних юридичних зобов'язань. Одним із найбільш вдалих багатосторонніх документів з питань кіберпростору вважають Конвенцію Ради Європи про кіберзлочинність. Втім, при детальному аналізі стану її ухвалення, стає зрозумілим, що навіть станом на квітень 2016 року лише 54 держави підписали Конвенцію, 6 з яких ще не ратифікували її. При цьому 26 держав зробили застереження, а 25 – оформили декларації [108].

У силу нерозвиненості договірного міжнародно-правового регулювання кіберпростору відбувається формування звичаєвого кіберправа. Крім того, збереження ролі звичаю як джерела міжнародного права пояснюється тим, що більшість договірних режимів не є універсальними, натомість звичаєві норми інколи мають більше охоплення за колом суб'єктів, що вважають себе зобов'язаними цією нормою. Для встановлення наявності міжнародних звичаїв у кіберпросторі необхідно проаналізувати відповідну практику держав, що охоплює період з моменту появи Інтернету до цього часу. При цьому

застосовується принцип «*opinio juris ac necessitatis*», у силу якого причиною дотримання індивідами певних норм та правил, що існують у рамках певної спільноти, є переконання (*opinio*), що така поведінка є загальновизнаною практикою в рамках спільноти, а отже становить юридичне зобов'язання (*necessitatis*) [109, с. 63].

Для того, щоб норма встигла стати загальним правилом поведінки держав, повинен пройти достатній період часу. У контексті швидкого розвитку ІКТ постало питання про те, як трактувати елемент тривалості загальної практики. Якщо така тривалість не є достатньою, чи доречно говорити про те, що звичай не може бути джерелом регулювання правовідносин в інформаційній сфері. Цікава думка з цього приводу була висловлена Роберто Аго, що сформулював концепцію *diritto spontaneo*, тобто миттєвого звичаєвого міжнародного права [110, с. 932]. Концепція ґрунтується на елементі *opinio juris*, не вимагаючи існування тривалої практики застосування норми поведінки. Підтвердженням такого підходу може слугувати рішення Міжнародного Суду ООН у справі про континентальний шельф Північного моря, яким було визнано, що обов'язковими умовами визнання існування миттєвого звичаю є частота та одноманітність застосування норми навіть протягом доволі короткого періоду часу [111].

Показовим прикладом миттєвого формування звичаєвих норм може вважатися міжнародне космічне право. Концепція миттєвого звичаю була підтримана представником США у Комітеті ГА ООН з питань мирного використання космічного простору у контексті ухвалення Генеральною Асамблеєю двох резолюцій щодо космічного простору. Так, йшлося про можливість миттєвого виникнення міжнародного звичаєвого права, тобто загального міжнародного права, застосовного *erga omnes*, шляхом одноголосного ухвалення резолюцій Генеральної Асамблеї [112, с. 136].

Бін Ченг вважає, що нова норма міжнародного звичаєвого права або іншими словами неписана норма міжнародного права може сформуватися в дуже стислі строки на основі «*opinio communis juris*», підтриманої усіма або лише деякими державами-членами ООН. А сам зміст норм міжнародного звичаєвого права може змінюватися залежно від відповідної *opinio juris* держав у кожен конкретний період часу. Формою закріплення такої норми може бути її відображення у тексті правовстановлюючої резолюції [112, с. 139]. Так, резолюції Генеральної Асамблеї ООН дозволяють охопити та систематизувати практику держав у

сферах, що стрімко розвиваються, хоча при цьому вони й зберігають свою декларативну форму. Прикладом формування миттєвого звичаю була визнана реакція міжнародного співтовариства на терористичну загрозу міжнародному миру та безпеці [113].

Процес формування звичаєвого права кіберпростору є доволі неоднозначним. Високий поріг анонімності часто не дозволяє провести необхідну атрибуцію між вчиненим діянням та винним суб'єктом. Держави висловлюючи політичну та моральну незгоду із відповідними порушеннями, утримуються від правових оцінок, тим самим залишаючи за собою ширші можливості вчинити подібним чином у майбутньому, якщо це відповідатиме їх економічним, політичним чи безпековим інтересам. З огляду на це, складно говорити про одноманітність державної практики. Різний рівень технологічного розвитку держав світу свідчить про більшу ймовірність формування регіональних звичаєвих норм у сфері кіберпростору, аніж універсальних стандартів.

У Міжнародній стратегії з питань кіберпростору, розробленій Білим Домом у 2011 році, йдеться про те, що формування норм поведінки держав у кіберпросторі не потребує нових звичаєвих норм міжнародного права та не заперечує ефективності чинних міжнародно-правових норм. Відтак, міжнародне право, що регулює поведінку держав у мирний час та у період війни, рівною мірою застосовується до кіберпростору [114]. У той же час, у документі містилося застереження про особливі характеристики мережевих технологій, що вимагають уточнення щодо того, яким чином діючі норми будуть застосовуватися до кіберпростору та які додаткові тлумачення необхідні задля розширення їх сфери дії.

Серед переваг звичаєвого міжнародного права з питань Інтернету Уоррен Чік називає наступні: залучення до процесу нормотворення усіх зацікавлених сторін, створення додаткового стимулу для держав та міжнародних організацій для подальшого розвитку та деталізації таких звичаєвих норм, а також сприяння судам у вирішенні зростаючої кількості спорів з метою гармонізації судової практики [115, с. 9].

Тут слід також згадати, що ідея про право індивідів на участь у формуванні звичаєвого міжнародного права датується ще 1967 роком. Саме тоді МакДугал, Ласвелл та Райсмен зауважили, що незважаючи на неможливість безпосередньої участі кожного індивіда у процесах нормотворення, визнання самого права такої участі на противагу

концепції міжнародного права як права міждержавного сприятиме більш ефективній участі індивідів та мінімізує відчуття політичної незначимості останніх [116, с. 193-194]. Про розширення правосуб'єктності на недержавних акторів говорили й інші вчені. Зокрема, згадувалося про зростання орієнтованості міжнародного права на забезпечення прав людини, що цілком логічно повинно сприяти зростанню залученості індивідів до процесів створення норм, спрямованих на регулювання правовідносин між ними [117, с. 123].

Протягом останніх трьох десятиліть у теорії міжнародного права сформувалася концепція «м'якого» права як чогось середнього між «твердим» правом та відсутністю нормативного регулювання. Деякі вчені висловлювали думку про те, що назріла необхідність у зближенні цих двох правопорядків з метою подолання дихотомії між «твердим» та «м'яким» правом, а також додаткового забезпечення виконання норм «м'якого» права за допомогою санкцій, доступних державам [118, с. 8]. Традиційно «тверде» право орієнтоване на закріплення чітких правил поведінки з метою гарантування передбачуваності та стабільності нормативних положень для відповідних суб'єктів правовідносин. Втім, такому підходу бракує достатньої адаптивності, а тому він не здатен своєчасно відображати перманентні зміни у правовідносинах у рамках інформаційного суспільства [119, с. 568–572].

В умовах глобального інформаційного суспільства суб'єкти міжнародного права зіштовхуються з ситуаціями, які виходять за рамки класичного нормативного регулювання, що поступово підриває авторитет діючих міжнародних інституцій та ставить під сумнів ефективність чинних міжнародно-правових норм та принципів. Наразі відсутня єдність міжнародного права та правопорядку, що склався та розвивається в рамках інформаційного суспільства. Фактично, відбувається латентна криза позитивного міжнародного права, пов'язана з тим, що держави та діючі міжнародні організації не можуть запропонувати ефективних альтернативних засобів регулювання правовідносин у рамках глобального інформаційного суспільства.

«М'якість» цілком може бути однією з ключових характеристик епістемології постмодернізму. Поняття «м'якого права» відображає дві основні тенденції у процесі глобалізації права: вражаючу мультиплікацію суб'єктів правотворчості та, як результат, галузей права, а також роздержавлення правових режимів [120].

Російська вчена Т. М. Нешатаєва зазначає, що у західній правовій доктрині сформувалася концепція поділу міжнародного права на «м'яке» право (рекомендаційні норми) та «тверде» право (обов'язкові норми) [121, с. 10]. Під «твердим» правом розуміють юридично обов'язкові правові документи, прийняті державами. У італійській правовій доктрині «м'яке» право визначається як правила поведінки, що в принципі не мають юридичної обов'язковості, але можуть мати практичний ефект [122, с. 208]. Норми «м'якого» права не обов'язково приймаються недержавними суб'єктами. Їх розробниками рівною мірою можуть бути держави. На думку І. І. Лукашука, норми «м'якого» права стають важливим елементом міжнародно-правової системи. Вони вирішують задачі, які з тих чи інших причин не може розв'язати «тверде» право [123, с. 163]. «М'яке» право дозволяє швидко досягти згоди та уникнути затягування переговорного процесу на довгі роки з метою вироблення компромісного рішення. Вони жодним чином не обмежують суверенні права держав, сприяючи розширеній та взаємовигідній співпраці з особливо важливих питань [124, с. 321].

На думку Є. Ерліха, для того, щоб зрозуміти, яке право дійсно є чинним, слід «відшукати живе право». Це означає дослідити середовище виникнення й дії права як емпіричної реальності. Джерелом пізнання права відтак повинні стати не закони, юридична догматика, юридична література, а безпосереднє спостереження життя, вчинків, вивчення звичаїв, документів, які відображають здійснення «права» [125]. Вчений закликає інших і сам досліджує дійсно практиковане в суспільстві «право». Не відкидаючи офіційного державного права, Ерліх, по суті, розширює базу праворозуміння, сприяє глибшому дослідженню його джерел. У свою чергу Лоуренс Лессіг зауважував, що основними регуляторами Інтернету та інших форм цифрової комунікації є закон, ринок, норма та архітектура чи код [126, с. 19].

«М'яке» право характеризується гнучкістю та високим ступенем адаптивності до змін, пов'язаних із розвитком та ускладненням об'єкту регулювання. Актами «м'якого» права можуть бути декларації та резолюції, кодекси поведінки та кращих практик, рекомендації та керівні принципи тощо. Домінування юридично обов'язкових міжнародно-правових документів впродовж тривалого часу залишало поза увагою великий масив актів «м'якого» права. Однак, поява концепції глобального інформаційного суспільства та

спроби її нормативного забезпечення надзвичайно гостро поставили питання про ефективність саме «м'якого» міжнародно-правового регулювання даної сфери правовідносин.

Цікавим є приклад Європейського Союзу, в рамках якого норми «м'якого» права стали особливо поширюватися після ухвалення Лісабонського плану дій 2000 року, яким запроваджувався відкритий метод координації [127]. Даний метод передбачав розробку актів «м'якого» права та добровільну співпрацю у визначених сферах, що повинні були стати альтернативою примусовим правовим приписам. ЄС робив неодноразові спроби створити максимально ефективну систему управління, засновану на поєднанні «м'якого» та «твердого» правового регулювання. У контексті ЄС дієвість засобів «м'якого» права може бути виміряна через оцінку того, наскільки вдалося досягти уніфікації регулювання у відповідних сферах на наднаціональному рівні. Традиційно обов'язковими актами ЄС вважалися директиви, які держави-члени імплементували у національне законодавство. Втім, труднощі виникали уже тоді, коли держави вважали, що їхні суверенні права занадто обмежуються на користь наднаціональних органів. Враховуючи технічну орієнтованість значної частини правових актів, пов'язаних з окремими аспектами функціонування інформаційного суспільства, необхідно передбачити максимально гнучкий механізм перегляду нормативних актів та внесення до них відповідних змін та поправок. Саме такий механізм і здатне забезпечити «м'яке» право.

Прихильники гібридності міжнародно-правового регулювання виступають за комбінування традиційного «твердого» права та «м'яких» правових процесів. Підкреслюючи переваги «м'якого» права як органічного соціального продукту, що забезпечує ефективність та плюралістичну повагу до різноманіття, вони стверджують, що воно може бути більш ефективним у поєднанні з «твердим» правом. Гібриди можуть мати різноманітну форму. Перевага надається поєднанню процесів відкритого методу координації з рамковими директивами. «М'яке» право, таким чином, виступає як «живе право», що доповнює традиційні «тверді» норми. «Твердо-м'які» гібриди вважаються високоефективними комбінаціями: їх «м'які» компоненти гарантують органічну оперативність реагування на суспільні потреби, сприяють плюралізму та співучасті, активізують взаємне навчання; «тверді» елементи забезпечують більш високий рівень

дотримання нормативних вимог, оскільки зникає можливість ігнорувати «м'які» норми, що дозволяє ефективно виправляти асиметрію між гармонізацією ринку та соціальною інтеграцією [120].

До середини 1990-х років держави-члени ЄС домовилися щодо створення європейського регуляторного забезпечення телекомунікаційного сектору засобами юридично обов'язкових правових приписів, що дозволило суттєво лібералізувати та гармонізувати правовідносини у даній сфері. Однак, ключова проблема була пов'язана з різними підходами самого ЄС та його держав-членів до перспектив управління телекомунікаціями. У той час, як ЄС виступав за створення наднаціонального механізму, держави-члени надавали перевагу міжурядовій системі контролю [128]. Ключову роль у розробці «м'якого» правового регулювання питань, пов'язаних з інформаційним суспільством і, зокрема, телекомунікаційним сектором відіграла Європейська Комісія. Вона виступила у ролі посередника між державами та технічними спільнотами з метою вироблення загальноприйнятних юридичних формулювань.

Крім того, самі держави-члени надали перевагу «м'яким» засобам правового регулювання як способу уникнення надмірного юридично обов'язкового регулювання, що прийматиметься на рівні ЄС. «М'яке» право дає державам-членам більшу свободу дій у контексті імплементації відповідних правових актів. Цікавим прикладом є поєднання засобів «м'якого» та «твердого» правового регулювання. Часто це проявляється у формі директиви, у тексті якої прописується ряд певних заходів, що за своєю природою є тимчасовим «м'яким» регулюванням. Так, Директива 2000/31/ЄС про електронну комерцію закріпила ряд правових положень, спрямованих на створення єдиного європейського ринку електронної комерції. У той же час, у документі міститься мінімум вимог до постачальників інформаційних послуг та зазначається, що держави-члени та Комісія мають заохочувати розробку кодексів поведінки та надавати можливість вільного вирішення зацікавленими сторонами, чи дотримуватись положень таких кодексів [129].

Такий змішаний підхід, застосований ЄС, має ряд переваг. По-перше, на момент прийняття Директиви було відсутнє розуміння особливостей розвитку електронної комерції в умовах інформаційного суспільства. ЄС тим самим убезпечив себе від застосування надто обтяжливих правових приписів до європейських фірм при здійсненні ними операцій на

глобальному ринку в мережі Інтернет, що лише почав набирати оберти. По-друге, з урахуванням швидких темпів технологічного прогресу ЄС намагався створити такі правові рамки, які не довелося б переглядати в короткостроковій перспективі лише через те, що вони здійснюють стримуючий ефект по відношенню до тих правовідносин, які покликані регулювати. По-третє, це була спроба створити кращий регуляторний механізм порівняно з телекомунікаційною сферою.

Ключовою характеристикою Інтернету є його транскордонний характер. З правової точки зору, кіберпростір є місцем переплетення багатьох юрисдикцій, принципів та норм, а тому він не може належати жодній суверенній державі. У зв'язку з цим виникає величезна кількість колізій, пов'язаних з практичним регулюванням правовідносин в інформаційному суспільстві. Так, особа може здійснити злочин у мережі, що порушуватиме правовий порядок одразу кількох держав. При цьому буде відсутня будь-яка фізична прив'язка до території таких держав, а місце знаходження винної особи буде неможливо встановити в силу технічних причин. Ще одним прикладом може бути надання правової допомоги в мережі в рамках юрисдикцій, відповідно до законодавства яких дана особа не має права займатися юридичною практикою. Отже, поряд з новими можливостями виникає чимало труднощів та загроз, що потребують належного регулювання на нормативному рівні.

Наразі не вироблено єдиних підходів до регулювання питань розвитку глобального інформаційного суспільства. Одні вчені підтримують концепцію саморегулювання, наголошуючи на тому, що будь-яке державне втручання суперечить самій природі Інтернету. Інші, навпаки, переконані, що саме держави здатні забезпечити рівні умови використання інформаційно-комунікаційних технологій. Однак, немає солідарності і в межах кожного з окреслених вище підходів. Так, у США саморегулювання заохочується у сферах електронної торгівлі та приватності. Втім, уряд залишає за собою виключні повноваження щодо таких питань як шахрайство, дитяча порнографія та національна безпека. В ЄС зберігається переважно централізований підхід до регулювання [130, с. 242]. Існування таких протилежних підходів створює колізії у правозастосуванні.

З одного боку, Інтернет-користувачі, провайдери та розробники програмного забезпечення краще розуміються на особливостях інформаційно-комунікаційних процесів та здатні приймати технологічно обґрунтовані норми та правила. З іншого боку, їм бракує

репрезентативності та відповідальності. У той же час, неврахування державами та міжнародними організаціями інтересів кінцевих Інтернет-користувачів стане передумовою для використання ними інформаційно-комунікаційних технологій з метою обходу надто обтяжливих та непрактичних правових приписів.

В умовах інформаційного суспільства відбувся перерозподіл владних функцій, що зумовило появу нових джерел права. Впродовж тривалого часу вважалося, що впорядкування суспільних відносин можливе лише під владою суверена, що виконує представницькі функції та притягує до відповідальності тих, хто не підкоряється його волі. Ніхто не може піддавати сумніву рішення суверенних держав, оскільки саме вони приймають обов'язкові до виконання правові норми. Міжнародне право є свого роду природним станом взаємодії держав. Крім того, ще у 1956 році Ф. Джессап звернув увагу на формування транснаціонального права, що регулює дії та події транскордонного характеру, охоплює як публічне, так і приватне міжнародне право, а також норми, що не підпадають під жодну з означених категорій [131].

Традиційно дотримання норм національного та міжнародного права пов'язане із загрозою застосування примусу та санкцій. В умовах глобального інформаційного суспільства даний принцип не діє. Спроби врегулювати на нормативному рівні випадки, пов'язані з мережевими крадіжками, спамом, розповсюдженням вірусів, кібератаками, кібертероризмом, засвідчили неефективність чинних міжнародно-правових механізмів, тим самим створивши сприятливі умови для поширення нових загроз міжнародному миру, індивідуальній та національній безпеці. Дуже вдале визначення Інтернету як саморегулівного простору індивідуальної свободи поза межами державного контролю знаходимо у Солума [132, с. 56].

З появою транснаціонального права нормотворчість перестає бути виключним правом держав. Велика кількість міжнародних документів з питань інформаційного суспільства була розроблена та прийнята за участі недержавних акторів. При вирішенні інфраструктурних питань організації Інтернету позиція суверенних держав не є головним пріоритетом. Так, ICANN, будучи глобальною корпорацією, зареєстрованою за законодавством штату Каліфорнія, приймає обов'язкові до виконання норми. При цьому відповідальність покладається на національних реєстраторів. Така впливовість приватної

компанії підриває класичну ідею верховенства суверенних держав.

Ефективними регуляторними інструментами в глобальному інформаційному суспільстві виявилися засоби «м'якого» міжнародного права, які хоч і не мають обов'язкової сили, втім надзвичайно оперативно реагують на нові виклики та відображають інтереси усіх відповідних суб'єктів. Незобов'язуючим нормам притаманна значна нормативна цінність [133, с. 449]. Показовим є той факт, що в інформаційному суспільстві застосовується значна кількість превентивних механізмів, спрямованих на попередження неправомірної поведінки. Автоматизація права через застосування таких технологій, як системи фільтрування електронних комунікацій, управління цифровими правами чи налаштування приватності за умовчанням відбувається згідно з принципом, відповідно до якого наслідки автоматично настають при конкретних технічних умовах. У той же час, в основу сучасного міжнародного права покладено принцип застосування санкцій у відповідь на порушення правових приписів [134].

Приватний сектор відреагував на труднощі суверенних держав щодо правозастосування у цифровому середовищі шляхом розробки технологічних засобів, що дозволяли правовласникам здійснювати моніторинг, керівництво та контроль за використанням об'єктів їхньої творчості. Деякі держави на законодавчому рівні закріпили так звану доктрину «трьох попереджень», відповідно до якої відключення користувача відбувається після трьох попереджень у порушенні авторських прав. Існує хибне переконання, що використання автоматизованих систем блокування та фільтрування контенту в мережі Інтернет вирішує проблему правозастосування у кіберпросторі та дозволяє уникнути конфлікту юрисдикцій і суперечностей у тлумаченні міжнародно-правових норм. Технологічні інновації обов'язково повинні бути враховані при розробці нормативно-правового регулювання. Так, у розумінні Директиви Європейського Парламенту та Ради 2000/46/ЄС «Про започаткування та здійснення діяльності установами-емітентами електронних грошей та пруденційний нагляд за ними» електронні гроші виконували функцію цифрового аналога паперових грошей, контроль за обігом яких здійснювався національними фінансовими інституціями. Втім, особливості електронних розрахунків та транзакцій засвідчили неефективність простого перенесення режиму регулювання онлайнових операцій у кіберпростір. У зв'язку з цим була прийнята нова

Директива 2009/110/ЄС.

Технологічна орієнтованість міжнародного права в епоху інформаційного суспільства є необхідною умовою його трансформації у дієвий регулівний механізм, що відповідає вимогам часу та інтересам суб'єктів. Якщо суб'єкти правовідносин не усвідомлюють чіткого зв'язку між вимогами правових приписів та своєю поведінкою у кіберпросторі, вони швидше за все відмовляться від дотримання таких приписів у силу їх невідповідності [135]. Одна з важливих проблем захисту прав та свобод людини в цифровому середовищі пов'язана з охороною авторського права та інших об'єктів інтелектуальної власності. Слід віднайти оптимальний баланс між закріпленими у статті 27 Загальної декларації прав людини «правом вільно брати участь у культурному житті суспільства, втішатися мистецтвом, брати участь у науковому прогресі і користуватися його благами» та «правом кожної людини на захист моральних і матеріальних інтересів, що є результатом наукових, літературних або художніх праць, автором яких вона є» [136]. Іншим серйозним аспектом є використання кіберпростору у військових цілях. Зростання кількості кібератак та нездатність держав гарантувати безпеку у кіберпросторі піднімають питання про пошук тих сил та механізмів, які зможуть забезпечити мир та правопорядок в інформаційному суспільстві.

«М'яке» право є динамічним за своєю природою і здатне оперативно реагувати на зміни у правовідносинах між відповідними суб'єктами. Виконуваність норм національного права забезпечується силою державного примусу. Щодо міжнародного права, то навіть «тверде» право ніколи не ставило за мету створити централізований правозастосовний механізм, який би здійснював контроль за виконанням державами взятих на себе міжнародно-правових зобов'язань. Таким чином, держави укладаючи формально обов'язкові міжнародні договори підвищують рівень довіри та гарантованості виконання зобов'язань. Цій же меті слугують інтеграційні об'єднання різних типів. Порушення норм «твердого» права має значно більш негативні наслідки для іміджу держави, ніж порушення приписів «м'якого» права.

Відмітною рисою актів «м'якого» права є значно менші витрати, пов'язані з їх укладенням, у порівнянні з класичними міжнародними договорами. Для укладення останніх держави, як правило, проводять не один етап переговорів та намагаються

мінімізувати можливі ризики, пов'язані з виконанням закріплених у договорі зобов'язань, оскільки відповідальність за їх порушення є більш серйозною. Крім того, процес прийняття міжнародного договору затягується в силу дотримання багатьох процедурних моментів.

Показовими у даному контексті є два наступні випадки. Упродовж тривалого часу Міжнародна організація праці (МОП) приймала проекти конвенцій, що підлягали подальшій ратифікації державами. Втім, останні все частіше почали відмовлятися від ратифікації даних конвенцій, що відповідно негативно позначалося на іміджі організації. Зрештою, було прийнято рішення про переорієнтацію МОП у напрямку розробки юридично необов'язкових документів, зокрема рекомендацій та кодексів поведінки. Високі витрати на переговорний процес були використані у якості тактики затягування при обговоренні Конвенції ОЕСР про боротьбу проти підкупу іноземних посадових осіб у міжнародних ділових операціях 1997 року. США прагнули ліквідувати комерційні диспропорції, викликані дією Акту про іноземні корупційні дії, шляхом прийняття юридично обов'язкового договору, який би закріплював однакові регуляторні рамки для всіх держав-членів ОЕСР. Держави, які у своїй комерційній практиці протидіяли будь-яким подібним ініціативам, виступили на підтримку США. Тим самим вони сподівалися затягнути прийняття міжнародного договору в силу високих витрат, необхідних для ведення переговорного процесу. У відповідь на це США висловились за ухвалення юридично необов'язкової рекомендації ОЕСР. Сторонам вдалося досягнути компромісу, встановивши короткі часові рамки для прийняття міжнародного договору або рекомендації, якщо відповідний договір не буде ухвалено в обумовлені строки [137].

Політизація обговорень правових актів не завжди є доречною, оскільки вона значно затягує переговорний процес та позбавляє суб'єктів об'єктивності при виробленні спільного рішення. Крім того, державам значно складніше погодитися на прийняття юридично обов'язкових міжнародно-правових документів, оскільки йдеться про певне обмеження їхнього суверенітету в загальних інтересах. Акти «м'якого» права дозволяють державам оцінити наслідки їхньої імплементації та внести відповідні зміни в оперативному порядку. Підтвердженням цьому є міжнародно-правові акти у ядерній сфері [138]. Незважаючи на те, що основні зобов'язання держав закріплені в Договорі про нерозповсюдження ядерної зброї та ряді інших юридично обов'язкових документів, чимало

важливих питань, зокрема захисту ядерних матеріалів, регулюється на рівні рекомендацій Міжнародного агентства з атомної енергії. У рекомендаціях знаходять відображення технічні аспекти, такі як управління запасами та транспортування. Відображення подібних питань у тексті міжнародного договору на практиці є дуже складним завданням. У рекомендаціях також закріплюються питання, пов'язані з розробкою відповідної національної політики, зокрема створенням національних агентств та наглядом за приватним сектором. У випадках, коли державам вдається досягнути високого рівня консенсусу щодо питань, прописаних в рекомендаціях, вони інкорпорують до тексту міжнародного договору, як це мало місце щодо поводження з відпрацьованим ядерним паливом та радіоактивними відходами.

Міжнародний торговельний режим також демонструє переваги «м'якого» права у переговорному процесі щодо критично важливих питань. Запропонований статут Світової організації торгівлі містив юридично обов'язкові зобов'язання, обмежував право виходу зі складу організації, а також регулював значну частину економічних питань. Напрацювати проект такого документу було дуже складно. Його сильна інституційна складова викликала протистояння з боку США. У зв'язку з цим у 1947 році держави-учасниці ухвалили Генеральну угоду з тарифів і торгівлі (ГАТТ) у якості компромісного тимчасового регулівного механізму, спрямованого на скорочення тарифів. Порівняно з проектом статуту СОТ ГАТТ був набагато м'якшим у своїх формулюваннях. Він був розрахований на нетривале застосування, містив лояльне положення про вихід з договору та передбачав створення лише базових інституцій. З часом, коли держави усвідомили переваги чіткої регламентації міжнародної торгівлі, ГАТТ перетворився у СОТ. Однак, даний приклад свідчить про те, що прийняття юридично обов'язкових міжнародно-правових документів є складним та тривалим процесом.

Таким чином, держави завжди постають перед проблемою вибору при наданні переваги «м'яким» чи «твердим» засобам міжнародно-правового регулювання. «М'яке» право з'являється там, де досягнення компромісу на рівні зобов'язуючих нормативних приписів є вкрай складним або у сферах, що є недостатньо дослідженими в теорії та практиці міжнародного права і потребують подальшого юридичного аналізу.

При укладенні міжнародних договорів держави часто неохоче погоджуються брати

на себе зобов'язання, що значно обмежують їх суверенні права, особливо якщо йдеться про створення наднаціональних органів, до відання яких передається частина повноважень держав в окремих сферах. «М'яке» право дозволяє державам мінімізувати ризики, пов'язані з обмеженням їхнього суверенітету, шляхом прийняття незобов'язуючих норм та створення міжнародних установ чи організацій з чітко прописаними делегованими повноваженнями. Нечіткі формулювання та слабкий інституційний механізм виконують захисну функцію щодо державного суверенітету. Прикладом може слугувати Рамкова конвенція Ради Європи про захист національних меншин. Так, держави часто прописують процедуру, відповідно до якої держави-члени повинні дотримуватися положень спеціального протоколу до договору для встановлення юрисдикції суду чи квазісудового органу щодо них. Може також встановлюватися вимога досягнення згоди державами-сторонами у спорі щодо передачі справи на судовий розгляд [139].

Глобальне інформаційне суспільство є новою концепцією у міжнародному праві, розвиток якої справляє еволюційний вплив як на його нормативну, так і на інституційну складову. Держави в особі уповноважених осіб, як правило, недостатньо добре та комплексно обізнані з особливостями функціонування цифрового середовища, а тому на даному етапі складно говорити про розробку юридично обов'язкових міжнародно-правових документів. Спершу необхідно чітко усвідомити переваги та небезпеки, пов'язані з кіберпростором та використанням ІКТ. На даному етапі недостатній рівень дослідженості кіберпростору є причиною прийняття рамкових та декларативних міжнародно-правових документів. Спеціалізовані установи ООН та інші міжнародні організації уповноважені здійснювати, як правило, технічну координацію, інформування та виступати з ініціативою прийняття відповідних документів. Втім, найбільш серйозні питання міжнародного співробітництва завжди вирішувалися шляхом безпосередніх політичних переговорів за участі держав. Наприклад, Віденська конвенція про охорону озонового шару містить хоча й обов'язкові, однак доволі широко прописані положення, що дозволяє державам вирішувати конкретні практичні питання, що виникають з часом, у ході переговорів [140]. Сюди ж можна віднести також міжнародні договори щодо захисту прав жінок та дітей. Іншу категорію домовленостей становлять міжнародні угоди, що є доволі детальними, але не мають обов'язкового характеру, як наприклад Гельсінський Заключний акт. Такі угоди

часто закріплюють інституційний механізм у вигляді міжнародних конференцій чи сесій щодо перегляду тексту документу, що надає державам можливість адаптувати взяті на себе зобов'язання з урахуванням практичного досвіду реалізації положень відповідної угоди.

Показовим прикладом ефективності та дієвості «м'якого» регулювання може слугувати застосовуваний Продовольчою та сільськогосподарською організацією ООН (ФАО) і Програмою ООН з навколишнього середовища (ЮНЕП) режим, відповідно до якого вимагалася попередня згода на міжнародне переміщення шкідливих хімічних речовин та пестицидів. У 1985 році ФАО ухвалила Кодекс поведінки в галузі розподілу та застосування пестицидів. У свою чергу ЮНЕП у 1987 році затвердила Керівні принципи щодо обміну інформацією про хімічні речовини в міжнародній торгівлі. У 1989 році дані дві організації вирішили об'єднати зусилля, спрямовані на попередження експорту обмежених речовин до країн, що розвиваються, та закріпити обов'язок і процедуру отримання попередньої обґрунтованої згоди щодо переміщення небезпечних хімічних речовин. За підтримки ФАО та ЮНЕП було проведено консультації з експертними групами у складі представників урядів та промисловості. На конференції в Ріо-де-Жанейро у 1992 році була зроблена невдала спроба закріпити згадану вище систему погодження на рівні міжнародного договору. За кілька років держави-члени обох організацій ініціювали формальні переговори щодо укладення міжнародного договору, в результаті яких у 1998 році було схвалено Роттердамську конвенцію про процедуру Попередньої обґрунтованої згоди відносно окремих небезпечних хімічних речовин та пестицидів у міжнародній торгівлі [141]. Фактично на конвенційному рівні було закріплено систему, яка успішно функціонувала на основі актів «м'якого» права ФАО та ЮНЕП.

Прийняття актів «м'якого» права завжди полегшує процес вироблення компромісного рішення. Крім того, незобов'язуючі міжнародно-правові документи дозволяють державам пристосувати взяті на себе обов'язки до конкретних обставин, що значно практичніше ніж спроби уніфікувати в єдиному документі різноманітні та часто протилежні національні практики. Тим самим держави отримують широкий простір для імплементації угоди з одночасним її пристосуванням до політичного та економічного середовища всередині країни, що в свою чергу підвищує ефективність правозастосування. Це особливо актуально, коли йдеться про багатосторонні переговори. Тут слід звернути

увагу на те, що одним із основних принципів глобального інформаційного суспільства визнається багатостороння участь, а тому прийняття актів «м'якого» права в результаті таких переговорів є абсолютно закономірним процесом. Присутність політичного інтересу держав завжди ускладнює досягнення компромісу. А відсутність будь-якого правового регулювання не може вважатися кращою альтернативою навіть у порівнянні з юридично необов'язковими актами «м'якого» права.

Історія міжнародного права свідчить про те, що часто довготривалі переговори щодо ключових міжнародних договорів завершуються прийняттям текстів, до яких держави роблять велику кількість застережень або взагалі відмовляються від їх підписання чи ратифікації. У результаті маємо повноцінний міжнародний договір, якому бракує ефективного правозастосування. А без цього міжнародний договір є мертвим. Адже основним його призначенням повинно бути врегулювання конкретного виду правовідносин за участі якомога ширшого кола суб'єктів. Крім того, в умовах глобального інформаційного суспільства окрема увага приділяється країнам, що розвиваються, які, на жаль, не мають достатніх важелів впливу при розробці та прийнятті юридично обов'язкових міжнародних документів. Їм також бракує відповідних інституційних механізмів для імплементації відповідних міжнародних договорів. Режим багатосторонньої участі дозволяє таким державам бути почутими та відстоювати свої інтереси, які хоч і у вигляді норм «м'якого» права, але будуть закріплені у міжнародних документах. Згодом відповідні положення буде значно легше перевести в категорію юридично обов'язкових, ніж намагатися досягти консенсусу щодо них в ході первинних переговорів з більш сильними та розвиненими державами.

Прикладом використання «м'якого» права для прискорення досягнення компромісу може бути Вассенаарська домовленість щодо контролю за експортом звичайних озброєнь та товарів і технологій подвійного використання 1996 року [142]. Вассенаарська домовленість є правонаступницею Координаційного комітету зі здійснення контролю над експортом, що представляв собою неформальну інституцію, за допомогою якої Захід здійснював контроль за експортом до країн радянського блоку. США наполягали на створенні нової інституції, яка б займалася також безпековими питаннями, пов'язаними з тероризмом, регіональними конфліктами та посиленням військових спроможностей такими

неспокійними державами як Ірак. Однак укладенню міжнародного договору заважав ряд факторів: держави мали кардинально протилежні ставлення до окремих країн та конфліктів; витрати на контроль над експортом не могли бути рівномірно розподілені між державами; різний рівень технічної готовності держав до використання складних систем контролю над експортом; велика кількість зацікавлених держав. Цих труднощів вдалося уникнути шляхом прийняття юридично необов'язкової угоди. Відповідно до документу передбачається обмін інформацією щодо передачі озброєнь, а також чутливих товарів і технологій подвійного використання. Дана інформація виконує попереджувальну функцію щодо підозрілих експортних операцій та сприяє здійсненню контролю за комерційними ризиками самими суб'єктами експортних операцій. Держави-учасниці угоди імплементували її вимоги в національне законодавство. США поступилися кількома своїми вимогами, зокрема про отримання попередньої згоди щодо експортних продажів. Натомість до тексту угоди увійшли положення щодо звичайних озброєнь та товарів подвійного використання, окремі контрольні переліки.

Не можна заперечувати і зростаючу роль недержавних акторів у процесі міжнародного правотворення. Переважна більшість документів, що наразі регулюють цілий спектр питань, пов'язаних з інформаційним суспільством, були розроблені саме у ході багатосторонніх переговорів із залученням усіх зацікавлених сторін. Крім того, приватний сектор відіграє важливу роль у розробці нормативних стандартів щодо інвестицій, прав людини та захисту навколишнього середовища. Фактично, відбувається творення транснаціонального права, у розумінні якого повністю нівелюється значення державних кордонів як територіальної основи для поширення відповідної юрисдикції. Крім того, велика кількість міжнародних органів з вирішення спорів приймають скарги як від держав, так і від приватних заявників. Слід також враховувати той факт, що після інкорпорації норм міжнародного права до національного законодавства, вони вільно застосовуються приватними суб'єктами. Роль недержавних акторів проявляється у зростанні їхнього авторитету на міжнародній арені. Так, Апеляційний орган СОТ постановив, що групи експертів повинні брати до уваги доповіді «друзів суду», у ролі яких часто виступають міжнародні неурядові організації. Можуть виникати суперечності і між самими недержавними акторами. Так, приватний сектор може блокувати прийняття юридично

обов'язкового міжнародного договору, оскільки домінуючим є економічний інтерес. Натомість правозахисні неурядові організації можуть докласти значних зусиль до розробки хоч і необов'язкових, однак детально прописаних актів «м'якого» права. Ще одним аргументом на користь «м'якого» міжнародно-правового регулювання може бути той факт, що на практиці дуже частими є випадки, коли дії держави суттєво розходяться з взятими на себе юридичними зобов'язаннями за міжнародним правом. У такому випадку навіть рамковий документ «м'якого» права буде більш дієвим, ніж міжнародний договір, якщо його правозастосування стане логічним продовженням волі суб'єктів.

Держави, будучи первинними суб'єктами міжнародного права, не позбавлені певних організаційних недоліків. Так, представництво урядів завжди відбувається за участі правлячих партій, які часто керуються власними інтересами при підтримці тих чи інших міжнародно-правових ініціатив. Подекуди вони можуть виходити не з позиції загальнодержавного інтересу, а навпаки просувати формулювання, вигідні для приватного сектору чи окремих політичних груп в обмін на їхню підтримку на виборах. Велика кількість актів «м'якого» права з питань глобального інформаційного суспільства може також бути пояснена тим, що найбільш зацікавлені сторони в особі міжнародних неурядових організацій, приватного сектору, спільнот Інтернет-користувачів не мають міжнародної правосуб'єктності, яка б гарантувала їм право участі у міжнародних договорах. Такі неформальні домовленості не потребують наступної ратифікації та будь-якого додаткового погодження, а тому одразу стають об'єктом прямого правозастосування.

Таким чином, «м'яке» право саме по собі наділене високою нормативною цінністю. Його не слід розглядати лише як можливий етап на шляху до прийняття юридично обов'язкових актів міжнародного права. Як показує проведений аналіз, акти «м'якого» права здатні заповнити правовий вакуум та стати ефективним засобом міжнародно-правового регулювання у тих сферах, де держави не можуть або не хочуть дійти згоди з окремих питань. Новизна концепції глобального інформаційного суспільства потребує певного часу для того, щоб зрозуміти принаймні її ключові складові, характеристики та особливості. Лише у результаті цього стане можливим вироблення юридично обов'язкових міжнародно-правових норм. Отже, незалежно від того, класифікуємо ми міжнародно-правову норму як «м'яку» чи «тверду», вона не перестає бути правовою за своєю

природою. Усе інше – лише додаткові підстави для теоретичних дискусій. На практиці ж має значення лише те, що норми «м'якого» права з питань глобального інформаційного суспільства дотримуються, адже участь у їх розробці беруть ті суб'єкти, чиї права та інтереси такі норми безпосередньо зачіпають та регулюють. Оскільки основним показником ефективності будь-якої правової норми є її правозастосування, то можна говорити про значний прогрес, досягнутий на основі багатостороннього діалогу з питань розвитку глобального інформаційного суспільства. На даному етапі закладені лише основи його функціонування, втім на міжнародному рівні ведеться постійна нормативна робота з розробки чітких принципів та норм у конкретних сферах, а також пошук та розробка ефективних переговорних платформ та контрольних механізмів. Для наочного підтвердження позиції автора щодо високої ефективності додаткових нормативних регуляторів питань розвитку глобального інформаційного суспільства, у наступному підрозділі дисертації наведемо конкретні приклади актів, прийняті як у результаті міждержавного, так і багатостороннього нормотворення.

2.2. Основні міжнародно-правові акти з питань розвитку глобального інформаційного суспільства

Міжнародне право традиційно розглядається як міждержавне право, що має основною метою забезпечення правового порядку. Концепція державного суверенітету вимагала згоди держав на встановлення норм поведінки у міжнародних відносинах. Протягом останніх десятиліть відбулися сутнісні зміни в системі міжнародного права, що поступово перетворюється у глобальне право, яке формується на основі консенсусу та визнає пріоритет правосуддя над правопорядком. Так, виникає форма права, що є реакцією на формування суспільства індивідів, а не держав.

На думку Д. Армстронга, глобалізація сприяла створенню такої економічної, соціальної, політичної та культурної взаємодії, що не може бути оцінена виключно в контексті міждержавних відносин та правових рамок, створених державами, втім вона не замінила ці рамки. Правильним буде говорити про те, що глобалізаційні процеси змінили спосіб поведінки держав шляхом переоцінки того, що означає бути державою на початку

нового тисячоліття. Це, в свою чергу, позначилося на соціальній взаємодії держав, у тому числі, через залучення міжнародної спільноти до формування відповідних норм та видозміні природи таких норм [143].

Першим сигналом для оспорювання виключних нормотворчих повноважень держав стала участь громадських організацій у розробці масиву міжнародно-правових норм у сфері захисту навколишнього середовища. Формування нових галузей економічного та екологічного права відбувалося в умовах визнання нормотворчого потенціалу різноманітних недержавних акторів, включаючи індивідів [144, с. 805].

Інформаційне суспільство в силу свого глобального та інклюзивного характеру спонукає до перегляду традиційних форм міжнародно-правового регулювання. Це пояснюється тим, що окремі аспекти інформаційного суспільства складно врегулювати за допомогою класичного для міжнародного права принципу «зобов'язування - контролю». Сучасні ІКТ розвиваються настільки швидкими темпами, що міжнародне право постійно знаходиться під тиском необхідності наздогнати випереджаючий його технологічний прогрес. У XXI столітті відповідні міжнародні акти повинні прийматися максимально оперативно з тим, щоб залишатися актуальними по відношенню до динамічного об'єкту регулювання, яким у даному випадку виступає глобальне інформаційне суспільство в цілому. Крім того, велика кількість цифрових продуктів та послуг є транскордонними за своїм характером та не обмежуються територією певної держави. Відповідно, виникає потреба у такому ж транскордонному міжнародно-правовому регулюванні та правовиконанні.

Міжнародне інформаційне право впродовж тривалого часу розвивалося з дотриманням принципу технологічної нейтральності та містило доволі загальні формулювання, що створювало ситуації правової невизначеності та відсутності належних гарантій прав та свобод Інтернет-користувачів. Ключовою проблемою, що не давала міжнародному праву стати універсальним регулятором інформаційного суспільства було спотворене сприйняття кіберпростору не як єдиного, цілісного утворення, а, навпаки, як сукупності розрізнених національних сегментів, що по аналогії з фізичним світом функціонують відповідно до національних законів держав. Наслідком такої правової фрагментації є конфлікт юрисдикцій та контролюючих функцій держав, а також надмірна

зарегульованість одних аспектів порівняно з правовим вакуумом у інших сферах функціонування інформаційного суспільства. Поява Інтернету змусила усі галузі міжнародного права пристосовуватися до нових реалій технологічно орієнтованого світу. Кіберпростір є новим середовищем, у якому відсутній наднаціональний суверен, ефективні, універсальні міжнародні договори та спеціалізована судова система [145]. Розбіжності у національно-правових підходах до регулювання правовідносин у кіберпросторі призводять до постійного конфлікту юрисдикцій, що буде наочно продемонстровано при аналізі відповідної судової практики у наступному підрозділі дисертації.

Міжнародне право не може розвиватися відокремлено від розвитку суспільства. Втім, якщо вже можна говорити про певну сформованість глобального інформаційного суспільства, то міжнародне право продовжує відставати від темпів розвитку сучасних ІКТ, що є визначальним чинником розвитку правовідносин у кіберпросторі. Так, ще наприкінці XIX століття суддя О. Холмс здійснив аналіз англо-американського загального права, у результаті якого дійшов висновку про те, що право є відображенням історії розвитку народу впродовж багатьох століть. Він звертається до прикладу деліктного права як підтвердження пристосування галузевих норм до технологічних змін [146]. Втім, Інтернет став тією технологічною інновацією, для якої вже недостатньо простого розширення сфери дії норм існуючих галузей міжнародного права. Так, кіберзлочини виходять за рамки класичного міжнародного кримінального права, хмарні технології потребують відповідних адаптацій авторського права, так само як і захист персональних даних набуває якісно нових характеристик у контексті міжнародного регулювання прав людини. Саме тому постає питання про формування специфічного масиву міжнародно-правових норм в інформаційній сфері та їх оформлення в комплексну галузь міжнародного публічного права – міжнародне інформаційне право.

Тут доречно згадати класифікацію, запропоновану А. Пазюком, який виділяє наступні напрями міжнародно-правового регулювання в інформаційній сфері: а) міжнародно-правове регулювання змісту поширюваної інформації (інформаційний контент), б) міжнародно-правове регулювання інформаційної і комунікаційної діяльності; в) міжнародно-правове регулювання використання обмежених інформаційних ресурсів; г) міжнародно-правове співробітництво з питань інформаційної безпеки; д) міжнародно-

правове регулювання використання інформаційно-комунікаційних технологій в інтересах людства, запобігання та подолання наслідків стихійних явищ тощо [21, с. 76].

При цьому, якщо розглядати глобальне інформаційне суспільство у широкому розумінні як воно запропоноване у авторському визначенні в підрозділі 1.1, тобто як усю повноту правовідносин (правопорядок), що виникають в інформаційній сфері, то за предметною сферою воно охоплює усі напрями міжнародно-правового регулювання в інформаційній сфері, перелічені А. Пазюком. У вузькому розумінні міжнародно-правові питання розвитку глобального інформаційного суспільства можна виділити у якості окремої підгалузі міжнародного інформаційного права, тим самим доповнивши запропоновану вченим класифікацію ще одним напрямом зі специфічним предметом регулювання. Таким чином, з урахуванням положень Женевського Плану дій 2003 року [50] та Доповіді Робочої групи щодо посиленої співпраці Комісії ООН з науки і техніки у цілях розвитку «Окреслення питань міжнародної державної політики щодо Інтернету» 2014 року [147] до питань розвитку глобального інформаційного суспільства, що потребують врегулювання на нормативному рівні, пропонується включати наступні: а) інформаційна та комунікаційна інфраструктура; б) використання ІКТ у цілях розвитку; в) управління Інтернетом; г) інституційні механізми посиленої та багатосторонньої співпраці; ґ) права людини онлайн; д) кібербезпека та відповідальна поведінка держав у кіберпросторі. Наведений перелік не є вичерпним та підлягає постійному перегляду і доповненню з метою приведення його у відповідність з технологічним прогресом та відповідними змінами в інформаційних правовідносинах. Два останні питання розвитку глобального інформаційного суспільства були виділені автором у якості найбільш суспільно важливих та нормативно розроблених, що й спонукало присвятити їм окремий розділ дисертаційного дослідження.

Наразі глобальне інформаційне суспільство перебуває у стані нормативної кризи, що може бути визначена як відсутність регуляторних та правових механізмів, необхідних для врегулювання відносин, опосередкованих використанням Інтернету. Звернемося хоча б до найбільш очевидних випадків нормативної кризи. Так, невирішеним на міжнародно-правовому рівні залишається питання регулювання контенту, правомірності застосування блокуючих та фільтруючих технологій, встановлення політично мотивованих обмежень на

поширення інформації та закріплення відповідних, співрозмірних санкцій. Серйозне занепокоєння викликає захист прав інтелектуальної власності у кіберпросторі. Проблема плагіату та піратства стала ще більш актуальною з появою Інтернету. Завдання міжнародного права полягає у встановленні розумного балансу між законними інтересами правоволоділців щодо створених ними об'єктів інтелектуальної власності та правом кожного на інформацію і доступ до знань.

Розвиток ІКТ змусив по-новому подивитися і на питання захисту приватності у кіберпросторі. Наразі сформувалася стійка тенденція до визнання неминучості технологічного детермінізму, що так чи інакше робить можливим стеження за особою, тим самим обмежуючи рамки її приватності. Складність полягає у тому, що в політичному дискурсі безпека завжди превалює над приватністю. Втім, зростаюча кількість міжнародних скандалів, пов'язаних з масовим стеженням держав, сприяє поступовій переоцінці пріоритетів на користь більш чіткого окреслення меж публічності та приватності, з метою забезпечення належного захисту останньої.

С. Бремен наводить цікавий приклад для ілюстрації того, наскільки інформаційні кордони держави є ширшими, ніж її фізичні, територіальні кордони. Так, дослідниця зазначає, що уряд США запитує персональні дані пасажирів авіарейсів ще до того, як ті покинуть аеропорти на території ЄС. І це при тому, що в рамках ЄС праву на приватність надається доволі високий рівень захисту. Автор звертає увагу на факт розмиття чітких та сталих меж між приватністю та публічністю, державою та світовою системою, що має наслідком не просто нормативну плутанину, а спричиняє нормативну кризу [148].

Серйозне занепокоєння викликає також питання боротьби з дитячою порнографією онлайн. Невизначеними залишаються міжнародні-правові рамки ведення бізнесу в Інтернеті, зокрема використання електронних розрахунків, банкінгу, здійснення комерційних транзакцій з цифровою інформацією та застосування електронного підпису [149, с. 317]. Крім того, нового звучання набуло питання соціальної нерівності у кіберпросторі. Зростання цифрового розриву між технологічно розвинутими країнами та країнами третього світу є серйозною перешкодою на шляху забезпечення рівних прав людини та громадянина в глобальному інформаційному суспільстві. Основним вигодоотримувачем від нормативної кризи міжнародного права є існуючий економічний та

політичний порядок. Швидкий технологічний розвиток поставив під питання ефективність та регуляторну спроможність діючих міжнародно-правових механізмів.

Згідно з Марсденом, лише зі зростанням присутності бізнесу та користувачів в Інтернеті питання визначення нормативних цінностей інформаційного суспільства набуло своєї політичної ваги [150, с. 32].

А. Чендер, у свою чергу, зауважує, що глобальний Інтернет чинить тиск на міжнародне право через виникнення зростаючої кількості правових колізій. У якості прикладу автор наводить спір між Антигуа та США щодо заборони азартних ігор онлайн, розглянутий у рамках процедури вирішення спорів СОТ; вимоги Бразилії до компанії *Google* щодо встановлення осіб, винних у розпалюванні мови ворожнечі; судовий процес у США у контексті застосування Статуту про делікти іноземців щодо притягнення до відповідальності компанії *Yahoo!* за підбурювання до тортур у Китаї; скаргу США проти Китаю в рамках Органу з вирішення спорів СОТ щодо контролю державних медіа над іноземними фільмами, фінансовою інформацією та музикою, зокрема *iTunes*. Наведені приклади є свідченням правової невизначеності з питань кіберторгівлі: від юрисдикції та протекціонізму до захисту прав споживачів та прав людини в цілому [151].

Втім, не всі експерти у сфері міжнародного права і не завжди погоджувалися з необхідністю вироблення окремого комплексу міжнародно-правових норм у сфері кіберпростору. Так, у 1996 році Ф. Істербрук стверджував про відсутність розумної необхідності у гармонізації процесуальних та матеріальних аспектів Інтернет-права, зазначаючи, що останнє є всього-на-всього прикладом поодинокого застосування існуючих правових норм до правовідносин з використанням нових технологій. Для більшої наочності абсурдності ідеї виокремлення Інтернет-права у якості окремої галузі права він порівнював останнє з конячим правом [152].

Подібні ідеї відстоював також Дж. Соммер, який заперечував існування кіберправа як самостійної галузі та вважав, що технології не можуть бути визначальним чинником розвитку права. Крім того, він зазначав, що більшість правових питань, пов'язаних з Інтернетом, не є новими, а чинні правові норми з часом пристосуються до технологічних особливостей. Вчений був переконаний не лише в ілюзорності існування кіберправа, але й вважав шкідливою саму ідею про його існування [153].

Натомість представник київської школи міжнародного права А. Пазюк стверджує, що участь у правовідносинах з управління Інтернетом як суб'єктів міжнародного приватного, так і суб'єктів міжнародного публічного права дозволяє припустити факт формування транснаціонального кіберправа (міжнародного права Інтернету), основу якого складуть правові норми, розроблені й прийняті в ході багатостороннього співробітництва за участю всіх зацікавлених сторін у форматі всесвітніх форумів [21, с. 216]. Крім того, вчений розрізняє трансформацію міжнародного інформаційного права *de lege lata* та формування автономного міжнародно-правового режиму Інтернету – міжнародного (транснаціонального) кіберправа *de lege ferenda* [21, с. 209].

У кіберпросторі відсутнє єдине суверенне джерело управління. Інтернет існує та функціонує як результат незалежної домовленості тисяч окремих операторів комп'ютерів та комп'ютерних мереж використовувати спільні протоколи передачі даних для обміну комунікаціями та інформацією з іншими комп'ютерами, які, у свою чергу, продовжують цей ланцюжок. Не існує жодного централізованого місця для зберігання даних, єдиного контролюючого органу чи комунікаційного каналу в Інтернеті. З технічної точки зору існування єдиної інституції, відповідальної за контроль усіх потоків інформації в Інтернеті, є абсолютно неможливим [154].

Й. Бенклер запропонував три рівні системи управління Інтернетом, зокрема рівень фізичної інфраструктури, логічної інфраструктури та контенту. При цьому регуляторний вибір здійснюється на кожному з цих рівнів інформаційного середовища. Так, рішення приймаються щодо права інтелектуальної власності, що може зумовити перерозподіл прав власності на контент, а також щодо дизайну програмного забезпечення, його стандартів та регулювання фізичної інфраструктури для здійснення Інтернет-комунікацій. На усіх згаданих рівнях помилкові рішення можуть призвести до відтворення моделі мас-медіа з перенесенням усіх недоліків у цифрове мережеве середовище [155].

Жодна держава не має суверенітету над усіма трьома рівнями системи управління Інтернетом, особливо щодо правовідносин, що відбуваються поза межами її території. Відмінне глобальне правове регулювання формується навколо питань, пов'язаних з Інтернетом. Подібно до права міжнародної торгівлі та міжнародного права навколишнього середовища управління Інтернетом викликало суттєві розбіжності між державами, а також

спричинило інтерес приватного сектору та громадянського суспільства до участі у глобальних процесах управління [156].

Ще у середині 90-х років Д. Джонсон та Д. Пост писали про те, що нові норми з'являтимуться у відповідь на появу широкого спектру нових феноменів, чітких аналогів яким немає у реальному світі. Такі нові правила відіграватимуть роль права, визначаючи правосуб'єктність та власність, способи та порядок вирішення спорів, а також ключові цінності поведінки суб'єктів онлайн. Вже тоді, на етапі зародження Інтернету, вони говорили про те, що визнання існування юридично значимого кордону між кіберпростором та реальним світом дозволить вирішити більшість юрисдикційних та правових труднощів, пов'язаних з транскордонними електронними комунікаціями. Такий підхід змінить підхід до розуміння права як системи норм, заснованої на географічних кордонах держав [20].

Ключовою проблемою відсутності універсального міжнародно-правового регулювання Інтернету є той факт, що глобальний за своєю природою феномен є об'єктом регулювання численних національних законів, що часто вступають у конфлікт між собою. Інша складність полягає у тому, що державам не вдалося виробити збалансований підхід до регулювання правовідносин, опосередкованих використанням Інтернету. Вимоги національних законів виявляються або занадто обтяжливими для суб'єктів правовідносин онлайн, або занадто нечіткими, тим самим позбавляючи таких суб'єктів належних гарантій захисту їх прав та законних інтересів.

Глобальним компаніям, таким як *Google, Yahoo!, Microsoft*, кожного разу при виведенні своїх послуг на новий ринок доводиться докладати величезних зусиль для того, щоб їх діяльність відповідала вимогам національних законодавств. Відсутність універсального режиму кіберпростору зумовлює ріст транзакційних витрат та збільшення кількості судових проваджень проти Інтернет-компаній. Яскравим прикладом того, наскільки різними можуть підходи до регулювання правовідносин в онлайн середовищі, є США та ЄС. Незважаючи на те, що усі великі Інтернет-компанії зареєстровані в Америці, їм доводиться керуватися у своїй діяльності законодавством ЄС при наданні відповідних послуг на території держав-членів ЄС. Фактично, маємо ситуацію, коли право ЄС поширює свою дію поза межі своїх територіальних кордонів.

Далі наведемо аналіз найбільш значимих міжнародно-правових актів з питань

глобального інформаційного суспільства, прийнятих в рамках універсальних та регіональних міжнародних організацій та об'єднань. Так, одним з найбільш прогресивних документів ООН в інформаційній сфері вважається *Конвенція Тампере про надання телекомунікаційних ресурсів для пом'якшення наслідків лих та здійснення операцій щодо надання допомоги 1998 року*, яка вступила в силу лише у січні 2005 року [157]. Конвенція є першою міжнародною угодою, що встановлює правові рамки використання телекомунікацій у цілях надання гуманітарної допомоги, послаблює регуляторні бар'єри, повністю охороняє інтереси держав, що запитують та надають допомогу (при цьому за державами залишається право здійснювати контроль за ходом надання такої допомоги на їх території), передбачає укладення двосторонніх договорів між провайдерами послуг та державами, що запитують або надають допомогу. У статті 1 документу міститься перелік термінів, що зустрічаються у тексті Конвенції. Найбільший інтерес представляють поняття неурядової організації та неурядового утворення, оскільки Конвенція є першою угодою такого типу, що поширює привілеї та імунітети на їх персонал. Особливо важливе значення має стаття 9, що передбачає зниження або скасування регламентаційних бар'єрів на шляху використання телекомунікаційних ресурсів для пом'якшення наслідків лих та полегшення ситуації, у тому числі шляхом надання телекомунікаційної допомоги. Це пояснюється тим, що до моменту прийняття конвенції транскордонне використання гуманітарними організаціями телекомунікаційного обладнання часто ускладнювалося регуляторними бар'єрами, що значно затягували процес імпорту та оперативного розміщення телекомунікаційного обладнання для ліквідації надзвичайних ситуація, якщо попередньо не було отримано згоду місцевих органів влади. При цьому під бар'єрами розуміються ліцензійні вимоги щодо використання визначених частот, обмеження на імпорт телекомунікаційного обладнання та рух гуманітарних груп. Угода значно спрощує використання телекомунікаційного обладнання, необхідного для спасання людського життя. Дана конвенція продемонструвала, що роль ІКТ в епоху глобалізації не зводиться виключно до інформування та полегшення комунікації, натомість технологічні досягнення можуть бути використанні для надання гуманітарної допомоги з метою подолання наслідків стихійних катастроф та спасання людського життя. Така допомога є вкрай критичною, враховуючи, що власні телекомунікаційні пристрої та мережі держави, що

постраждала від катастрофи, як правило, виводяться з ладу.

Конвенція ООН з прав дитини 1989 року забороняє будь-які форми сексуальної експлуатації дітей. І, хоча, у документі не міститься визначення дитячої порнографії та немає положень, які б напряму стосувалися поширення дитячої порнографії в Інтернеті, цілком доцільним видається розширене тлумачення статті 34 Конвенції щодо заборони використання дітей у зйомках порнографічних матеріалів [158]. Логічно припустити, що якщо на конвенційному рівні незаконним визнається сам факт експлуатації дітей з метою створення матеріалів порнографічного характеру, так само незаконним буде поширення подібних матеріалів, незалежно від засобів їх розповсюдження. Натомість у преамбулі *Факультативного протоколу до Конвенції про захист прав дитини щодо торгівлі дітьми, дитячої проституції та дитячої порнографії 2000 року* згадується зростання доступності дитячої порнографії в Інтернеті та в рамках інших технологій, а також наголошується на важливості більш тісної співпраці та партнерства між урядами та індустрією Інтернету щодо виробництва, поширення, експорту, передачі, імпорту, навмисного зберігання дитячої порнографії та її реклами. При цьому згідно з Протоком дитячою порнографією є зображення будь-якими засобами дитини, що здійснює реальні або змодельовані відверто сексуальні дії, або будь-яке зображення статевих органів дитини, головним чином, в сексуальних цілях [159]. Логічно припустити, що під будь-якими засобами цілком обґрунтовано розуміти також Інтернет.

Дещо більшу конкретику можна знайти в *Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насилля 2007 року*, відому також як Лансаротська конвенція. Підпункт f) пункту 1 статті 20 Конвенції зобов'язує держави-члени вжити необхідні законодавчі та інші заходи з метою встановлення кримінальної відповідальності за, зокрема, умисне отримання доступу до дитячої порнографії за допомогою ІКТ. Втім, держави можуть залишити за собою право не застосовувати повністю або частково саме цей підпункт. Нововведенням стало визнання кримінально караною будь-якої умисної пропозиції про зустріч, з якою дорослий за допомогою ІКТ звертається до дитини, що не досягла віку, з якого відповідно до законодавства держави-члена їй дозволяється вступати у сексуальні відносини, з метою вступити з такою дитиною у сексуальні відносини або використати її у цілях виробництва дитячої порнографії, за

умови, що за такою пропозицією послідували практичні дії, спрямовані на проведення такої зустрічі [160]. Таке явище ще називається грумінгом та набуває все більшої популярності в Інтернеті. Фактично, жоден інший міжнародно-правовий документ не містить положень щодо криміналізації грумінгу. Дана конвенція є особливо актуальною в контексті зростання сексуальної експлуатації та сексуального насилля над дітьми як на національному, так і на міжнародному рівнях, зокрема щодо зростаючої присутності дітей в Інтернеті та недобросовісного використання правопорушниками можливостей ІКТ. Революційним аспектом конвенції є включення до її тексту положень, що стосуються таких нових форм насилля як експлуатація дітей з використанням нових ІКТ. Фактично конвенція посилює захист дітей від неправомірного використання ІКТ зловмисниками.

У 2011 році ЄС затвердив *Директиву про боротьбу з сексуальним насиллям та експлуатацією дітей, а також дитячою порнографією*. Фактично це був перший акт ЄС у сфері кібербезпеки. У документі зазначається, що сексуальне домагання дітей є загрозою, що має специфічні характеристики у контексті Інтернету, оскільки останній відкриває невідомі раніше можливості для збереження анонімності користувачів, приховування реальної ідентичності та особистих характеристик, таких як вік особи. Передбачається вилучення дитячої порнографії з серверів, а там, де це неможливо, запровадження альтернативних механізмів блокування доступу з території ЄС до веб-сайтів, що містять чи поширюють дитячу порнографію. Крім того, у Директиві згадується, що в рамках програми «За безпечний Інтернет» було створено мережу гарячих ліній, що покликані збирати інформацію та обмінюватися звітами щодо основних типів незаконного контенту онлайн. Передбачається також вжиття попереджувальних заходів. Так, на держави-члени покладається зобов'язання вживати відповідні заходи, у тому числі через Інтернет, такі як підвищення обізнаності, дослідницькі та наукові програми, а там, де це необхідно, вступати у співпрацю з відповідними неурядовими організаціями та іншими зацікавленими сторонами з метою підвищення обізнаності та зменшення ризику того, що діти стануть жертвами сексуального насилля чи експлуатації. Крім того, у Директиві наголошується на тому, що свідоме, з використанням ІКТ отримання доступу до дитячої порнографії повинне бути криміналізоване [161]. Такий підхід має особливо важливе значення для правоохоронних органів, коли очевидним є факт відкриття злочинцем веб-сайту з дитячою

порнографією, втім немає доказів скачування ним відповідних матеріалів. При цьому, слід мати на увазі, що скачування порнографічних матеріалів не завжди має місце, а тому визнання самого факту перегляду самостійним злочином є цілком обґрунтованим. Директива відіграє важливе значення у зв'язку з тим, що сексуальна експлуатація дітей зросла з появою та розвитком ІКТ, зокрема через використання соціальних мереж та чат-сервісів.

У 2003 році ЮНЕСКО ухвалила *Рекомендацію про розвиток і використання багатомовності та загальний доступ до кіберпростору*, що передбачає вжиття необхідних зусиль для зменшення мовних бар'єрів та активізації інтерактивного спілкування в Інтернеті шляхом розробки відповідного контенту усіма мовами світу, у тому числі мовами корінного населення. Крім того, визнається загальність доступу до Інтернету як інструменту сприяння реалізації прав людини. Інтернет-користувачам повинен бути гарантований доступ до інформації, що є суспільним надбанням. Наголошується на необхідності співпраці держав з усіма зацікавленими сторонами з питань збалансування інтересів власників авторських прав та суспільства щодо доступу до об'єктів авторських прав з використанням кіберпростору [16].

Одночасно з Рекомендацією була прийнята Хартія про збереження цифрового надбання, відповідно до якої цифрове надбання охоплює унікальні ресурси людських знань та форм вираження. Документ регулює питання доступу до цифрового надбання та попередження його втрати, а також збереження культурного надбання усіх народів, держав та культур [162].

Одним з прогресивних документів Ради Європи в інформаційній сфері можна також вважати *Конвенцію про інформаційне та правове співробітництво щодо «послуг інформаційного суспільства» 2001 року*, відповідно до якої сторони обмінюються текстами проектів внутрішніх норм щодо «послуг інформаційного суспільства» та співпрацюють у сфері правового сприяння та функціонування інформаційної системи, створення якої передбачається нормами цієї Конвенції. При цьому під «послугами інформаційного суспільства» розуміються будь-які послуги, що зазвичай надаються за винагороду на відстані через використання електронних засобів та на індивідуальну вимогу отримувача таких послуг [163].

У квітні 2015 року Рада Європи ухвалила *Рекомендацію щодо вільного, транскордонного потоку інформації в Інтернеті*, спрямовану на захист та сприяння вільному руху інформації в онлайновому середовищі та гарантування того, що блокування контенту є сумісним зі стандартами захисту прав людини та не становить втручання у міжнародний Інтернет-трафік [164].

Розбудова вільного, відкритого та безпечного Інтернету була визнана основним пріоритетом *Стратегії з управління Інтернетом*, розробленої Радою Європи на період з 2012 по 2015 роки. Нова стратегія розрахована на 2016-2019 рр. Ключова ціль документу зводиться до забезпечення формування людиноцентричної публічної політики з питань Інтернету, захисту прав Інтернет-користувачів, а також гарантування поваги та захисту прав людини онлайн. Зокрема, стратегія містить перелік конкретних заходів, спрямованих на захист свободи вираження поглядів, приватності та безпеки Інтернет-користувачів, а також їх залучення до багатостороннього діалогу з питань управління Інтернетом [165].

У 1999 році в рамках ЄС було затверджено *План дій щодо зміцнення безпечного використання Інтернету шляхом боротьби з незаконним та шкідливим контентом у глобальних мережах*. План дій було розроблено спільними зусиллями урядів держав-членів, користувачів та Інтернет-індустрії. Документ спрямований на заохочення ефективних моделей саморегулювання, попередження та повідомлення батьків і вчителів, посилення співпраці та обміну досвідом і кращими практиками, покращення координації в межах Європи, забезпечення відповідності між підходами, що діють в ЄС та поза його межами. План дій містить чотири ключові напрямки діяльності, зокрема створення безпечного середовища (шляхом саморегулювання Інтернет-індустрії), розробка систем фільтрування та рейтингування, вжиття заходів щодо підвищення обізнаності, координація та оцінка досягнутих результатів [166]. Показовим є те, що вже наприкінці 1990-х років саморегулювання було визнане у якості ефективного засобу протидії незаконному та шкідливому контенту онлайн.

Згодом послідувало прийняття у 1999 році ініціативи *«Електронна Європа – інформаційне суспільство для всіх»*, що повинна була забезпечити максимальне використання переваг інформаційного суспільства в межах ЄС. На виконання ініціативи було прийнято кілька планів дій щодо побудови електронної Європи. Кінцева мета

документа полягала у залученні всіх і кожного до цифрового суспільства та онлайн середовища. Для досягнення цілей ініціативи пріоритетними завданнями для ЄС залишатимуться створення ефективної правової бази щодо комунікаційних послуг, електронної торгівлі тощо. Документ охоплює питання забезпечення широкосмугового доступу, кібербезпеки, електронної інклюзивності, електронного уряду, електронного навчання, електронної медицини, електронного бізнесу [167].

У 2010 році Європейська Комісія ввела в дію *«Цифровий порядок денний для Європи»*, що є одним із семи стовпів Стратегії Європа-2020, яка окреслює напрямки розвитку ЄС на період до 2020 року. Основною метою Цифрового порядку денного є формування єдиного цифрового ринку. Крім того, передбачається діяльність щодо покращення взаємодії та стандартів, зміцнення довіри та безпеки онлайн, забезпечення швидкісного та надшвидкісного доступу до Інтернету для всіх, інвестиції у дослідження та інновації, розвиток цифрової грамотності, навичок та інклюзивності, а також використання переваг ІКТ для забезпечення сталого розвитку європейського суспільства [168]. Фактично, Порядок денний став продовженням, започаткованої у 2005 році ініціативи і2010 – Європейське інформаційне суспільство для росту та зайнятості (2005-2010). Для того, щоб Україна могла стати повноправним членом європейського інформаційного простору, адаптація національного законодавства до Цифрового порядку денного повинно бути визнано одним зі стратегічних пріоритетів нашої держави.

У рамках СНД одним з перших документів в інформаційній сфері стала *Угода про співпрацю у сфері інформації 1992 року*. Далі у 1996 році була затверджена *Концепція інформаційного простору СНД*. Так, під інформаційним простором розуміється сукупність національних інформаційних просторів держав-учасниць СНД, що взаємодіють на основі відповідних міждержавних договорів щодо узгоджених сфер діяльності. Концепція спрямована на посилення співпраці держав щодо розвитку міждержавних інформаційних обмінів. У документі зазначається, що процес розвитку держав-учасниць СНД не є лінійним, а тому швидкість входження кожної з держав до світового інформаційного простору теж може відрізнятися. Йдеться про необхідність розвитку нормативно-правової бази в інформаційній сфері, зокрема прийняття міждержавних документів про транскордонне розповсюдження інформаційної продукції. При цьому повинне

дотримуватися право суверенних держав на незалежне формування власного інформаційного простору, а також повинен забезпечуватися достатній рівень інформаційної безпеки. Основними напрямками розвитку національних законодавств визнаються: регулювання відносин власності на інформацію, інформаційні ресурси, інформаційні структури і технології; регулювання доступу до інформації; забезпечення безпеки функціонування інформаційних та телекомунікаційних систем, захист авторських прав суб'єктів на основі міжнародного права. Було також виділено два етапи формування та розвитку інформаційного простору СНД: 1996-1997 та 1998-2000 рр. [169]. У цілому, Концепція містить доволі загальні формулювання та не визначає в чому саме полягає специфіка інформаційного обміну між державами-учасницями СНД.

У 2012 році держави-члени АТЕС підписали *Санкт-Петербурзьку декларацію «Забезпечення довіри та безпеки у використанні ІКТ для сприяння економічному росту та процвітанню»*, якою визнається необхідність співпраці в регіоні з метою забезпечення цілісності та відказостійкості мереж і вжиття заходів для посилення безпеки ІКТ. Розвиток інклюзивного мережевого суспільства визнається необхідною передумовою отримання соціально-економічних переваг. При цьому зазначається, що Азійсько-Тихоокеанське інформаційне суспільство знаходиться у стані розвитку. У документі послідовно знаходять своє відображення питання розвитку ІКТ, що сприяють новому росту; посилення соціально-економічних заходів за допомогою ІКТ, створення мережі довіри та безпеки ІКТ; сприяння регіональній та економічній інтеграції; зміцнення співпраці у сфері ІКТ [170]. Положення декларації також не відзначаються своєю деталізованістю та окреслюють лише загальні рамки розвитку співробітництва в інформаційній сфері.

У рамках «Групи восьми» (G-8) було прийнято один з основоположних документів у сфері розвитку глобального інформаційного суспільства – *Окінавську хартію глобального інформаційного суспільства 2000 року*. Фактично Хартія стала першим міжнародно-правовим документом, що визначив основи взаємодії зацікавлених суб'єктів у сфері формування глобального інформаційного суспільства. Положення Хартії перекликалися з цілями розвитку тисячоліття ООН. Документ структурно складається з чотирьох частин, присвячених відповідно використанню можливостей цифрових технологій, подоланню цифрового розриву, розвитку глобальних можливостей та подальшому розвитку. Хартія не

містить визначення глобального інформаційного суспільства. Визнається життєво важлива роль приватного сектору у розробці інформаційних та комунікаційних мереж, однак створення передбачуваної, транспарентної та недискримінаційної політики і нормативної бази у сфері інформаційного суспільства залишається прерогативою держав. Захист приватності та персональних даних не повинен перешкоджати вільному потоку інформації. Зусилля міжнародного співтовариства повинні бути спрямовані на забезпечення безпечного та вільного від злочинності кіберпростору. Стратегія розвитку інформаційного суспільства повинна супроводжуватися розвитком людських ресурсів, можливості яких відповідали б вимогам інформаційної ери. Йдеться також про неможливість прийняття універсальної стратегії глобального інформаційного суспільства з огляду на різноманітність умов та потреб, що склалися в країнах, що розвиваються. При цьому заохочуються власні ініціативи таких країн щодо прийняття послідовних національних програм та створення належної нормативної бази. Підкреслюється важливість міжнародної співпраці між усіма зацікавленими сторонами як на двосторонньому, так і на багатосторонньому рівнях. Була також створена Група з можливостей інформаційних технологій (*DOT Force*), на яку покладися завдання щодо активного сприяння діалогу з країнами, що розвиваються, міжнародними організаціями та іншими зацікавленими сторонами для просування міжнародної співпраці з метою формування політичного, нормативного та мережевого забезпечення тощо [34].

Питання Інтернету знову стали предметом серйозного обговорення на саміті «Групи восьми» у 2011 році та були відображені у розділі другому підсумкового документа – *Довільської декларації «Незмінна відданість свободі та демократії»*. У преамбулі зазначається, що вперше на рівні глав держав вдалося погодити ряд ключових принципів, у тому числі щодо свободи, поваги приватності та інтелектуальної власності, багатостороннього управління, кібербезпеки та захисту від злочинності, що повинні лягти в основу розвитку Інтернету. Цікавим є поєднання в тексті документу доволі суперечливих принципів розвитку Інтернету. Так, з одного боку визнаються принципи відкритості, транспарентності та свободи Інтернету, а з іншого – заново підтверджується зобов'язання вживати ефективні дії щодо боротьби з порушеннями прав інтелектуальної власності у сфері цифрових технологій у даний час і в майбутньому. Таким чином, захист прав

інтелектуальної власності виявляється більш пріоритетним порівняно з іншими правами людини, такими як, наприклад, свобода вираження поглядів. У той же час, довільна та невибіркова цензура і обмеження доступу до Інтернету були визнані такими, що суперечать міжнародним зобов'язанням держав, у зв'язку з чим є абсолютно неприпустимими. Окремим пунктом закріплено обов'язок вжиття необхідних зусиль для попередження використання ІКТ у терористичних та кримінальних цілях, а також посилення міжнародної співпраці щодо захисту критично важливих ресурсів, ІКТ та інших об'єктів інфраструктури. За урядами закріплюється обов'язок співпраці з усіма іншими зацікавленими сторонами щодо розробки норм поведінки у кіберпросторі та спільних підходів до його використання. Позитивним моментом є визнання багатосторонньої моделі управління Інтернетом, однак ключова роль залишається за державами [171].

У листопаді 2015 року під час саміту в Анталії лідери держав-членів Великої двадцятки (G-20) схвалили комюніке, яким, серед іншого, затвердили ряд положень щодо кіберпростору, що відображені в останньому пункті документу. Так, держави взяли на себе зобов'язання щодо скорочення цифрового розриву та визнали особливу відповідальність щодо забезпечення безпеки і стабільності у кіберпросторі. З цією метою було встановлено заборону вчинення чи підтримки крадіжок інтелектуальної власності з використанням ІКТ, у тому числі торговельних секретів чи будь-якої іншої конфіденційної бізнес-інформації, з метою надання компаніям конкурентних переваг. При цьому держави повинні забезпечувати повагу приватності та захист від незаконного та свавільного втручання у сферу приватності, включаючи контекст цифрових комунікацій. Крім того, Велика двадцятка високо оцінила нормативну діяльність ООН у сфері кібербезпеки та схвалила доповідь Групи урядових експертів щодо досягнень у сфері інформації та комунікацій у контексті міжнародної безпеки за 2015 рік, тим самим визнавши, що міжнародне право і, зокрема, Статут ООН застосовуються до поведінки держав у кіберпросторі. Держави-члени також визнали себе зобов'язаними дотримуватися норм щодо відповідальної поведінки держав у кіберпросторі згідно з Резолюцією ООН A/C.1/70/L.45 [172]. Дане комюніке хоч і не має юридично обов'язкової сили, втім є позитивним прикладом досягнення консенсусу державами з таких критичних питань в кіберпросторі, як кібербезпека та відповідальна поведінка держав.

У *Комюніке ОЕСР щодо принципів розробки Інтернет-політики від 2011 року* закріплені основні принципи, що повинні сприяти збереженню відкритості Інтернету з одночасним захистом приватності, безпеки, дітей онлайн, інтелектуальної власності та відновленням довіри до Інтернету. Дані принципи розроблені з урахуванням унікальних соціальних, технічних та економічних характеристик Інтернет-середовища. Відкритий та доступний Інтернет визнається передумовою дотримання свободи вираження поглядів та законного обміну інформацією, знаннями і поглядами. Принципи були розроблені за участі представників урядів, приватного сектору і громадянського суспільства та зводяться до наступного: захист глобального, вільного потоку інформації; зміцнення відкритої, розподіленої та взаємопов'язаної природи Інтернету; заохочення інвестицій та конкуренції у сфері високошвидкісних мереж та послуг; сприяння розвитку транскордонних послуг; забезпечення багатосторонньої участі у процесах прийняття рішень; заохочення ініціативи щодо розробки кодексів поведінки; захист приватності; обмеження відповідальності посередників тощо [173].

В одній із доповідей щодо оцінки діяльності ВОІВ у сфері електронної торгівлі зазначається, що хоча представники урядів, експерти з питань інтелектуальної власності та інші зацікавлені сторони досягли згоди щодо того, що електронна торгівля, Інтернет та інші засоби здійснення транскордонних транзакцій спричинили появу нових викликів режиму захисту інтелектуальної власності, досі не вдалося дійти консенсусу щодо того, як саме повинні бути врегульовані дані питання [174]. У 2001 році ВОІВ оприлюднила *Спільну рекомендацію щодо положень про захист знаків та інших прав промислової власності на позначення в Інтернеті* [175], що певним чином гармонізує спроби тлумачення чинного матеріального права, не зачіпаючи при цьому питання юрисдикції та застосовного права. І, хоча, документ обійшов стороною найбільш дискусійні питання та пройшов детальне обговорення, втім далеко не всі положення зрештою були прийняті абсолютним консенсусом.

У *Декларації Монтре «Про захист персональних даних у глобальному світі: універсальне право, що поважає багатоманітність» від 2005 року*, ухваленій Асамблеєю уповноважених з питань захисту даних та приватності, міститься заклик до ООН щодо розробки юридично обов'язкового документу, що чітко закріплює право на захист

персональних даних та приватності. Крім того, у тексті документу згадуються також міжнародні та наднаціональні організації, організації громадянського суспільства, виробники обладнання та програмного забезпечення, що у своїй діяльності повинні дотримуватися та розвивати принцип захисту приватності та персональних даних, а також розробити відповідні контрольні механізми [176].

Підсумковим документом сьомого саміту країн-членів БРІКС стало підписання *Уфімської декларації* у липні 2015 року. У документі визнається неприпустимість використання ІКТ та Інтернету у спосіб або з метою порушення прав людини та фундаментальних свобод, включаючи право на приватність. Закріплюється однаковий режим захисту прав людини офлайн та онлайн. Підтверджується відданість принципам відкритості, нефрагментованості та безпеки Інтернету, а також залучення зацікавлених сторін до вирішення питань розвитку, участі у функціонуванні Інтернету та підтриманні його безпеки. У той же час, ключова роль у розробці міжнародної політики з питань Інтернету, а також розробки відповідної універсальної угоди щодо боротьби з кіберзлочинністю повинна належати ООН. У Декларації також засуджується масове електронне стеження та збирання даних індивідів, що визнаються порушенням суверенітету держав та прав людини, зокрема права на приватність [177]. Втім, позиції держав щодо кібербезпеки та суверенітету у кіберпросторі в межах самої БРІКС не є настільки вже однозначними. Росія та Китай традиційно дотримуються державоцентричного підходу, у той час як Індія, Бразилія та Південна Африка переконані у перспективності багатостороннього підходу до управління Інтернетом. Наразі державам вдається зберігати відносну єдність, однак у тих випадках, коли держави виступають у самостійній ролі, стає помітним розходження з принципових питаннях. Так, Індія відмовилася підписувати переглянутий Регламент МСЕ, тим самим не визнавши керівної ролі держав у процесах регулювання кіберпростору.

У жовтні 2015 року Міжпарламентський союз (*Inter-Parliamentary Union*) одноголосно ухвалив *резолюцію «Демократія у цифрову еру і загроза приватності та індивідуальним свободам»*, у якій міститься заклик до парламентів країн-учасниць долучитися до розробки та імплементації загальної стратегії розвитку Інтернету на користь всього людства. Державам пропонується зняти усі правові обмеження щодо свободи

вираження поглядів та не перешкоджати вільному руху інформації, а також дотримуватися принципу мережевої нейтральності. Крім того, повинна бути приведена у відповідність з міжнародним правом та гармонізована практика держав щодо захисту приватності. Згадується необхідність консультування з усіма зацікавленими сторонами у процесі прийняття рішень [178]. Загалом, документ відображає прогресивні ідеї розвитку кіберпростору та закріплює загальні рамки співпраці держав щодо широкого кола питань розвитку інформаційного суспільства.

На основі проведеного аналізу нормативно-правових актів з питань розвитку глобального інформаційного суспільства автором пропонується їх класифікація за предметною сферою дії. Групування регуляторних актів у досліджуваній сфері покликане полегшити їх використання у правозастосовній діяльності. Так, першу групу становлять акти, спрямовані на регулювання глобального інформаційного суспільства як самостійного феномену (Окінавська хартія глобального інформаційного суспільства, Конвенція РЄ про інформаційне та правове співробітництво щодо «послуг інформаційного суспільства», Ініціатива «Електронна Європа – інформаційне суспільство для всіх»). Другу групу формують міжнародно-правові акти з питань кіберпростору (Рекомендація ЮНЕСКО про розвиток і використання багатомовності та загальний доступ до кіберпростору, Хартія про збереження цифрового надбання, Концепція інформаційного простору та Угода про співпрацю у сфері інформації СНД, Комюніке Великої двадцятки за результатами саміту в Анталії, Декларація Монтре «Про захист персональних даних у глобальному світі: універсальне право, що поважає багатоманітність», Уфімська декларація країн-членів БРІКС, Довільська декларація «Групи восьми» «Незмінна відданість свободі та демократії» тощо). Міжнародно-правові акти, що увійшли до третьої групи, сфокусовані на питаннях управління та функціонування Інтернету (Рекомендація РЄ щодо вільного, транскордонного потоку інформації в Інтернеті, Стратегія РЄ з управління Інтернетом, План дій ЄС щодо зміцнення безпечного використання Інтернету шляхом боротьби з незаконним та шкідливим контентом у глобальних мережах, «Цифровий порядок денний для Європи», Комюніке ОЕСР щодо принципів розробки Інтернет-політики). Класифікуючою ознакою наступної категорії є заборона сексуальної експлуатації дітей та дитячої порнографії (Конвенція ООН з прав дитини та Факультативний протокол до неї від

2000 р., Лансаротська конвенція, Директива ЄС про боротьбу з сексуальним насиллям та експлуатацією дітей, а також дитячою порнографією). Окрему групу становлять також міжнародно-правові акти щодо використання ІКТ у цілях розвитку людства (Конвенція Тампере, Санкт-Петербурзька декларація держав-членів АТЕС «Забезпечення довіри та безпеки у використанні ІКТ для сприяння економічному росту та процвітанню»). Самостійний предмет міжнародно-правового регулювання становлять також питання інтелектуальної власності (Спільна рекомендація ВОІВ щодо положень про захист знаків та інших прав промислової власності на позначення в Інтернет).

У серпні 2015 року Спеціальний доповідач ООН з питань приватності Дж. Каннатачі заявив про необхідність розробки Женевської конвенції з питань Інтернету, спрямованої на захист персональних даних та попередження загрози масового стеження з використанням цифрових технологій [179]. Текст подібної міжнародної угоди під назвою *«Міжнародний договір про право на приватність, захист від неналежного стеження та захист інформаторів»*, відомої також як «Угода Сноудена», був запропонований групою активістів на чолі з Едвардом Сноуденом. Наразі доступним в мережі є лише короткий огляд угоди [180]. Думки міжнародної спільноти розділилися. Так, Д. Фідлер ставить під сумнів необхідність ухвалення ще однієї міжнародної угоди, що заново підтвердить загальновизнане право на приватність та незаконність здійснення масового стеження. Він вказує на відсутність логічних підстав вважати, що держави, які не дотримуються чинних міжнародно-правових актів, погодяться зобов'язати себе додатковими обмеженнями у випадку прийняття цієї угоди. На думку автора, в угоді можуть бути запропоновані нові, більш жорсткі механізми контролю та захисту. Втім, знову ж таки, чи потрібно для цього ухвалювати окрему угоду, якщо держави можуть домовитися щодо такого механізму в рамках існуючих міжнародно-правових актів. У той же час, досить проаналізувати міжнародні договори у сфері захисту прав людини та передбачені ними контрольні механізми, щоб зрозуміти що держави завжди прагнули уникнути надмірного обмеження своїх владних повноважень [181].

М. Мілановіч стверджує, що затвердження подібної міжнародної угоди буде негативним прецедентом, оскільки засвідчить неспроможність чинного міжнародного права врегулювати питання масового стеження. Натомість, вчений вважає, що наразі існує

достатня кількість міжнародних угод, що ефективно справляються з регулюванням цієї сфери, зокрема Міжнародний пакт про громадянські та політичні права, Європейська конвенція з прав людини та Американська конвенція з прав людини, а також обширна практика ЄСПЛ з цього питання. Крім того, він переконаний, що такі держави, як США, Великобританія, Росія та Китай, що найбільш активно вдаються до практики масового стеження, ніколи не погодяться на підписання такої угоди, а без їх участі ухвалення такої угоди не має сенсу [182].

Натомість Дж. Каннатачі впевнений, що подібний аргумент є абсолютно диковинним, адже якщо слідувати такій логіці, то конвенція про заборону хімічної зброї ніколи не була б укладена. На його думку, потребують також уточнення стаття 12 Загальної Декларації прав людини та стаття 17 Міжнародного пакту про громадянські та політичні права у контексті визначення поняття приватності. Він зазначає, що швидкий розвиток ІКТ змінює контекст правовідносин, що потребує відповідного відображення на нормативному рівні. Наразі недостатньо просто закріпити право на приватність, натомість окрім загальних принципів необхідно прописати конкретні способи та засоби захисту, що підлягають застосуванню відповідно до контексту правовідносин. Таким чином, загальні принципи зберігатимуть свою чинність, а спеціальні потребуватимуть постійного перегляду та оновлення. Каннатачі проводить також цікаву аналогію з морським, космічним та екологічним правом, зазначаючи, що вирішити ті складні питання, що становлять предмет регулювання цих галузей міжнародного права, вдалося лише шляхом укладення відповідних міжнародних договорів. А, отже, відповідна угода повинна бути укладена із питань кіберпростору [183].

Різниця в нормативно-правових підходах в рамках регіональних організацій може бути пояснена різним рівнем технологічного розвитку держав. Так, Г. Фаррелл вважає, що ухвалення універсальних норм є можливим за умови, коли держави поділяють спільні цінності. Втім, погляди держав світу щодо режиму використання та захисту кіберпростору суттєво відрізняються. Крім того, різняться також підходи держав щодо визнання відкритої, універсальної природи Інтернету та забезпечення кібербезпеки, що, в свою чергу, ускладнює ухвалення загальнообов'язкових міжнародних договорів глобального характеру. Держави охоче погоджуються на прийняття міжнародно-правових норм, що відповідають загальним інтересам та за умови, що держава, яка виступає ініціатором ухвалення

відповідної норми, не використовує її зі злим умислом. Так, надання розголосу практиці масового стеження США змусило окремі держави з насторогою віднестися до так палко відстоюваних американцями принципів відкритості, універсальності та безпеки Інтернету. Це, в свою чергу, дало додаткові аргументи прихильникам ідеї суверенітету у кіберпросторі, таким як Росія та Китай. До того ж, держави не є єдиними, а часто навіть найважливішими, акторами у кіберпросторі, що змушує їх прислухатися та враховувати думку приватного сектору та громадянського суспільства [184].

Як зазначає В. Талімончик, у рамках ЄС регулюється велика кількість питань інформаційного обміну. Для ЄС характерне таке ж різноманіття проблем, як і для Ради Європи. У той же час, остання приділяє більшу увагу політичним проблемам інформаційного обміну, праву людини на інформацію та його гарантіям у різних умовах, а сферу інтересів ЄС формують економічні аспекти міжнародного інформаційного обміну. Обмін інформацією у межах ЄС є одним з факторів, що забезпечує функціонування спільного ринку. Саме тому навіть шляхи вирішення соціальних проблем інформаційного обміну закріплюються на нормативному рівні у контексті подолання економічних труднощів. При цьому Рада Європи приймає документи загального характеру, а нормотворчість ЄС орієнтована на ухвалення конкретних програм, у рамках яких вирішуються різноманітні питання інформаційного обміну, такі як комп'ютерна безпека, мовне різноманіття, розбудова інформаційного суспільства, тощо. Крім того, регулювання в рамках ЄС шляхом прийняття обов'язкових актів характеризується більшим ступенем оперативності, що відповідає потребам науково-технічного прогресу. Натомість прийняття текстів міжнародних договорів державами-членами Ради Європи може бути доволі тривалим процесом та затягнутися на кілька років [185].

При розробці універсальних міжнародних договорів слід утримуватися від абсолютизації ролі ІКТ у 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 та інфраструктурну інтеграцію.

Глобалізація зумовлює необхідність перегляду зафіксованих жорстких меж між національною та міжнародною сферами регулювання, тим самим змінюючи наше уявлення

про належність тієї чи іншої групи міжнародних відносин до відповідної сфери регулювання [186]. Наразі можемо спостерігати більш гнучкий підхід до нормативно-правого регулювання, який передбачає відхід від ідеї, згідно з якою право повинне походити з єдиного владного джерела, яким є суверен [187, с. 76]. 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 в силу 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 в силу жодних причин. Тенденція до збереження розмежування між національним та міжнародним правом дуже швидко втрачатиме свою актуальність у контексті питань розвитку глобального інформаційного суспільства. Пріоритетними формами регулювання повинні стати універсальні стандарти та саморегулювання.

Наразі відсутня зацікавленість суб'єктів міжнародних відносин в універсальному регулюванні 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 піднімають питання про перегляд існуючих регуляторних рамок.

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. У 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

глобального інформаційного суспільства повинно бути стандартизованим за своєю природою та окреслювати допустимі види поведінки і 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. В умовах перехідного періоду міжнародного права від права міждержавного до права транснаціонального та переділу нормотворчих повноважень зросла роль міжнародних судових інституцій у формуванні стандартів правозастосування з питань розвитку глобального інформаційного суспільства, про що й піде мова у наступному підрозділі.

2.3. Роль судової практики у формуванні основ міжнародно-правового регулювання з питань розвитку глобального інформаційного суспільства

Лакмусовим папірцем ефективності нормативно-правового регулювання є його здатність пристосовуватися до змін, що відбуваються в контексті об'єкту регулювання. До цього часу відбулася достатня кількість дискусій з питань розбудови глобального інформаційного суспільства та нормативних основ його функціонування. Наразі існує нагальна потреба у виробленні конкретних рішень. Сучасні інформаційні відносини продовжують розвиватися за схемою, коли держави прагнуть зберігати свою першість у нормотворчій сфері. При цьому, усі спроби домовитися завершуються черговою домовленістю перенести обговорення до наступної зустрічі в рамках одного з багатосторонніх інституційних механізмів. Натомість конкретні дії мають місце з боку приватних компаній, технічних спільнот та громадянського суспільства, що значно краще розуміють потреби кінцевих Інтернет-користувачів.

Імовірно, єдиним традиційним механізмом, що встигає оперативно реагувати на зміни у кіберпросторі та окреслювати тенденції розвитку міжнародно-правового регулювання, є міжнародні судові інституції. Правовий вакуум часто є причиною надмірної

перевантаженості судів, що є фактично єдиною інстанцією, здатною розтлумачити особливості правозастосування з питань розвитку глобального інформаційного суспільства.

Наразі міжнародні суди не просто вирішують спори, але активно заявляють про своє місце у процесах глобального управління розвитком інформаційного суспільства. В умовах міжнародно-правового вакууму їх рішення фактично закладають основу правозастосування у кіберпросторі. Часто при розгляді справ міжнародні суди виходять за рамки конкретного спору, встановлюючи загальні принципи поведінки у контексті певних правовідносин, тим самим перебираючи на себе нормотворчу функцію. Суб'єкти міжнародного права посилаються на рішення міжнародних судових установ з питань Інтернету значно частіше, ніж на відповідні нормативно-правові акти. Це можна пояснити прогресивністю судової практики порівняно зі складністю прийняття міжнародно-правових норм загальнообов'язкового характеру. Втім, досі подібні зміни у нормотворчій діяльності судових установ не знайшли належного відображення у доктрині міжнародного права.

Феномен міжнародного судового правотворення є найбільш помітним на прикладі судових установ, що приймають рішення з достатньою регулярністю для того, щоб можна було говорити про певну спадковість та розвиток [188, с. 21]. При цьому судове правотворення не слід вважати побічним ефектом вирішення спорів. Прикладом цього може бути створення Міжнародного центру з врегулювання інвестиційних спорів, що стало відповіддю на неможливість держав домовитися про застосовне матеріальне право. Була надана перевага судовому процесу над матеріальним правом, що зрештою призвело до формування масиву інвестиційного права як результату вирішення інвестиційних спорів [189, с. 127].

Традиційно доктрина міжнародного права розглядає судові установи в контексті вирішення спорів та тлумачення міжнародно-правових норм, тим самим обмежуючи їх функціональну спроможність. Фактично міжнародне судочинство зводиться до застосування абстрактних норм до конкретних справ. Втім, слідуючи логіці Канта рішення кожної індивідуальної справи не може бути виведене із абстрактних концепцій [190, с. 13]. Ще Г. Кельзен говорив про неможливість чіткого розмежування між правотворенням та правозастосуванням [191, с. 82–83]. На думку Р. Брендома, кожне рішення щодо використання чи тлумачення певної концепції стає частиною сутнісного наповнення цієї

концепції. Дискреційні та творчі повноваження при правозастосуванні є частиною нормотворення [192, с. 180]. Згідно з доктриною *res judicata* суди приймають рішення з урахуванням конкретних обставин та правовідносин між сторонами у спорі. По суті ж, таке рішення має наслідки, що виходять далеко за рамки розглядуваного спору. Воно може бути використане для обґрунтування позиції сторін у наступних подібних спорах в аспекті тлумачення певної норми міжнародного права [193, с. 39]. Таким чином, йдеться про відповідність судової практики справедливим нормативним очікуванням сторін, тобто того як сторонам слід поводитися та, найголовніше, тлумачити міжнародне право. Такий підхід дає сторонам підстави сподіватися на вирішення своєї справи згідно з усталеною практикою відповідної міжнародної судової установи, що у випадку конкуруючої юрисдикції може бути причиною надання переваги одній з них перед іншими. При детальному аналізі чітких та подекуди категоричних формулювань, що використовуються суддями міжнародних судів для обґрунтування своїх рішень, можна помітити їх орієнтованість на прогресивний розвиток міжнародного права.

Судові рішення мають відмінний від основних джерел міжнародного права вплив на міжнародний правопорядок. Вони використовуються у якості аргументів та формують загальний міжнародно-правовий дискурс. Нормотворчий потенціал судових рішень залежить не лише від волі відповідних суб'єктів (*voluntas*), але й від логіки самого рішення (*ratio*). Таким чином, нормотворчий ефект судового рішення залежить від його сприйняття та застосування в подальшій практиці. У багатьох рішеннях у якості основної аргументації позиції сторін та самого суду використовуються саме прецеденти, а не норми міжнародних договорів. У випадку з інформаційним суспільством це може бути пояснено відсутністю відповідних спеціалізованих міжнародних угод, завдяки чому судова практика виявляється більш обширною та зрозумілою. Розвиток міжнародного права в аспекті відображення питань глобального інформаційного суспільства повинен відбуватися з урахуванням нормотворчої функції судових установ, що відповідає динамічності та багатоманітності правовідносин у досліджуваній сфері.

Інтернет-компанії та оператори отримують величезну кількість транскордонних запитів з боку органів державної влади, судів та окремих індивідів. Міжнародне право досі не дало відповіді щодо того, яким чином повинне відбуватися правозастосування з питань

кіберпростору та якими будуть гарантії належного судового процесу, його відкритості та справедливості.

Чимало спорів, пов'язаних з Інтернетом, вирішується в національних судах. При цьому практика правозастосування може значно відрізнятися залежно від країни. Однією з найбільших труднощів, з якою й досі доводиться зіштовхуватися національним судам, є встановлення персональної юрисдикції. Адже більшість національних законів презюмує наявність достатнього мінімуму зв'язку відповідача з відповідною юрисдикцією. Підставою для оспорювання наявності юрисдикції часто ставало те, що зв'язок з відповідачем можна встановити лише через сервер, що знаходиться в іншій державі. На наступному етапі труднощі виникають з визначенням застосовного матеріального права. Встановлення компетентного правопорядку з посиланням на державу місцезнаходження сервера практикують компанії, чиї сервери знаходяться у США. Адже саме законодавство США містить доволі ліберальні норми та відстоює свободу слова на противагу праву на приватність, що є одним з фундаментальних прав людини в рамках ЄС. Не менш проблемним є процес виконання рішень іноземних судів з питань, пов'язаних з Інтернетом. Норми публічного порядку можуть значно відрізнятися в державі, де була розпочата певна Інтернет-активність, та державі, у якій мали місце наслідки такої активності [194, с. 1963].

З питань глобального інформаційного суспільства міжнародні суди застосовують концепцію динамічного тлумачення. Величезна кількість справ пов'язана з принциповою несумісністю транснаціональної природи Інтернету та обмеженими державними кордонами національними законами. У той же час, сплеск тероризму в Європі додав жару в дискусії щодо обов'язку онлайн платформ моніторити та видаляти відповідний контент. Крім того, горизонтальна природа режиму відповідальності посередника, що застосовується в ЄС, підняла питання щодо розмежування авторського права та свободи вираження поглядів. Не припиняються також дискусії між прихильниками більш жорстких регуляторних заходів з міркувань кібербезпеки та тими, хто відстоює фундаментальні права та свободи Інтернет-користувачів. Згідно з даними ВОІВ у 2015 році майже на 4% порівняно з попереднім роком зросла кількість справ, пов'язаних з доменними іменами, що були розглянуті Центром арбітражу та посередництва [195].

Нижче розглянемо справи міжнародних судових установ та національних судів, що

набули найбільшого резонансу та стали знаковими для розвитку Інтернету та глобального інформаційного суспільства в цілому.

Рішення Суду Європейського Союзу

У *справі щодо «права бути забутим»* (*right to be forgotten*) або *«права позбутися індексації»* (*right to be de-indexed*) Суд ЄС розглянув роль компаній при прийнятті рішення щодо запитів, які до них надходять [196]. Фактично суд дозволив громадянам ЄС звертатися до пошукових систем з проханням вилучити з результатів пошукового запиту посилання, що є відповіддю на пошук за їхнім ім'ям. Для того, щоб інформація була видалена, вона повинна відповідати наступним критеріям: вважатися неспіврозмірною, невідповідною, більше не відповідною, надмірною або такою, що не відповідає публічному інтересу.

Національна комісія Франції з інформатики та свобод наполягала на тому, що на виконання рішення суду *Google* повинен повністю видаляти деіндексований контент, щоб доступ до нього неможливо було отримати через використання інших доменів поза межами ЄС. За словами голови комісії така вимога не є спробою екстериторіального застосування законодавства Франції. Все, чого вони вимагають, це простого дотримання права ЄС неєвропейськими компаніями, що пропонують свої послуги в Європі [197].

Позиція *Google* зводилася до того, що жодна держава не повинна мати повноважень контролювати доступ користувача до контенту в третій країні. Такий підхід повністю суперечить відкритій природі Інтернету. «Право бути забутим» не є загальновизнаним правом людини, а лише європейським стандартом. Крім того, контент, що вважається незаконним в одній країні, може не мати жодних обмежень в іншій [198].

Втім, невиконання вимог Національної комісії могло загрожувати компанії величезними штрафами. І тому у січні 2016 року *Google* вирішив змінити спосіб виконання судового рішення. Компанія планує розпочати використання географічного блокування IP-адрес з метою заборонити доступ користувачів ЄС, до контенту, вилученого з пошукових систем. Наразі *Google* вилучив відповідні пошукові результати лише з локальних версій пошукової системи в ЄС.

Насправді дане рішення має чимало негативних наслідків. Перш за все, *Google* вимушений у кожному конкретному випадку приймати суб'єктивне і одночасно соціально важливе рішення щодо видалення контенту. Суспільний інтерес не може вимірюватися нормативними приписами ЄС. Крім того, це рішення підриває довіру користувачів до пошукових систем, оскільки наразі особа може суттєво скоригувати пошук за своїм ім'ям, тим самим зумовивши видалення інформації, що на думку інших користувачів може вважатися необхідною. Дане рішення можна також розглядати у контексті спроб держав здійснювати цензуру контенту. З часом обмеження наче сніговий ком лише наростають: від боротьби з дитячою порнографією та порушенням авторських прав – до захисту ділової репутації.

У *справі «Digital Rights Ireland»* [199] Суд ЄС встановив порушення статей 7 та 8 Хартії основних прав ЄС та визнав недійсною Директиву ЄС 2006/24/ЕС, відповідно до якої провайдери Інтернет послуг повинні були зберігати телекомунікаційні дані користувачів, що у випадку необхідності могли бути використані для сприяння попередженню та переслідуванню злочинів. Директива мала своєю метою гармонізацію законодавства держав-членів ЄС щодо збереження строком до двох років метаданих (дані про Інтернет-трафік, місцезнаходження користувачів тощо) щодо електронних листів, повідомлень та телефонних дзвінків користувачів у межах ЄС. Одночасні судові провадження щодо законності запропонованих заходів було розпочато в Ірландії та Австрії. Громадська організація «*Digital Rights Ireland*» стверджувала, що Директива стане основою для нормативних актів, що легалізують масове стеження в порушення основоположних прав людини. Вищий суд Ірландії та Конституційний суд Австрії визнали себе некомпетентними проводити оцінку таких заходів доки не буде встановлено чинність самої Директиви. З огляду на це обидва суди направили запити до Суду ЄС, де провадження були об'єднані. Суд ЄС встановив, що Директива порушує право на захист персональних даних та повагу до приватного життя. На думку Суду, Директива також не пройшла тест на пропорційність запропонованих нею заходів для досягнення переслідуваної мети. Директиві бракувало конкретності в аспекті часових рамок, умов зберігання даних та обов'язків провайдерів Інтернет-послуг і органів безпеки, що мають право вимагати доступу до таких даних. Рішення у цій справі стало важливим етапом на шляху утвердження сприятливого

нормативного середовища для захисту приватності та персональних даних онлайн. Воно має особливе значення в контексті програм масового стеження, що здійснюються урядами найбільш технологічно розвинених країн.

1 жовтня 2015 року Суд ЄС прийняв знакове рішення у справі *«Weltimmo SRO v. Hungarian National Authority for Data Protection and Freedom of Information»*, яким визнав, що компанії, які здійснюють свою діяльність в одній країні та надають послуги мовою цієї країни, навіть за умови, що їх штаб-квартира знаходиться в іншій країні, можуть бути притягнені до відповідальності органами із захисту персональних даних [200]. Це рішення матиме серйозні наслідки для компаній, що здійснюють свою діяльність у кількох юрисдикціях у межах ЄС. Дотримання різнорідних національних приписів може стати надскладним завданням для таких компаній. Фактично своїм рішенням суд скасував так званий принцип єдиного вікна (*one-stop-shop approach*). Суд також детально розглянув і визнав доволі гнучкою концепцію місця здійснення господарської діяльності (*establishment*), що передбачає ведення ефективної та реальної діяльності через стійкі утворення. При аналізі питання компетентної юрисдикції Суд ЄС провів розмежування між повноваженнями вести розслідування та застосовувати санкції.

Рішення у даній справі може призвести до великої кількості випадків конфлікту юрисдикцій. Можливим рішенням може стати уніфікований нормативний акт у межах ЄС з питань захисту персональних даних, прийняття якого заплановано на кінець 2017 року.

Так, словацький веб-сайт нерухомості *Weltimmo* було оштрафовано угорською владою за порушення приписів угорського законодавства про захист персональних даних. Досі компанії підпорядковувалися юрисдикції держави місцезнаходження штаб-квартири. З цією метою чимало компаній обирали Великобританію чи Ірландію (напр., *Facebook*), де законодавчі приписи щодо захисту персональних даних є доволі ліберальними та сприятливими для бізнесу.

У справі «*BestWater International GmBH v. Mebes*» Суд ЄС заборонив власникам авторського права обмежувати можливість Інтернет-користувачів розміщувати на інших веб-сайтах гіперпосилання на об’єкт, захищений авторським правом, що знаходиться у відкритому доступі [201]. При цьому, техніки, що використовуються, не повинні копіювати чи відтворювати об’єкт, захищений авторським правом. Суд постановив, що коли власник

авторського права дозволяє опублікування твору в Інтернеті, він передбачає доступ до нього усіх Інтернет-користувачів як публіки в цілому. Таким чином, коли особа здійснює синхронізацію посилань на твір, що вже знаходиться у відкритому доступі будь-де на просторах Інтернету, такі дії не можуть вважатися новим опублікуванням, здійсненим без дозволу автора та в порушення його виключних прав. Цим самим Суд ЄС підтвердив своє попереднє рішення у справі «*Svensson v. Sverige AB*» з тим лише застереженням, що таке перенаправлення за посиланням забороняється, якщо сайт, на якому вперше було опубліковано об'єкт авторського права, містить обмеження доступу, наприклад, на підставі оплати за підписку [202].

У справі *«Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)»* Суд ЄС постановив, що Інтернет-провайдери не можуть бути зобов'язані встановлювати системи фільтрування з метою блокування завантаження незаконного контенту [203]. На думку Суду, таке необмежене фільтрування порушує Директиву ЄС про електронну торгівлю та може стати перешкодою для правомірного використання Інтернету і законної передачі даних. Інтернет-провайдери не повинні здійснювати загальний моніторинг контенту, що передається через їхні мережі. Однак, контент-провайдери можуть вимагати від Інтернет-провайдерів блокування доступу третіх осіб, що порушують їхні права. Використання систем фільтрування може стати загрозою для свободи інформації, оскільки складно автоматизувати всі нюанси розмежування між законним та незаконним контентом. Це, в результаті, може призвести до блокування законних комунікацій. Суд також зазначив, що невибіркові системи фільтрування будуть порушувати фундаментальні права Інтернет-користувачів, зокрема право на захист персональних даних, отримання та передачу інформації, що закріплені у Хартії основних прав ЄС. Крім того, Суд зазначив, що IP-адреси є охоронюваними персональними даними, оскільки вони дозволяють з точністю ідентифікувати відповідних користувачів.

Питання про те, чи є, зокрема, динамічні IP-адреси персональними даними та відповідно чи можуть вони зберігатися окрім як з метою надання Інтернет-послуг було розглянуто Судом 25 лютого 2016 року на запит Німецького федерального суду [204]. Питання полягає в тому, що у випадку з динамічними IP-адресами оператор веб-сайту не володіє необхідною ідентифікуючою інформацією для встановлення особи користувача за

допомогою наявних у його розпорядженні IP-адрес. Така інформація знаходиться у третьої сторони – Інтернет-провайдера та може бути отримана лише через надсилання запиту.

Крім того, Суд ЄС повинен встановити відповідність німецького акту «Про телемедіа» Директиві ЄС 95/46/ЕС «Про захист персональних даних». Так, згідно з національним законом Інтернет-провайдер може збирати та обробляти персональні дані користувачів без їхньої згоди лише в тій мірі, в якій це необхідно для забезпечення загального функціонування веб-сайту чи здійснення платежів. Відповідно, слід встановити необхідність дотримання положень щодо обробки персональних даних в контексті IP-адрес. При цьому, відповідно до національного акту така обробка дозволяється лише, якщо вона є необхідною в цілях задоволення законного інтересу контролера та не порушує інтереси і основоположні права суб'єкта даних, якими у даному випадку є користувачі. У ході судового слухання увага Суду була більше звернена саме до другого питання.

Рішення Суду у цій справі дозволить поставити крапку у суперечках щодо розрізнення між статичними і динамічними IP-адресами та їх приналежністю до категорії персональних даних. Втім, Суд може обмежитися метою, з якою німецька влада збирала IP-адреси, тим самим залишивши відкритим питання про розмежування між різними видами IP-адрес. У такому випадку вже німецький суд буде вирішувати про переважання безпекових інтересів оператора над правом на приватність Інтернет-користувачів. Чим завершиться розгляд цієї справи стане зрозумілим після представлення генеральним адвокатом Суду ЄС свого висновку у травні 2016 року.

У жовтні 2011 року Суд ЄС виніс знакове рішення щодо визначення компетентної юрисдикції при розгляді справ, пов'язаних з порушенням прав особи в Інтернеті. Рішення було прийняте на основі об'єднання двох проваджень у справах «*eDate Advertising GmbH vs. X*» та «*Olivier and Robert Martinez vs. MGN Limited*» [205]. Зокрема, Суд встановив, що стаття 5(3) Регламенту Брюссель I «Про юрисдикцію, визнання та виконання судових рішень у цивільних і комерційних справах» дозволяє особі, чиї права було порушено шляхом опублікування певної інформації в Інтернеті, подати позов як до суду держави місця реєстрації провайдера чи здійснення ним основної господарської діяльності, так і до суду держави свого громадянства чи будь-якої іншої держави-члена ЄС, з території якої можна отримати доступ до оспорюваного контенту. Однак, в останньому випадку

юрисдикція судів буде обмежуватися розміром шкоди, завданої на території відповідної держави. При цьому, у розумінні Директиви про електронну торгівлю провайдер послуг не повинен зазнавати більших обмежень, ніж ті, що передбачені матеріальним правом держави місця реєстрації провайдера.

Рішення Європейського суду з прав людини

У своєму рішенні від червня 2015 року у справі «*Delfi v. Estonia*» Європейський суд з прав людини (надалі – «ЄСПЛ») визнав відповідальність естонського Інтернет-порталу новин *Delfi* за анонімні, образливі коментарі його читачів виправданим втручанням у свободу вираження поглядів [206]. Суд в обґрунтування своєї позиції посилався на екстремістську природу коментарів, їх опублікування на професійному сайті комерційних новин, недостатність заходів з боку новинного порталу для видалення оспорюваних коментарів та низьку імовірність судового переслідування користувачів, що розмістили такі коментарі. Дане рішення може стати причиною надмірно прискіпливого ставлення посередників до розміщуваного на їх ресурсах контенту з метою уникнення відповідальності. Ще однією опцією є відключення функції коментування, що призведе до обмеження можливостей для свободи вираження поглядів. У цій справі ЄСПЛ не визнав порушення права вільно передавати інформацію, на яке посилалася *Delfi* відповідно до статті 10 Європейської конвенції з прав людини.

Цілком імовірно, що справа була б вирішена на користь *Delfi* за умови її розгляду в Суді ЄС. Адже відповідно до Директиви ЄС про електронну торгівлю посередники звільняються від відповідальності у випадку застосування ними до коментарів користувачів механізму «повідомити та вилучити»: повідомлення про незаконне розміщення та вимога вилучити контент (*Notice and Take Down*).

У лютому 2016 року у справі «*MTE and Index v. Hungary*» ЄСПЛ знову розглянув питання відповідальності посередників та цього разу встановив факт порушення свободи вираження поглядів, тим самим реабілітувавши себе в очах правозахисників та Інтернет-користувачів [207]. Справа стосувалася відповідальності неприбуткової саморегулівної організації провайдерів Інтернет-контенту «*MTE*» та Інтернет-порталу новин «*Index*» за образливі коментарі, розміщені на їх веб-сайтах. При цьому Суд відзначив, що ця справа відрізняється від справи «*Delfi v. Estonia*» тим, що коментарі не містили основних елементів

мови ненависті та заклику до насилля. Натомість вони стосувалися питань, що становлять суспільний інтерес. Суд також наголосив, що при оцінці природи коментарів необхідно враховувати контекст та стиль спілкування на відповідних веб-порталах. Крім того, *Delfi,* на відміну від *MTE* був комерційним порталом. ЄСПЛ також постановив, що угорські суди не віднайшли необхідний баланс між конкуруючими правами на свободу вираження поглядів та повагу до ділової репутації.

Цікавим є той факт, що Суд далі розвинув тлумачення концепції «повідомити та вилучити». Було визнано, що система «повідомити та вилучити» може слугувати ефективним інструментом збалансування відповідних прав та інтересів, якщо вона передбачає механізм швидкого реагування. Таким чином, було звужено сферу дії рішення порівняно з рішенням у справі «*Delfi v. Estonia*», яким передбачався загальний моніторинг контенту. На основу цього рішення можна говорити про позитивні зрушення в контексті відповідальності посередників. Надмірність охоронних заходів для боротьби з мовою ненависті, дифамацією та іншими порушеннями онлайн у якості побічного ефекту може спричинити невиправдані обмеження для реалізації прав Інтернет-користувачів.

Свобода вираження поглядів онлайн стала предметом розгляду ЄСПЛ у справі «*Cengiz and Others v. Turkey*» [208]. Суд одноголосно постановив, що рішення турецького суду про блокування доступу до *YouTube* на період з 5 травня 2008 року до 30 жовтня 2010 року становило порушення статті 10 Європейської конвенції з прав людини. ЄСПЛ визнав, що накладення загальної заборони порушує права на свободу вираження поглядів, отримання та передачу інформації. Суд провів розмежування зі справою «*Akdeniz v. Turkey*» [209], у якій йшлося про блокування доступу до музичних веб-сайтів. Блокування доступу до *YouTube* призвело до недієвості популярної платформи для розкриття політичних питань, що містить специфічну інформацію, доступ до якої доволі складно отримати з використанням інших засобів. У випадку з музичним порталом доступ до відповідних музичних файлів можна було отримати шляхом використання альтернативних засобів. Крім того, *YouTube* розкриває політично важливу інформацію, яку часто обходять увагою популярні медіа. Тим самим канал сприяє розвитку громадської журналістики.

Цей випадок також перекликається з іншим важливим рішенням ЄСПЛ у справі «*Yildirim v. Turkey*» [210], де мало місце блокування в тій же Туреччині цілого домену

Google Sites через розміщення лише на одному з веб-сайтів контенту, що був сприйнятий як образливий по відношенню до пам'яті Ататюрка. Відмінність полягає у тому, що в цій справі Ахмет Їлдірім був позбавлений доступу до власного веб-сайту, а у випадку з *YouTube* накладена заборона опосередковано зачепила інтереси позивачів. Тут важливим є той факт, що статус жертви був визнаний не за особами, що прямо постраждали внаслідок блокування, а за тими, чиї права були порушені. Тобто, право оскаржити накладену заборону отримали звичайні Інтернет-користувачі, а не онлайн платформи чи власники контенту.

У своєму рішенні від 2007 року у справі «*Copland v. UK*» ЄСПЛ розглянув питання щодо меж приватності на робочому місці [211]. Так, згідно з обставинами справи позивач, працюючи особистим помічником директора коледжу, в силу своїх обов'язків часто співпрацювала з робочих питань з новопризначеним заступником директора. З часом з'ясувалося, що останній здійснював моніторинг дзвінків, електронної кореспонденції та Інтернет-трафіку позивача нібито з метою попередження використання службового обладнання в особистих цілях. На той момент у Сполученому Королівстві право на приватність не було закріплене на законодавчому рівні. ЄСПЛ встановив порушення статті 8 Європейської конвенції з прав людини щодо поваги до приватного життя.

Втім, у своєму рішенні від 12 січня 2016 року у справі «*Bărbulescu v Romania*» ЄСПЛ зайняв протилежну позицію щодо електронного стеження за працівниками [212]. Суд визнав, що доступ роботодавця до приватної кореспонденції працівника становив обмеження права на приватність, однак не порушував статтю 8 Європейської конвенції з прав людини. Свою позицію у цій справі ЄСПЛ обґрунтував тим, що внутрішніми правилами роботодавця прямо заборонялося будь-яке непрофесійне використання обладнання на робочому місці. Відповідно, роботодавець мав право доступу до аккаунту працівника у *Yahoo Messenger*, добросовісно припускаючи, що спілкування зводилося до обговорення робочих питань. Суд також визнав розумним бажання роботодавця перевірити, чи працівники виконують свої професійні обов'язки в робочий час. Крім того, моніторинг було визнано пропорційним, оскільки інші дані та документи, що зберігалися на комп'ютері, не стали об'єктом перевірки. Відповідно, роботодавець діяв у межах своїх дисциплінарних повноважень. Однак, Суд не став досліджувати, чому застосовані

обмеження були визнані такими, що переслідують законні цілі та відповідають закону. Недостатньо були досліджені й самі фактичні обставини справи, що залишаються доволі суперечливими при детальному аналізі показань обох сторін.

Рішення ЄСПЛ від грудня 2015 року у справі *«Роман Захаров проти Росії»* стало важливим у контексті практики масового стеження держав та надмірної абстрактності національних законів у цій сфері [213]. У ході судового розгляду ЄСПЛ заново підтвердив принципи, визнані у його попередніх рішеннях. ЄСПЛ застосував досить широкий підхід до аналізу обставин даної справи, зазначивши, що якщо особа заявляє про те, що вона стала об'єктом стеження, їй достатньо довести лише розумну імовірність, особливо враховуючи той факт, що у більшості випадків отримати відповідні докази буде абсолютно неможливим. Крім того, заявники можуть скаржитися на весь регуляторний механізм у сфері стеження *in abstracto*, без необхідності доведення, що саме вони стали об'єктом такого стеження. Позитивним моментом є те, що Суд дослідив не лише положення російського законодавства, але й практику надання дозволів на здійснення стеження. Відкритим залишається питання про позицію суду щодо екстериторіального стеження та стеження за участі третіх держав.

У контексті цього рішення було сформульовано ключові вимоги до нормативних актів у розглядуваній сфері. Так, запити щодо перехоплення комунікацій індивідів повинні бути максимально детальними, зокрема містити інформацію щодо конкретних осіб, телефонних номерів чи місць. Прямий доступ правоохоронних органів до телекомунікаційних мереж не надає належних та ефективних гарантій проти зловживань. Запити щодо надання дозволу на стеження повинні бути об'єктом детальної перевірки та відповідати певним стандартам. Ця справа стала знаковою для перевірки відповідних національних законів на відповідність принципам законності, необхідності та пропорційності, розроблених ЄСПЛ. Так, у Великобританії обговорюються поправки до закону про повноваження слідчих органів, у якому тепер повинні бути враховані застереження, висловлені судом.

У справі *«Редакція газети «Правое дело» і Штекель протиУкраїни»* ЄСПЛ розглянув питання правомірності використання представниками ЗМІ інформації, розміщеної в Інтернеті, та повторної публікації таких матеріалів [214]. У постанові по даній

справі ЄСПЛ вперше визнав, що стаття 10 Європейської конвенції з прав людини повинна тлумачитися як така, що покладає на держави позитивне зобов'язання по встановленню належної нормативно-правової бази для забезпечення ефективного захисту свободи вираження поглядів журналістами в Інтернеті. У цій справі на заявників було покладено обов'язок виплатити збитки за повторну публікацію тексту, автор якого був невідомий. Текст мав об'єктивно дифамаційний характер і був знайдений ними в Інтернеті (текст супроводжувався приміткою із зазначенням джерела і того, що газета не мала відношення до тексту). Вони також повинні були опублікувати спростування і свої вибачення, незважаючи на те, що це не було передбачено законом.

При розгляді справи за статтею 10 Європейської конвенції ЄСПЛ встановив, що втручання, з приводу якого була подана скарга, не було «передбачено законом», як це вимагається пунктом другим цієї статті, оскільки на той момент українське законодавство не надавало захист журналістам, що повторно опублікували матеріал з Інтернету. Крім того, національні суди відмовилися поширювати на цю ситуацію дію положень, що захищали друковані засоби масової інформації.

ЄСПЛ зауважив, що ризик завдання шкоди здійсненню та використанню прав людини і свобод, зокрема права на повагу до приватного життя, який становлять інформація з Інтернету та комунікація в ньому, є безумовно вищим, ніж ризик, який походить від преси. Встановивши порушення статті 10 Європейської конвенції щодо відсутності адекватних гарантій використання журналістами інформації, отриманої з Інтернету, ЄСПЛ визнав, що відсутність чітких, зрозумілих, доступних положень у національному законодавстві щодо використання журналістами інформації з Інтернет-джерел призводить до неможливості передбачення ними наслідків своїх дій. Імовірно, позиція ЄСПЛ у даній справі матиме особливе значення для захисту свободи вираження поглядів журналістами в Інтернеті. Відсутність належної нормативної бази може, на думку ЄСПЛ, слугувати для ЗМІ перепоною на шляху виконання функції «сторожових псів» демократії.

У справі *«Газета «Україна-Центр» проти України»* ЄСПЛ звертає увагу на джерела інформації, які використовують ЗМІ [215]. Так, заявник (газета «Україна-Центр») опублікував статтю, яка містила інформацію журналіста щодо звинувачення кандидата на

посаду міського голови Кіровограда в замовному вбивстві, представлену на прес-конференції цього кандидата в Українському незалежному інформаційному агентстві новин (УНІАН). У рамках розгляду цивільного позову національні суди визнали опубліковану інформацію дифамаційною, неправдивою, не підтвердженою офіційними джерелами та присудили сплатити значну компенсаційну суму позивачеві. Заявник стверджував, що національний суд не врахував, що опублікована інформація була доступною широкій громадськості та опублікована на сайті УНІАН. Окрім того, пропозиції щодо публікації спростування, які надавала газета як до, так і протягом судового розгляду, були відхилені.

У цьому рішенні Європейський суд повторив установлений раніше принцип свободи слова та захисту журналістів, зазначивши, що «повідомлення новин, засноване на інтерв'ю або відтворенні висловлювань інших осіб, відредагованих чи ні, становить один із найважливіших засобів, за допомогою яких преса може відігравати свою важливу роль «сторожового пса суспільства». Таким чином, у даній справі ЄСПЛ підтвердив право журналістів на використання опублікованої та доступної інформації.

Рішення національних судів

Сполучені Штати Америки

Одним з найперших знакових рішень американських судів у контексті Інтернету стало рішення суду Західного округу Пенсильванії у справі *Zippo Manufacturing v. Zippo Dot Com. Inc.*, у якій йшлося про різницю між активними та пасивними веб-сайтами та було встановлено, що віддалені, пасивні веб-сайти не наділяють суд персональною юрисдикцією.

Нещодавнім прикладом недолугості правової фрагментації в інформаційній сфері є справа *Microsoft*, у якій США хочуть витребувати електронні листи у справах щодо наркотиків 2013 року з аккаунту поштового сервісу *Hotmail*, розташованого в Ірландії. Фактично, перед нью-йоркським судом стоїть завдання визначити межі екстериторіальної дії суверенних прав США та, зокрема, норм щодо доступу до даних користувачів, що знаходяться на серверах, розташованих в межах юрисдикції Ірландії.

Microsoft наполягає на застосуванні ірландського права. Компанія зайняла жорстку позицію, відповідно до якої одностороннє правозастосування, що відкрито чи приховано посягає на суверенні права іншої держави, буде неодмінно мати серйозні наслідки у

міжнародних відносинах. Але найгірше те, що під загрозою опинилася приватність громадян США. Натомість, уряд США заявляє, що оскільки *Microsoft* є американською корпорацією зі штаб-квартирою у Вашингтоні, усі дані, що зберігаються на її серверах у будь-якій точці світу, можуть абсолютно законно бути затребувані у судовому порядку.

Microsoft оскаржила рішення суду про передачу даних, посилаючись на той факт, що записи зберігаються у базі даних іноземної держави та належать самим Інтернет-користувачам, а не корпорації. Крім того, таке рішення суду, на думку компанії, породжує конфлікт юрисдикцій та створює недопустимий прецедент застосування екстериторіальної юрисдикції. Слід також зазначити, що ордер на обшук не містить необхідних специфікацій та надає майже необмежений доступ до електронних скриньок. Рішення у даній справі закладе прецедент щодо правозастосування у сфері хмарних технологій.

У нещодавній справі за участі компанії «*Apple*» перед американськими судами гостро постало питання віднайдення балансу між правом на приватність та національною безпекою. Так, ФБР вимагає від компанії розблокувати *iPhone 5s*, що належав одному з терористів, винному у вбивстві 14 осіб у Сан Бернардіно (Каліфорнія), зазначаючи що даний захід є виключним у контексті обставин, що склалися, з метою попередження наступних атак. У судовому рішенні від компанії не вимагається взламувати кодування, натомість пропонується створити нове програмне забезпечення, яке б дозволило ФБР швидко підібрати пароль без пошкодження даних [216]. На підтримку «*Apple*» виступили такі компанії як *Google, Microsoft, Twitter, Airbnb, AT&T* тощо, що направили до суду записки друзів суду (*amicus brief*) [217].

Станом на березень 2016 року компанія «*Apple*» була стороною у дванадцяти судових провадженнях, в яких уряд вимагав розблокування 12 приладів [218]. 1 березня 2016 року окружний суд східного округу Нью-Йорку у іншій кримінальній справі щодо торгівлі наркотиками постановив, що компанія «*Apple*» не зобов'язана проти своєї волі допомагати урядовим слідчим отримати доступ до даних заблокованого телефону [219]. При цьому, зазначається, що ФБР прагне не просто отримати докази у даній конкретній справі, а швидше закласти небезпечний прецедент примушування приватних технологічних компаній співпрацювати з органами кримінального переслідування та допомагати останнім обходити технологічні обмеження. Оскільки Конгрес США дозволив компаніям

створювати телекомунікаційні прилади з відповідними заходами безпеки, відсутні підстави стверджувати, що компанія «*Apple*» якимось чином порушила чинне законодавство, дозволивши своїм користувачам блокувати власні прилади. Натомість немає жодного законодавчого акту, який би надавав уряду необмежені повноваження щодо примусового залучення приватних компаній до співробітництва у кримінальних справах. На думку суду, уряд намагається використати кожну подібну судову справу для розширення сфери дії «Акту про усі судові документи» (*All Writs Act*) 1789 року, оскільки Конгрес ніколи не погодиться на надання уряду необґрунтовано широких повноважень у сфері розслідування кримінальних справ.

9 лютого 2016 року окружний суд округу Массачусетс прийняв знакові рішення у *справах проти Гарвардського університету та Массачусетського технологічного інституту* [220]. Обидві справи стосувалися необхідності супроводжувати субтитрами навчальні відео онлайн. Позов було подано на основі Акту про американців з обмеженими можливостями (*Americans with Disabilities Act*) та розділу 504 Акту про реабілітацію. В обох справах суд визнав цифрове право на спілкування за глухими або особами, що мають вади слуху. Крім того, він відзначив, що особи з обмеженими можливостями повинні мати рівні з іншими можливості доступу до розміщеного в Інтернеті контенту. Таким чином, було підтверджено доступність Інтернету для кожного.

У справі «*United States v. Cotterman*» [221] Апеляційний Суд Дев'ятого Округу США зіштовхнувся з труднощами здійснення прикордонного контролю у випадку, коли дані розташовані на хмарному сервісі. При використанні хмарних технологій «вразливі» дані користувачів, аналогічні тим, що можуть мати паперову форму, зберігаються на віддалених серверах, а не на самих пристроях, за допомогою яких можна отримати доступ до таких даних. Цифровий пристрій, таким чином, виступає лише у якості провідника інформації з хмарного сховища на зразок ключа від банківського сейфу. При цьому, слід звернути увагу на той факт, що хоча саме цифрове сховище й не перетинає кордон, воно може розглядатися як невід'ємна частина пристрою, що надається для огляду при проведенні контролю. Доступ до хмарного сервісу фактично робить доступними величезні масиви даних та інформації про особу. Саме тому у даній справі суд постановив, що представники державних органів повинні мати достатні підстави для підозрювання особи з тим, щоб

проведення обшуку комп'ютеру на кордоні вважалося правомірним. Так, законною підставою для здійснення обшуку може бути судовий наказ. Надто широке тлумачення права прикордонних органів здійснювати обшук часто стає підставою обмеження цифрового права на приватність в обмін на право в'їзду в країну. Суд зауважив, що цифрове життя особи не повинне зазнавати втручання в силу факту перетину кордону. У рішенні також зазначалося, що раніше люди подорожували з обмеженою кількістю речей. Однак, технологічний прогрес зробив можливим брати з собою в подоріж великі масиви особистої інформації на переносних приладах. У той же час, доступ до таких приладів означатиме не просто обшук валізи, а всього, що коли-небудь у ній перевозилося. У даній справі суд вперше встановив обмеження повноважень державних органів здійснювати обшук електронного приладу на кордоні. Відкритим залишилося питання про те, що слід розуміти під експертним обшуком. У той же час, обґрунтована підозра була визначена як наявність конкретних та відчутних фактів, що демонструють достатню імовірність існування кримінальної діяльності.

Німеччина

У січні 2016 року *у справі за позовом Федерації німецьких організацій споживачів* від 2010 року Федеральний суд Німеччини визнав функцію пошуку друзів (*friend finder*) *Facebook* незаконною та такою, що становить недобросовісну конкуренцію і порушує німецьке законодавство щодо захисту персональних даних [222]. Дана функція надає соціальній мережі доступ до списку контактів електронної пошти користувача, внаслідок чого відбувається розсилка запрошень приєднатися до мережі тим, хто ще не має *Facebook* аккаунту. На думку суду, *Facebook* не вжив достатніх заходів з метою інформування користувачів щодо використання даних з їх списку контактів. Наразі ще залишається невстановленим які практичні наслідки матиме дане рішення для соціальної мережі та її послуг на території Німеччини. Слід також зазначити, що *Facebook* не єдина компанія, що використовує подібні маркетингові інструменти з метою залучення нових користувачів.

Франція

12 лютого 2016 року Апеляційний суд Парижу підтвердив можливість подання позовів проти *Facebook* у Франції [223]. Справа стосувалася французького вчителя, чий аккаунт було тимчасово заблоковано після того, як він поділився фото відвертої картини з

паризького Музею Орсе. Суд відхилив заперечення соціальної мережі про те, що згідно з її умовами надання послуг застосовною є юрисдикція штату Каліфорнія. Рішення французького суду може закласти небезпечну практику притягнення *Facebook* до відповідальності поза межами США.

Одним з найвідоміших рішень щодо визначення компетентної юрисдикції у справах, пов'язаних з Інтернетом, стало рішення французького суду за позовом Ліги проти расизму та антисемітизму (LICRA) та Союзу єврейських студентів Франції (UEJF) до американської компанії *Yahoo!*. Остання звинувачувалася у тому, що на її веб-сайті проходив аукціон, де, серед іншого, були виставлені пам'ятки нацизму, що заборонені згідно з французьким законодавством. Верховний суд Франції постановив, що *Yahoo!* повинна розробити систему фільтрування, яка б не дозволяла французьким користувачам брати участь в аукціоні. У протилежному випадку на компанію накладалися штрафні санкції. *Yahoo!* хоч і видалила всю продукцію з нацистською символікою зі свого сайту, однак звернулася із зустрічним позовом до окружного суду північного округу Каліфорнії з проханням визнати, що рішення, винесене французьким судом, є невиконуваним по відношенню до американської компанії, особливо враховуючи те, що веб-сайт, щодо якого виник спір, був розташований на серверах, які знаходилися в США. У 2001 році американський суд задовільнив вимоги заявника та зазначив, що *Yahoo!* не зобов'язана виконувати рішення щодо обмеження контенту. Так, американське законодавство застосовується до веб-сайтів, адміністрування яких здійснюється з території США. Крім того, відповідно до Першої поправки до Конституції США власник має право на свободу слова, а рішення іноземних судів не підлягають виконанню. Через два роки французький суд зняв кримінальні обвинувачення з *Yahoo!*, зазначивши, що за виключенням незаконного аукціону у Франції компанія ніколи не робила спроби виправдати воєнні злочини чи злочини проти людяності. Однак, у січні 2006 року Апеляційний суд США дев'ятого округу встановив відсутність персональної юрисдикції окружного суду у даній справі по відношенню до французьких організацій LICRA та UEJF, повернув справу на дорозслідування з вказівкою відхилити позов [224]. У травні 2006 року Верховний Суд США відмовив у перегляді справи по суті.

Великобританія

Принцип територіальності був застосований англійським судом для обґрунтування

своєї юрисдикції у справі «*R v. Graham Waddon*» [225], пов'язаній з публікацією інформації в Інтернеті у контексті Акту про непристойні публікації 1959 року. Було встановлено, що публікація мала місце, коли зображення порнографічного характеру були завантажені на веб-сайт та коли вони були збережені з сайту користувачами. Відповідач заперечував проти юрисдикції суду, посилаючись на те, що опублікування інформації відбулося за кордоном, оскільки фізично сервери, на яких зберігалися дані, знаходились у США. Суд постановив, що у розумінні Акту 1959 року опублікування включає також зберігання даних в електронній формі та їх передачу. Передача оспорюваної інформації провайдеру та її отримання мали місце в межах юрисдикції англійських судів. Рішення у цій справі є прикладом застосування територіального законодавства до транскордонного феномену, яким є Інтернет. Фактично, був застосований підхід, згідно з яким незалежно від фізичного місцезнаходження даних порнографічного характеру, суди держави, де відбувається завантаження такого контенту користувачами, можуть також розглядати справи щодо незаконності його опублікування, якщо це передбачено відповідно до національного законодавства.

Австралія

Подібний підхід був застосований і австралійським судом у справі «*Dow Jones & Company Inc. v Gutnick*», у якій йшлося про розміщення в Інтернеті матеріалів дифамаційного характеру [226]. Так, було встановлено, що опублікування статті онлайн мало місце в межах юрисдикції держави, де стаття була доступна користувачам, незалежно від того, де вона була завантажена в мережу чи місця знаходження серверів. Такий територіальний підхід до регулювання діяльності Інтернет-провайдерів означатиме, що останні узгоджуючи відповідні дії з законами однієї держави, завжди порушуватимуть закони якоїсь іншої держави. Фактично, така позиція судів надає позивачам можливість маніпулювання з вибором найбільш вигідної для них юрисдикції у справах, пов'язаних з опублікуванням відповідної інформації в Інтернеті.

Ірландія

Своїм рішенням у справі «*EMI Records (Ireland) Ltd & ors v. Eircom Ltd*» від квітня 2011 року Вищий суд Ірландії визнав, що IP-адреси не є персональними даними у розумінні Акту про захист персональних даних Ірландії [227]. Рішення стосувалося угоди, укладеної

між найбільшим ірландським Інтернет-провайдером *Eircom* та чотирма лідируючими звукозаписуючими компаніями – *EMI, Sony, Universal and Warner*, якою запроваджувалася кількарівнева система реагування, спрямована на боротьбу з незаконним обміном файлами. Згадана система передбачала залучення незалежної агенції *DetectNet* для здійснення сканування на предмет порушення авторських прав з боку Інтернет-користувачів. У випадку встановлення порушення користувачами *Eircom,* останній передавали IP-адреси таких користувачів, яка у свою чергу повинна була вжити відповідні заходи (спочатку попередження, яке, якщо залишалося проігнорованим, приводило до відключення доступу до Інтернету). В обґрунтування своєї позиції суд пояснив, що *DetectNet* не має доступу до ідентифікуючої інформації власників IP-адрес, а отже не може самостійно, без допомоги третьої сторони встановити особу Інтернет-користувачів. У силу цього, IP-адреси, що знаходяться у володінні *DetectNet,* не є персональними даними. При цьому, поза увагою національного суду залишилася Директива 95/46/ЕС про захист персональних даних. Крім того, суд визнав відсутність порушення з боку *Eircom*, оскільки обробка даних здійснювалася на основі згоди користувачів з умовами надання послуг цим Інтернет-провайдером, а також у зв'язку з тим, що така обробка була необхідною для виконання умов контракту та зобов'язань за ним. Рішення ірландського суду є суперечливим в контексті визнання принципу мережевої нейтральності та вкотре засвідчує різнорідність підходів до питання захисту персональних даних навіть у межах самого ЄС.

Таким чином, проаналізовані судові рішення свідчать про те, що правовідносини сторін, опосередковані використанням Інтернету часто стають предметом розгляду національних судів. При цьому, позивачі надають перевагу тим юрисдикціям, що є для них найбільш сприятливими та зрозумілими в контексті застосовуваного права. Велика кількість судових проваджень щодо різноманітних аспектів Інтернету є показником того, що за правопорушення, вчинені в межах глобальної мережі або з її використанням, цілком реальним є притягнення до відповідальності. При цьому недосконалим залишається процес кваліфікації відповідних діянь як протиправних, а також сам процес застосування національного законодавства до транскордонних правовідносин. Саме тому окремо слід виділити практику Європейського суду з прав людини та Суду ЄС, що здійснюють колосальну роботу в контексті розширювального тлумачення діючого міжнародного права

та адаптації відповідних норм та принципів до динамічно прогресуючого розвитку глобального інформаційного суспільства. Фактично, гармонізація правозастосування з питань розвитку глобального інформаційного суспільства відбувається на рівні ухвалення судових рішень провідними судовими установами. Крім того, прослідковується також значний нормотворчий потенціал судових інституцій у тому розумінні, що саме суди виявилися найбільш спроможними оперативно реагувати на зміни в ускладнених технологічною складовою правовідносинах, тим самим окреслюючи тенденції та напрямки розвитку відповідного нормативного регулювання, що лише з проходженням певного часу знаходить відображення у відповідних міжнародно-правових актах.

ВИСНОВКИ ДО РОЗДІЛУ 2

Встановлено, що в умовах глобального інформаційного суспільства відбувся фактичний перерозподіл владних та нормотворчих функцій, що зумовило зростання ролі «м'якого» права та судових рішень у якості додаткових нормативних регуляторів суспільних відносин, опосередкованих використанням Інтернету. З появою транснаціонального права нормотворчість перестає бути виключним правом держав, підтвердженням чому є постійно зростаюча кількість регуляторних актів з питань розвитку глобального інформаційного суспільства, що були розроблені та прийняті за участі недержавних акторів.

Технологічна орієнтованість міжнародного права в епоху глобального інформаційного суспільства є необхідною умовою його прогресивного розвитку та трансформації у дієвий регулівний механізм, що відповідає вимогам часу та інтересам суб'єктів.

Нетривала історія розвитку глобального інформаційного суспільства є однією з основних причин відсутності великого масиву договірних міжнародно-правових норм у цій сфері, що доволі успішно компенсується зміцненням звичаєвих норм. Характерною особливістю останніх є миттєвість їх формування та відсутність компоненту тривалості застосування норми поведінки. Більшість договірних режимів не є універсальними, натомість звичаєві норми інколи мають більше охоплення за колом суб'єктів, що вважають

себе зобов'язаними цією нормою. Різний рівень технологічного розвитку держав світу свідчить про більшу ймовірність формування регіональних звичаєвих норм з питань розвитку глобального інформаційного суспільства, аніж універсальних стандартів.

Міжнародні договори з питань розвитку глобального інформаційного суспільства часто укладаються вже після того, як на практиці фактично сформувались певні суспільні відносини, виявивши прогалину у чинному міжнародно-правовому регулюванні. У результаті цього в умовах глобального інформаційного суспільства спостерігається відсутність органічної єдності міжнародного права та правопорядку, що склався та розвивається на основі множинності нормативних регуляторів, розроблених у ході багатостороннього діалогу між усіма зацікавленими суб'єктами.

Протягом останніх трьох десятиліть у теорії міжнародного права сформувалася концепція «м'якого» права як чогось середнього між «твердим» правом та відсутністю нормативного регулювання. «М'яке» право характеризується гнучкістю та високим ступенем адаптивності до змін, пов'язаних з виокремленням та ускладненням питань розвитку глобального інформаційного суспільства. Крім того, «м'яке» право передбачає максимально гнучкий механізм перегляду нормативних актів та внесення до них відповідних змін та поправок.

Враховуючи, що одним із основних принципів глобального інформаційного суспільства є багатостороння участь, прийняття актів «м'якого» права в результаті переговорів між усіма зацікавленими сторонами є закономірним процесом.

Глобальність інформаційного суспільства формує потребу у такому ж глобальному міжнародно-правовому регулюванні та правовиконанні. Прогресивний розвиток міжнародного права з питань розвитку глобального інформаційного суспільства проявляється у формуванні окремої комплексної галузі – міжнародного інформаційного права. При цьому, якщо розглядати глобальне інформаційне суспільство у широкому розумінні як воно запропоноване у авторському визначенні в підрозділі 1.1, тобто як усю повноту правовідносин (правопорядок), що виникають в інформаційній сфері, то за предметною сферою воно охоплює усі напрями міжнародно-правового регулювання в інформаційній сфері. У вузькому розумінні міжнародно-правові питання розвитку глобального інформаційного суспільства можна виділити у якості окремої підгалузі

міжнародного інформаційного права зі специфічним предметом регулювання. Так, до питань розвитку глобального інформаційного суспільства, що потребують врегулювання на нормативному рівні, пропонується включати наступні: а) інформаційна та комунікаційна інфраструктура; б) використання ІКТ у цілях розвитку; в) управління Інтернетом; г) інституційні механізми посиленої та багатосторонньої співпраці; ґ) права людини онлайн; д) кібербезпека та відповідальна поведінка держав у кіберпросторі. Наведений перелік не є вичерпним та підлягає постійному перегляду і доповненню з метою приведення його у відповідність з технологічним прогресом та відповідними змінами в інформаційних правовідносинах. Два останні питання розвитку глобального інформаційного суспільства були виділені автором у якості найбільш суспільно важливих та нормативно розроблених, що й спонукало присвятити їм наступний розділ дисертаційного дослідження.

На основі проведеного аналізу нормативно-правових актів з питань розвитку глобального інформаційного суспільства автором розроблено їх класифікацію за предметною сферою дії. Групування регуляторних актів у досліджуваній сфері покликане полегшити їх використання у правозастосовній діяльності. Так, першу групу становлять акти, спрямовані на регулювання глобального інформаційного суспільства як самостійного феномену (Окінавська хартія глобального інформаційного суспільства, Конвенція РЄ про інформаційне та правове співробітництво щодо «послуг інформаційного суспільства», Ініціатива «Електронна Європа – інформаційне суспільство для всіх»). Другу групу формують міжнародно-правові акти з питань кіберпростору (Проект рекомендацій ЮНЕСКО щодо розвитку і використання багатомовності та універсального доступу до кіберпростору, Концепція інформаційного простору та Угода про співпрацю у сфері інформації СНД, Комюніке Великої двадцятки за результатами саміту в Анталії, Декларація Монтре «Про захист персональних даних у глобальному світі: універсальне право, що поважає багатоманітність», Уфімська декларація країн-членів БРІКС, Довільська декларація «Групи восьми» «Незмінна відданість свободі та демократії» тощо). Міжнародно-правові акти, що увійшли до третьої групи, сфокусовані на питаннях управління та функціонування Інтернету (Рекомендація РЄ щодо вільного, транскордонного потоку інформації в Інтернеті, Стратегія РЄ з управління Інтернетом, План дій ЄС щодо зміцнення безпечного використання Інтернету шляхом боротьби з

незаконним та шкідливим контентом у глобальних мережах, «Цифровий порядок денний для Європи», Комюніке ОЕСР щодо принципів розробки Інтернет-політики). Класифікуючою ознакою наступної категорії є заборона сексуальної експлуатації дітей та дитячої порнографії (Конвенція ООН з прав дитини та Факультативний протокол до неї від 2000 р., Лансаротська конвенція, Директива ЄС про боротьбу з сексуальним насиллям та експлуатацією дітей, а також дитячою порнографією). Окрему групу становлять також міжнародно-правові акти щодо використання ІКТ у цілях розвитку людства (Конвенція Тампере, Санкт-Петербурзька декларація держав-членів АТЕС «Забезпечення довіри та безпеки у використанні ІКТ для сприяння економічному росту та процвітанню»). Самостійний предмет міжнародно-правового регулювання становлять також питання інтелектуальної власності (Спільна рекомендація ВОІВ щодо положень про захист знаків та інших прав промислової власності на позначення в Інтернет).

У ході дослідження вдалося виявити зростаючу роль міжнародних судових установ, зокрема Європейського суду з прав людини та Суду ЄС, у процесах нормотворення з питань глобального інформаційного суспільства. Саме суди виявилися здатними найбільш оперативно реагувати на зміни у правовідносинах в рамках глобального інформаційного суспільства та закладати тенденції розвитку відповідного міжнародно-правового регулювання. Крім того, судова практика формує основи правозастосування в аспекті розширювального тлумачення чинних міжнародно-правових норм у їх застосуванні до питань розвитку глобального інформаційного суспільства.

Судові рішення мають відмінний від основних джерел міжнародного права вплив на міжнародний правопорядок. Вони використовуються у якості аргументів та формують загальний міжнародно-правовий дискурс. Розширення нормотворчого потенціалу міжнародних судових установ з питань глобального інформаційного суспільства та застосування судами концепції динамічного тлумачення є свідченням прогресивного розвитку міжнародного права у досліджуваній сфері. У той же час, у контексті попередження та уникнення негативних тенденцій екстериторіального правозастосування особливої актуальності набуває ухвалення відповідних міжнародно-правових актів з питань розвитку глобального інформаційного суспільства.

Основні висновки розділу висвітлені в наукових працях автора [228-233].

РОЗДІЛ 3
МІЖНАРОДНЕ СПІВРОБІТНИЦТВО З ПИТАНЬ РОЗВИТКУ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Наразі найбільш обговорюваними питанями розвитку глобального інформаційного суспільства визнаються права людини онлайн, захист персональних даних та кібербезпека. Їм присвячена найбільша кількість міжнародно-правових актів у сфері розвитку глобального інформаційного суспільства. Відповідно, на основі їх аналізу автором буде продемонстровано ефективність адаптації міжнародного права до швидко прогресуючих інформаційних правовідносин та правопорядку. Вивчення позитивних прикладів прогресивного розвитку міжнародного права з окремих питань глобального інформаційного суспільства дозволить вивести певні закономірності та особливості формування специфічного режиму міжнародно-правового регулювання інформаційних правовідносин в межах самостійної галузі – міжнародного інформаційного права. Предметне наповнення третього розділу дисертації є невипадковим. Питання прав людини онлайн, захисту персональних даних та співробітництва у сфері кібербезпеки були виділені автором у якості найбільш суспільно важливих та нормативно розроблених. Так, їм присвячено окремі розділи Женевському Плані дій 2003 року, Доповіді Робочої групи щодо посиленої співпраці Комісії ООН з науки і техніки у цілях розвитку «Окреслення питань міжнародної державної політики щодо Інтернету» 2014 року, Фінальному документі ВСІС+10 тощо. Крім того, окреслені напрямки становлять основу багатостороннього діалогу щодо співробітництва з питань розвитку глобального інформаційного суспільства.

Навіть якщо керуватися чисто формальною юричною логікою права людини завжди знаходилися у центрі уваги міжнародного співтовариства. Це особливо справедливо в умовах глобального інформаційного суспільства, розвиток якого зумовив перехід від

державоцентричної до людиноцентричної системи міжнародних відносин. І хоча самі права людини залишаються незмінними, розширюється тлумачення їх змістового наповнення та виникає потреба у створенні специфічних засобів і механізмів правового захисту, які б враховували специфіку кіберпростору. Одним із найбільш яскравих та вдалих прикладів поступової трансформації міжнародного права до умов глобального інформаційного суспільства є сфера захисту персональних даних. Крім того, це питання органічно переплітається з попереднім, оскільки зачіпає одне з фундаментальних прав людини у цифрову еру – право на приватність. Питання безпеки ніколи не зникало з міжнародного порядку денного, а розвиток глобального інформаційного суспільства лише переніс їх у нову кіберплощину. При цьому, саме кібербезпека викликає чимало суперечностей з приводу предметної підпорядкованості цієї сфери міжнародного співробітництва. Саме у питанні кібербезпеки держави найменш схильні поступатися своїм суверенітетом на користь багатосторонніх інституційних механізмів, побудованих за принципом участі усіх зацікавлених сторін. Адже традиційно суб'єкти, до відання яких належали безпекові питання, вважалися найбільш впливовими у міжнародних відносинах.

3.1. Міжнародно-правові стандарти захисту прав людини онлайн

Розвиток глобального інформаційного суспільства нерозривно пов'язаний із питанням захисту прав людини онлайн. Технологічний прогрес зумовив непропорційно швидкий ріст загроз та порушень прав людини. Інтернет відкриває практично безмежні можливості для зловмисників. Однією з основних причин є перманентне відставання міжнародного права в аспекті створення ефективних правових механізмів захисту прав людини онлайн. Онлайнове середовище є простором, у якому цінності прав людини часто ігноруються та порушуються. Потенційний негативний вплив порушень прав людини онлайн на демократичний розвиток та безпеку індивіда і держави вимагають створення ефективних та відмінних від вже існуючих механізмів захисту таких прав. Основна складність полягає у тому, що прояви порушень прав людини онлайн доволі складно відслідкувати, оцінити та застосувати ефективні засоби протидії. Поширеною стала

практика застосування технологічних засобів (напр., блокування та фільтрування) у відповідь на порушення прав людини онлайн або їх попередження. Новими правами людини, визнання яких стало можливим лише в умовах глобального інформаційного суспільства, є доступ до Інтернету та «право бути забутим».

Питання захисту прав людини має таку ж тривалу історію розвитку, як і саме міжнародне право, у нормах якого знайшли своє відображення мінімальні стандарти забезпечення прав людини. Досі було вироблено величезну кількість міжнародно-правових угод у сфері прав людини і, здавалося б, усе, що можна було б сказати, уже сказано та закріплено у відповідних міжнародних та національних актах. Держави світу доволі давно досягли згоди щодо фундаментальних принципів та мінімальних стандартів прав людини, що донедавна становили незмінне ядро права прав людини. Втім, швидкий розвиток ІКТ додав нового звучання концепції прав людини та розширив можливості їх реалізації. Універсальний доступ до кіберпростору [16] розглядається деякими вченими не лише як засіб, що сприяє реалізації прав людини, але як самостійне право. Так, доступ до Інтернету отримує визнання загальнолюдської цінності, а не простої технологічної передумови, доступної розвиненим країнам, для надання ще одного майданчику для здійснення прав людини.

У контексті прав людини держави володіють одночасно позитивними та негативними зобов'язаннями (уникати порушень). З одного боку, вони повинні надавати гарантії захисту прав людини, а з іншого – саме держави є чи не найбільшими їх порушниками. На відміну від інших суб'єктів держави володіють необхідними владними повноваженнями, що роблять можливими зловживання у даній сфері. Держави часто нехтують свободою вираження поглядів нібито з міркувань національної безпеки. Задача міжнародного права, таким чином, зводиться до перманентного збалансування суперечливих інтересів різних зацікавлених сторін. Втім, не дивно, що держави, будучи первинним суб'єктом міжнародного права, є також єдиним суб'єктом, що завжди отримує бажане. З появою Інтернету відбулися певні зміни у розподілі владних повноважень на міжнародній арені. Відповідно, державам доводиться рахуватися з позицією великих технологічних корпорацій.

Слід зазначити, що у момент своєї появи Інтернет-середовище було значною мірою

невпорядкованим та стихійним. Натомість наразі ринок послуг інформаційного суспільства, надання яких опосередковане використанням Інтернету, в переважній більшості поділений між кількома найбільшими приватними корпораціями. Держави у своїх спробах контролювати діяльність останніх періодично накладають на них правові обмеження щодо збирання та обробки інформації, втім не поспішають обмежувати чи взагалі хоч якимось чином врегулювати їх діяльність з передачі таких даних державним правоохоронним органам. Однією з основних причин невирішеності проблеми масового стеження є економічний тиск. Однак, часто держави не докладають самостійних зусиль для збору персональних даних Інтернет-користувачів. Замість них це роблять приватні компанії, від яких держави згодом вимагають копію зібраних даних.

Згідно з даними британського «*Guardian*» *Facebook* підтвердив зростання кількості урядових запитів щодо надання даних та вилучення контенту у першій половині 2015 року. У цілому, показник урядових запитів щодо отримання персональних даних зріс на 18% у світі у першій половині 2015 року. Вдвічі, порівняно з першою половиною 2014 року, зросли випадки обмеження поширення контенту в силу порушення національних законів та сягнули позначки, що становить 20 568 таких випадків. Більшість урядових запитів щодо зняття контенту були пов'язані з кримінальними справами щодо пограбувань чи викрадення дітей. Держави переважно запитували базову інформацію про Інтернет-користувачів, зокрема IP-адреси чи доступ до розміщеного ними контенту, у тому числі онлайн публікацій. Найбільша кількість запитів надійшла від правоохоронних органів США, Франції, Німеччини та Великобританії. Індія та Туреччина виявилися лідерами у контексті вилучення контенту, що суперечить національному законодавству [234].

Серед вчених та практикуючих юристів у сфері міжнародного права довго не було згоди щодо того, чи існує необхідність у виробленні окремого комплексу прав людини для онлайн середовища, так званих «цифрових прав», чи достатнім буде розширити сферу дії існуючих засобів правового захисту та відновлення порушених прав з тим, щоб охопити Інтернет. Було запропоновано чимало аргументів в обґрунтування обох позицій. Втім, компетентним міжнародним організаціям знадобився певний час для вироблення відповідного міжнародно-правового режиму захисту прав людини онлайн.

У цілях дисертаційного дослідження під цифровими правами або правами людини

онлайн пропонується розуміти права людини, реалізація та захист яких відбуваються в межах або у зв'язку з кіберпростором шляхом використання Інтернету та/або сучасних ІКТ. Концепція цифрових прав охоплює існуючі права людини у контексті їх застосування в Інтернеті, тим самим розширюючи обсяг окремих прав. Разом з тим, у міжнародному праві спостерігається тенденція до визнання доступу до Інтернету у якості самостійного права.

Ще у 1988 році відомий італійський філософ права Н. Боббіо звернув увагу на те, що найбільша проблема нашого часу полягала не у формулюванні прав людини, а у їх захисті [235]. Дане твердження є особливо справедливим у контексті прав людини у цифрову еру, оскільки права лишилися тими ж, однак суттєво змінилися способи їх захисту. Тут варто згадати статтю Дені О'Брайана, що розпочинається наступними словами: «Реальним тестом на наявність у вас прав є не приписи закону, а те, що відбувається, коли ви робите спробу реалізувати їх» [236].

У червні 2012 року Рада ООН з прав людини ухвалила знакову резолюцію, якою вперше підтвердила, що ті ж права, якими людина володіє офлайн, повинні захищатися онлайн, особливо свобода вираження поглядів, що застосовується незалежно від державних кордонів та з використанням будь-яких засобів за власним вибором особи, відповідно до статті 19 Загальної Декларації прав людини та Міжнародного пакту про громадянські та політичні права [237].

Як справедливо зазначає Маттіас Кеттеман, відсутня необхідність заново формулювати права людини. Натомість уже існуючі права слід застосовувати до справ, пов'язаних з Інтернетом, у контексті викликів, що виникають онлайн. Автор звертає увагу на технологічну нейтральність мови, якою написана стаття 19 Загальної Декларації прав людини у контексті використання будь-яких засобів. Він також зазначає, що посилання на статтю 19 Міжнародного пакту про громадянські та політичні права містить у собі певні загрози свободі вираження поглядів онлайн, оскільки вона передбачає застосування обмежень, що можуть стати предметом зловживань з боку держав, які намагатимуться зберегти контроль над реалізацією цього права онлайн. При цьому боротьба проти незаконного контенту не повинна використовуватися державами у якості виправдання для здійснення цензури онлайн [238].

Важливе питання про те, чи слід цифрові права вважати правами людини підняв

Джошуа Копштайн. На думку вченого, наша цифрова ідентичність є невід'ємною частиною кожного як особи. Він наводить приклад великих компаній, що маніпулюють споживацькою поведінкою своїх користувачів шляхом відстеження та обробки їх цифрової активності та даних, доступних онлайн. Копштайн наполягає на тому, що найбільша проблема цифрової ери полягає у переважаючому розумінні прав людини як концепції, що пов'язана виключно з фізичною ідентичністю особи. Натомість персональні дані повинні визнаватися частиною нас як людей, тим самим розширюючи поняття прав людини на цифрові права [239].

Продовжуючи дискусію, Магдалена Гавронська зауважує, що наразі ми живемо в цифровому світі, що прийшов на зміну аналоговому та завдяки своїй транскордонній природі відкрив новий вимір прав людини. Вона вважає, що назріла необхідність у глобальній кампанії за цифрові права з метою перегляду міжнародно-правових документів з прав людини у контексті відображення у них технологічних досягнень та їх впливу на права людини [240].

Доволі схожих поглядів дотримується Джованні Сартор, який вважає, що ІКТ не просто відкривають нові способи здійснення прав людини, але є передумовою самого існування окремих прав людини чи принаймні визначення їх внутрішнього наповнення. Він звертається до права на доступ до Інтернету на рівних умовах як прикладу трансформації технологічних можливостей спочатку у моральне, а згодом у нормативно визначене право людини [241, с. 298].

У той же час, Кетлін Бергер переконана, що складна архітектура Інтернету є причиною незадовільного стану реалізації прав людини онлайн. Вона ставить під сумнів можливість прямої трансформації усіх прав людини в онлайн середовище та залишає відкритим питання про те, чи буде при цьому змінюватися тлумачення таких прав. Далі автор наводить приклад політичної дискусії через використання додатку *Google Hangouts* у якості реалізації права на об'єднання онлайн, так і не знайшовши для себе відповіді щодо того, чи становить таке об'єднання окремий вид права на об'єднання, чи підпадає під класичне тлумачення цього права [242].

У свою чергу А. МакДіармід та М. Шиарз аналізують сприятливі передумови реалізації прав людини онлайн та виділяють мережеву нейтральність у якості основного

принципу. Згідно з їхнім підходом, порушення цього принципу шляхом блокування відповідних інформаційних ресурсів чи обмеження передачі певного контенту Інтернет-користувачами може мати серйозні негативні наслідки для права на свободу вираження поглядів. Автори наголошують на тому, що Інтернет є не просто ще одним засобом масової інформації для одностороннього поширення контенту та інформації, але також платформою для розвитку нових комунікаційних інструментів. На зразок того, як свобода вираження поглядів є стимулюючим чинником для інших прав людини, Інтернет відкриває можливості для розвитку різноманітних медіа та послуг, що, у свою чергу, сприяють реалізації свободи вираження поглядів та інших прав людини [243, с. 36].

Завершуючи огляд теоретичних підходів до дихотомічної природи прав людини офлайн та онлайн, варто згадати позицію Спеціального доповідача ООН з питань свободи вираження поглядів Девіда Кайе, який зауважив, що наразі ми в переважній більшості висловлюємо свої погляди онлайн. У зв'язку з цим, оглядаючись назад через п'ять років, проведення межі між офлайном та онлайном буде здаватися нам чимось дивним. Враховуючи темпи та масштаби переміщення всіх та всього з офлайнового до онлайнового середовища, питання зводиться фактично до зміни місця взаємодії. Д. Кайе також висловив свою позицію щодо збалансування кібербезпеки та прав людини, зазначивши, що кібербезпека не зводиться до забезпечення безпеки інфраструктури, але також індивідуальної безпеки особи в онлайн середовищі. На його думку, відсутність узгодженості між цими двома концепціями може частково бути пояснена неналагодженістю взаємодії між групами, що займаються питаннями безпеки та прав людини в структурі ООН. Крім того, Спеціальний доповідач переконаний, що для усунення ідеологічних суперечностей необхідно відмовитися від політизації питання цифрових прав та повернутися до фундаментальних принципів та норм міжнародного права прав людини [244].

Як було зазначено вище, реалізація прав людини в онлайновому середовищі надає їм нового виміру, зберігаючи при цьому той самий рівень захисту. Далі буде проаналізовано, які основні права людини формують комплекс цифрових прав. Перш за все, слід розпочати з базового права на доступ до Інтернету. Досі міжнародна спільнота не виробила єдиного підходу щодо того, чи є Інтернет окремим правом чи лише технологічною передумовою,

що сприяє реалізації інших загальновизнаних прав людини. Скептики проводять аналогію з технологічними досягненнями попередніх століть, такими як радіо, телефон та телеграф, тим самим переконуючи, що Інтернет є всього навсього складною цифровою мережею, що має цінність лише в контексті технічних переваг, які вона надає для реалізації прав людини [245]. З іншого боку, існує велика група прихильників визнання доступу до Інтернету у якості самостійного права людини. Для обґрунтування своєї позиції останні вказують на те, що сам факт відсутності доступу до Інтернету позбавляє індивідів, юридичних осіб та держави можливості бути повноправними членами глобального інформаційного суспільства [246]. У зв'язку з цим вони наполягають на визнанні доступу до Інтернету у якості базового права людини.

Вважаємо, що сучасне міжнародне повинне містити як негативні, так і позитивні зобов'язання держав щодо гарантування права на доступ до Інтернету. Так, негативне зобов'язання передбачає обов'язок держави утримуватися від будь-яких обмежень доступу індивідів до Інтернету. У той же час, позитивне зобов'язання презюмує активну участь держави у створенні належної інфраструктури, необхідної для надання універсального, безперервного доступу до швидкісного Інтернету.

На думку А. Пазюка, доступ до Інтернету уможливлює здійснення майже всіх соціально-економічних прав та є рушієм суспільного розвитку. Водночас, учений задається питанням, чи кореспондує обов'язку держав надавати доступ до Інтернету відповідне право людини на такий доступ [21, с. 131].

Відсутність нормативного закріплення права на доступ до Інтернету містить потенційну загрозу умисного відключення з будь-яких мотивів, без попереднього повідомлення та пояснення причин. Ще одним важливим аспектом права на доступ до Інтернету є необхідність закріплення на законодавчому рівні мінімальної швидкості передачі інформації, яку кожна держава та Інтернет-провайдери повинні забезпечити кожному Інтернет-користувачу. Особливої уваги потребує питання забезпечення доступності засобів електронної комунікації для осіб з обмеженими можливостями у контексті надання онлайн послуг та пристосування таких засобів до їх потреб. Не менш важливим є створення необхідних умов та механізмів для навчання Інтернет-користувачів безпечній та свідомій поведінці в онлайн середовищі, а також постійне підвищення

обізнаності Інтернет-користувачів щодо їхніх прав з метою спонукання їх до здійснення свідомого вибору при реалізації своїх прав онлайн.

Право доступу до Інтернету у якості універсальної (публічної) послуги визначене Директивою ЄС «Про універсальні послуги» 2009 року, яка закріплює право кожного в межах ЄС на доступ до мінімального набору доступних електронних комунікаційних послуг хорошої якості, включаючи доступ до Інтернету [247].

Кодекс ЄС про онлайнові права підтверджує вищезгадане положення Директиви у розділі I «Права та принципи, що застосовуються при доступі до онлайн послуг та їх використанні» [248]. Кодекс не вводить в обіг нові права, однак містить базові права та принципи. Документ не має юридично обов'язкової сили, однак окремі права та принципи, відображені в його тексті, повинні дотримуватися в силу їх обов'язковості згідно з іншими міжнародно-правовими актами.

Не можна залишити без уваги й «Порядок денний у сфері сталого розвитку на період до 2030 року», що, серед іншого, передбачає суттєве зростання доступу до ІКТ, а також гарантування універсального та доступного Інтернету у найменш розвинених країнах до 2020 року [63].

У практиці ЄСПЛ питання доступу до Інтернету вперше було підняте у 2012 році. У справі «Їлдірім проти Туреччини» Суд зазначив, що право безперешкодного доступу до Інтернету також повинно бути визнане [210]. На національному рівні суди також визнають невідповідність обмежень доступу до Інтернету. Так, Апеляційний суд Англії та Уельсу постановив, що накладення на відповідача абсолютної заборони володіти комп'ютером чи мати доступ до Інтернету є неприпустимою. Таке обмеження є неспіврозмірним, оскільки обмежує відповідача у користуванні тим, що становить невід'ємну частину щоденного життя більшості населення, а також є вимогою роботодавців [249]. У наведених справах була оцінена пропорційність обмежень свободи вираження поглядів з урахуванням права на доступ до Інтернету. Такий підхід сприятиме застосуванню триступеневого тесту для встановлення відповідності обмежень доступу до Інтернету вимогам частини другої статті 10 Європейської конвенції з прав людини.

Декларація Комітету Міністрів Ради Європи про права людини та верховенство права в інформаційному суспільстві закріплює ряд прав людини, що повинні бути об'єктом

захисту в інформаційному суспільстві. Визнається, що ІКТ суттєво сприяють реалізації наступних прав: право на свободу вираження поглядів, інформації та комунікації; право а повагу до приватного життя та кореспонденції; право на освіту та важливість заохочення доступу до нових інформаційних технологій; право на справедливий суд та неприпустимість покарання, не передбаченого законом; захист власності; право на вільні вибори та свободу об'єднань [250].

На думку М. Караніколаса, права людини в онлайновому середовищі походять від універсальних прав людини, таких як право на свободу вираження поглядів, участь у культурному та політичному житті, а також право на свободу об'єднань. Інтернету належить ключова роль у сприянні реалізації цих прав. Вчений вказує на те, що права людини є похідними від особистості, факту народження людиною, а не від наявності правового зв'язку з будь-якою державою. Це особливо проявляється в контексті Інтернету, що стирає кордони між державами [251].

Дж. Джарвіс провів ще більш детальний аналіз та запропонував проект біллю прав у кіберпросторі, що містить наступні цифрові права та свободи: право на зв'язок, право на свободу слова, право на свободу користуватися рідною мовою, право на об'єднання, право діяти, право контролювати дані, право на власну ідентичність, повага до суспільних благ та відкритість Інтернету [252].

У жовтні 2015 року міжнародна неурядова організація «*Freedom House*» опублікувала щорічний звіт «Свобода в мережі 2015», у якому вказано, що свобода в Інтернеті в країнах світу п'ятий рік поспіль рухається у напрямку спадання. Згідно зі звітом зросла кількість випадків вилучення контенту. Органи державної влади 42 із 65 досліджених країн вимагали від приватних компаній чи Інтернет-користувачів обмеження доступу чи видалення онлайнового контенту, що стосувався політичних, релігійних чи соціальних питань. У той же час, почастішали арешти та випадки шантажу. У 40 державах були ув'язнені особи, звинувачені у поширенні інформації з політичних, релігійних чи соціальних питань через соціальні мережі. Починаючи з червня 2014 року 14 держав ухвалили нові закони, якими посилили заходи масового стеження, та ще більше країн почали застосовувати удосконалене обладнання для стеження. Уряди як демократичних, так і авторитарних держав світу послідовно наголошували на тому, що кодування є

терористичним інструментом, та намагалися заборонити або обмежити використання засобів захисту приватності [253].

Відповідно до звіту Україна посіла 37 місце (серед 100 країн, де 0 відображає найвищий рівень свободи в мережі, а 100 - найнижчий) та була визнана частково вільною країною у контексті забезпечення свободи в Інтернеті. Звіт охоплює період з червня 2014 по травень 2015 року та містить вказівки на ряд порушень в українському онлайновому просторі. Внаслідок тиску з боку бойовиків у східній Україні було тимчасово заблоковано проукраїнський контент на серверах, розташованих в регіоні. У квітні 2015 року була тимчасово припинена діяльність 30 000 веб-сайтів внаслідок вилучення Службою Безпеки України серверів, на яких нібито знаходився антиукраїнський контент. Діяльність більшості веб-сайтів було відновлено у найближчі тижні, втім деякі з них так і не почали працювати заново. Арешт журналіста, звинуваченого у державній зраді за розміщення відео, у якому він засуджував обов'язкову мобілізацію, продемонструвало зростаючу нетерпимість української влади до критичного контенту онлайн. Онлайн журналісти, активісти та блогери зі Східної України зазнавали незаконного залякування, піддавалися побиттю, катуванням, викраденню та іншому недостойному поводженню за висловлення проукраїнських поглядів [254].

У червні 2014 року на вимогу Генеральної Асамблеї ООН Верховний комісар з прав людини представив доповідь «Право на приватність у цифрову еру», у якій розглянув питання захисту та зміцнення права на приватність у контексті зростаючої практики масового стеження держав. Глибоке занепокоєння було висловлене у зв'язку з перетворенням масового стеження з виняткового заходу у дурну звичку [255].

Синтія Вонг з міжнародної неурядової організації «*Human Rights Watch*» вказує у своїй статті, що стеження порушує не лише право на приватність, але й такі права, як свобода вираження поглядів, об'єднань, пересування та право на адвоката. Крім того, вона зауважує, що держави повинні захищати право на приватність користувачів навіть поза межами своєї території. У глобалізованому, мережевому світі нерозумно стверджувати, що право на приватність припиняється при перетині державного кордону, у той час, як саме стеження є транскордонним за своєю природою. Автор також переконана, що приватний сектор при отриманні запитів щодо здійснення стеження чи збирання даних зобов'язаний у

першу чергу поважати права людини [256].

Крім того, у квітні 2015 року Глобальна комісія з управління Інтернетом запропонувала соціальний контракт з питань приватності та безпеки. Комісія заявила, що стеження онлайн та збирання даних повинні бути обмежені метою, чітко окресленою до початку таких заходів, а також бути передбачені законом та відповідати принципам необхідності і пропорційності [257].

У нещодавно оприлюдненій доповіді Центру «Карнегі Європа» під назвою «Управляючи кіберпростором: дорожна карта трансатлантичного лідерства» зазначається, що не варто сподіватися на ухвалення загальнообов'язкових, багатосторонніх норм з питань збалансування приватності та безпеки. Відмінності у політичних, соціальних та культурних контекстах держав є настільки суттєвими та роз'єднаними, що урядам навряд чи вдасться досягнути такої високої цілі [258]. У тексті доповіді міститься також посилання на дослідження Європейського Парламенту, у якому йдеться про те, що саме ціль та масштаби стеження є тими показниками, що відрізняють демократичний режим від поліцейської держави [259]. Дана доповідь цілком справедливо може вважатися одним з найбільш детальних сучасних досліджень, що використовує комплексний підхід для аналізу питань приватності, свободи вираження поглядів та потоків даних в Інтернеті, а також сфер управління Інтернетом, електронної торгівлі, кібербезпеки та кібервійни. Ще більшого значення документу надає той факт, що у ньому містяться пропозиції щодо майбутнього партнерства у зазначених сферах.

Тим не менше, міжнародному праву все ще належить віднайти розумний баланс між підтриманням безпеки та наданням достатніх гарантій прав людини в умовах розвитку глобального інформаційного суспільства. З моменту появи питань, пов'язаних з Інтернетом, у порядку денному глобальних зустрічей не припиняються суперечки з приводу їх співвідношення. Прогресивний розвиток міжнародного права залежатиме від його здатності збалансувати суперечливі політичні інтереси в аспекті визнання прав людини та кібербезпеки як рівно важливих цінностей глобального інформаційного суспільства.

Резолюція Генеральної Асамблеї ООН від 13 грудня 2015 року містить окремий розділ, присвячений правам людини в інформаційному суспільстві [60]. У документі підтверджується універсальність, неподільність, взаємозалежність та взаємозв'язок усіх

прав людини та основоположних свобод. Далі визнається потенціал ІКТ у зміцненні реалізації прав людини, покращенні доступу до інформації, сприянні свободі вираження поглядів та свободі об'єднань. Крім того, заново наголошується на однаковому поводженні та захисті прав людини офлайн та онлайн. Так, комунікація визначається як фундаментальний соціальний процес, базова людська потреба та основа усіх соціальних організацій, а отже визнається ключовою цінністю інформаційного суспільства.

Рада Європи цілком заслужено може бути визнана лідером у створенні нормативних стандартів у сфері прав людини онлайн. Організація визнала усі раніше прийняті правові акти щодо захисту прав людини рівною мірою застосовними до Інтернету. Одним з найбільш відомих документів є Посібник з прав людини для Інтернет-користувачів, що надає рівні гарантії прав людини та фундаментальних свобод як онлайн, так і офлайн [260]. Посібник не запроваджує нові права та фундаментальні свободи. Втім, доступ до Інтернету визнається важливим засобом реалізації прав та свобод, а також участі в демократичних процесах. Згідно з Посібником доступ повинен надаватися за розумну ціну та бути недискримінаційним. Індивіди повинні мати якомога ширший доступ до Інтернет-контенту, додатків і послуг, користуючись пристроями на власний вибір.

Нещодавно Рада Європи ухвалила нову Рекомендацію щодо захисту та зміцнення права на свободу вираження поглядів та права на приватне життя у контексті мережевої нейтральності. У документі визнається висока цінність Інтернету у контексті здійснення права на свободу вираження поглядів. Особлива увага приділяється принципу мережевої нейтральності, що лежить в основі недискримінаційного поводження з Інтернет-трафіком та права користувачів отримувати та передавати інформацію і користуватися послугами на власний вибір. Рекомендація також містить Керівні принципи щодо мережевої нейтральності. Зокрема, виділяються наступні принципи: однакове поводження з Інтернет-трафіком, плюралізм та різноманітність інформації, приватність, транспарентність та відповідальність [261].

Принцип мережевої нейтральності є необхідною передумою реалізації прав людини онлайн. Для того, щоб підкреслити його важливість та комплексність було надано авторське визначення принципу мережевої нейтральності, під яким пропонується розуміти право користувачів Інтернету отримувати доступ до інформації та послуг без дискримінації

за типом інформації, її обсягом, характером послуги, технічним способом або технічними пристроями, що їх застосовує конкретний користувач, а також імунітет операторів мережі від притягнення до відповідальності за передачу третіми сторонами контенту та додатків, що вважаються незаконними або небажаними.

У середині січня 2016 року новий голова ОБСЄ Франк-Вальтер Штайнмаєр уперше звернувся з офіційною промовою до Постійної Ради ОБСЄ, окреслюючи цілі та основні заходи в період головування Німеччини у 2016 році. Штайнмаєр зазначив у своїй промові, що повага прав людини та демократичне управління є складовими компонентами спільної політики безпеки в Європі. Він пообіцяв швидко призначити нового Представника з питань свободи ЗМІ, який повинен буде замінити Дуню Міятович на цій посаді (*авторська примітка:* 23 березня 2016 року Рада міністрів ОБСЄ продовжила мандат Дуні Міятович ще на рік. До цього вона двічі обиралася на посаду на трирічний термін). Штайнмаєр також підтвердив повну відданість концепції безпеки, що поєднує підтримання миру з повагою прав людини та фундаментальних свобод [262]. Особливий акцент у 2016 році буде зроблено на забезпеченні фундаментального права на свободу вираження поглядів, включаючи питання безпеки журналістів та пропаганди у період конфліктів, а також свободі об'єднань та мирних зібрань. Людський вимір був визнаний серед ключових пріоритетів головування Німеччини в ОБСЄ. У той же час, громадянське суспільство було визнане рівноправним партнером у формуванні спільної політики мирного та безпечного майбутнього в регіоні. Приділяючи більшу увагу правам людини, Німеччина може зміцнити свій імідж як надійного партнера у питаннях захисту інтересів індивідів в інформаційному суспільстві. Імовірність зростання впливу Німеччини збільшилася ще й у зв'язку з замішаністю урядів США та Великобританії у скандалах, пов'язаних з масовим стеженням, що негативно позначилося на популярності останніх.

На жаль, простого визнання рівного рівня захисту онлайнових та офлайнових прав недостатньо. З метою гарантування ефективного здійснення цифрових прав уряди країн світу повинні переглянути своє національне законодавство та відобразити у ньому специфічні характеристики Інтернету як нового простору взаємодії між урядом та населенням. Крім того, такі правові норми повинні бути максимально уніфікованими, враховуючи неможливість ефективного регулювання транскордонного Інтернету за

допомогою територіальних законів. Усі держави повинні гарантувати однаковий рівень захисту прав людини онлайн. У протилежному випадку фрагментація регулювання матиме наслідком численні судові спори та конфлікт юрисдикцій. Оскільки на універсальному рівні досягнення згоди щодо загальновизнаних норм у даній сфері виявилося складним завданням, деякі держави ухвалили доволі прогресивні національні акти.

Так, у квітні 2014 року Бразилія ухвалила безпрецедентний правовий акт «*Marco Civil da Internet*», що став біллем про права Інтернет-користувачів в цій країні. Закон було розроблено у ході багатосторонніх консультацій, що збільшило рівень довіри до нього та дозволило охопити в його тексті максимально широке коло питань у сфері цифрових прав. Законом закріплюються загальновизнані принципи користування Інтернетом, зокрема свобода слова, захист приватності та персональних даних, а також мережева нейтральність. Доступ до Інтернету визнається необхідною передумовою реалізації прав громадянина та ряду базових прав людини [263].

«*Marco Civil*» отримав міжнародне визнання як новий тип законодавства, спрямованого на забезпечення прав індивідів у контексті їх застосування до Інтернету. З точки зору захисту користувачів закон отримав найвищу оцінку як найбільш інноваційний нормативний акт, що надає максимальний рівень захисту. У вересні 2015 року Глобальна комісія управління Інтернетом оприлюднила дослідження, що містить оцінку «*Marco Civil*» через призму застосування методології, розробленої колишнім Спеціальним доповідачем ООН з питань свободи вираження поглядів Франком Ла Рю [264].

Пізніше, у листопаді 2015 року, міжнародна правозахисна організація «*Article 19*» опублікувала доповідь про ефективність застосування «*Marco Civil*». Надається позитивна оцінка досягнутих результатів з питань відповідальності провайдерів послуг, приватності онлайн та доступу до Інтернету. У той же час, зазначається, що доступ до Інтернету досі не було визнано публічною послугою. «*Article 19*» також вказує на такі недоліки, як дискримінація пакетів даних, використання нульового рейтингу та *Internet.org*, що є серйозним порушенням принципу мережевої нейтральності. Не безперешкодним виявився й процес імплементації електронного уряду. Окрема увага приділяється законопроекту 215/2015 (який критики охрестили проектом закону про шпигунство), спрямованому на законодавче закріплення «права бути забутим». Крім того, проектом пропонується

запровадження кримінальної відповідальності за посягання на гідність особи, а також планується розширення переліку обов'язкових даних, які користувачі будуть зобов'язані надати для отримання доступу до сервісів Інтернету. Згодом такі дані можуть бути передані будь-якому державному органу на його запит, без необхідності отримання попереднього судового дозволу [265]. Цей законопроект становить серйозну загрозу праву на свободу вираження поглядів. У випадку прийняття він перекреслить усі позитивні здобутки «*Marco Civil*» та надовго сповільнить розвиток цифрових прав у Бразилії.

У законодавстві України доступ до Інтернету не включено до переліку загальнодоступних (універсальних) телекомунікаційних послуг. Відповідно до Стратегії розвитку інформаційного суспільства в Україні формування сучасної інформаційної інфраструктури передбачає, серед іншого, створення інфраструктури широкосмугового доступу до Інтернету на всій території України, а також створення в усіх населених пунктах України умов для доступу до Інтернету, в тому числі шляхом розбудови мережі пунктів колективного доступу [33]. У січні 2015 року була оприлюднена Стратегія сталого розвитку «Україна – 2020», що передбачає реформу телекомунікаційної інфраструктури та захисту інтелектуальної власності, запровадження програми електронного урядування, розвитку інформаційного суспільства та медіа тощо. Одним із 25 стратегічних індикаторів реалізації Стратегії визнається частка проникнення широкосмугового Інтернету, яка станом на 2020 рік повинна складати 25 абонентів на 100 осіб [266]. Механізми захисту прав людини онлайн потребують адаптації правозастосовної практики України до світових та європейських стандартів з метою підвищення їх ефективності шляхом врахування технологічних особливостей кіберпростору.

Беручи до уваги усі новації, що постали перед міжнародним правом у цифрову еру, концепція прав людини онлайн є чи не єдиною, що отримала універсальну підтримку та знайшла доволі чітке відображення у зростаючій кількості міжнародно-правових документів. Для багатьох людей у всьому світі Інтернет все ще залишається всього лише засобом спілкування та доступу до великих масивів інформації. Саме тому, первинне завдання усіх зацікавлених сторін полягає у тому, щоб показати індивідам переваги нового виміру прав людини, що проявляються у їх застосуванні в онлайновому середовищі. Задача міжнародного права полягає у прийнятті викликів цифрової ери та забезпеченні

динамічного реагування на відповідні зміни в онлайновому середовищі. Сфера прав людини може слугувати прикладом прогресивного розвитку міжнародного права та ефективності реагування на нові виклики, що з'явилися у міжнародному порядку денному у зв'язку з переходом до глобального та інклюзивного інформаційного суспільства.

Іншим актуальним питанням у глобальному порядку денному з питань розвитку глобального інформаційного суспільства є вироблення універсального режиму захисту персональних даних. Наразі ЄС та США застосовують значною мірою протилежні підходи до регулювання поводження та обробки персональних даних, що має безпосереній відношення до транскордонної передачі таких даних телекомунікаційними мережами. Так, ЄС схвильований передачею персональних даних своїх громадян до компаній, розташованих у США, та закликає їх до посилення захисту та надання додаткових гарантій. У контексті обробки персональних даних політика інституцій ЄС орієнтована на захист прав людини, у той час, як США захищає в першу чергу інтереси споживачів та орієнтуються на отримання прибутку. У зв'язку з цим, встановленню перспектив вироблення універсального міжнародно-правового режиму передачі та поводження з персональними даними присвячено наступний підрозділ дисертаційного дослідження.

3.2. Становлення універсального міжнародно-правового регулювання у сфері захисту персональних даних

З появою сучасних ІКТ, зокрема Інтернету, відбулася сутнісна трансформація процесів збирання, обробки та обміну інформацією. Передача персональних даних була зведена до надзвичайно швидких та технологічно зручних процедур. Щоденно приватні та державні структури отримують доступ до величезних масивів особистої інформації. Індивіди втрачають можливість ефективного контролю за використанням їх персональних даних. У зв'язку з цим не втрачає своєї актуальності та набуває нового окрасу питання захисту приватності фізичних осіб.

Так, Загальна декларація прав людини 1948 року закріплює, що ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, а кожна людина має право на захист закону від такого втручання або таких посягань. Міжнародний пакт про

громадянські та політичні права 1966 року майже дослівно відтворює зазначену норму. Конвенція про захист прав людини і основоположних свобод 1950 року (надалі – «ЄКПЛ») передбачає право кожного на повагу до його приватного і сімейного життя.

Важливість захисту персональних даних визнається також і в прецедентній практиці. У справі Фішера Суд ЄС підтвердив, що принципи захисту даних є загальними принципами права Співтовариства [267]. У справі *Rechnungshof* Суд зазначив, що положення Директиви 95/46/ЄС у тій мірі, в якій вони регламентують обробку персональних даних, що може призвести до порушення, зокрема права на недоторканість приватного життя, повинні завжди тлумачитися в контексті основних прав, що формують невід'ємну частину загальних принципів права Співтовариства [268]. Європейський суд з прав людини також визнав захист персональних даних у якості основного права, оскільки воно охоплюється правом на захист недоторканості приватного життя, передбаченого статтею 8 ЄКПЛ [269-272].

Наразі регулювання транскордонної передачі даних відбувається на різних рівнях. Так, більшість держав на законодавчому рівні закріпили право на недоторканість приватного життя. Власники ліній зв'язку та технічних засобів домовляються про загальні стандарти технічної сумісності, тарифи та протоколи. У свою чергу постачальники послуг використовують власний протокол конфіденційності, а користувачі дотримуються відповідних норм онлайнового етикету [273, с. 509].

Існує декілька передумов, що виправдовують застосування міжнародного права до правовідносин транснаціонального характеру в сфері захисту приватності. Відсутність універсального міжнародно-правового захисту приватності має наслідком порушення таких основних прав людини як незаконне зберігання персональних даних, зберігання неточних персональних даних, а також несанкціоноване використання чи опублікування таких даних. Крім того, суттєві розбіжності в національних підходах до регулювання досліджуваної сфери створюють перешкоди для вільного обміну персональними даними між різними державами. Національний підхід до регулювання сфери персональних даних був запроваджений кілька десятиліть тому, а отже не міг враховувати особливостей глобальної інформаційної екосистеми. Діючі нормативно-правові акти щодо досліджуваного питання втратили свою актуальність та повинні бути приведені у відповідність з досягненнями

технологічного прогресу.

Наразі вкрай важливим є створення сприятливого правового середовища, що в першу чергу означає прийняття сучасної нормативної бази, заснованої на єдиних стандартах. Це, в свою чергу, значно прискорить та полегшить транскордонний обмін інформацією на міжнародному рівні. Крім того, слід уникати надмірного регулювання. Формування універсальних регулівних механізмів повинно відбуватися з урахуванням передових практик держав у досліджуваній сфері та оптимізації існуючих нормативних актів.

Протягом тривалого часу нерозв'язаним залишається протистояння країн Європейського Союзу та США в контексті свободи поширення інформації в Інтернеті. Так, ЄС підтримує ідею контролю за контентом з метою уникнення розповсюдження шкідливих та заборонених матеріалів. У той же час, США виступають послідовними прихильниками права на свободу вираження. Тут постає питання й про застосовну юрисдикцію та вибір компетентного правопорядку. Таким чином, задача міжнародного права полягає у тому, щоб віднайти правильний баланс між суперечливими національними та регіональними підходами до регулювання транскордонних потоків інформації. Так, основна складність полягає у тому, що в силу універсальності Інтернету контент, створений в одній державі з дотриманням діючих у ній правових приписів, може вважатися шкідливим чи таким, що порушує правовий порядок у будь-якій іншій державі. Прикладами таких юрисдикційних конфліктів можуть слугувати судові справи *CompuServe* та *Yahoo!*. При вивченні питання про перспективи формування універсального нормативно-правового регулювання в досліджуваній сфері особливий інтерес представляють останні міжнародно-правові ініціативи та судові рішення щодо захисту персональних даних та приватності.

Як справедливо відзначає Голдсміт, екстериторіальне регулювання Інтернету виправдане уже в силу того, що кіберпростір за своїм функціональним призначенням нічим не відрізняється від транснаціональної діяльності держав, що здійснюється за допомогою інших засобів. Крім того, кожна держава має право регулювати ті екстериторіальні діяння, що приносять шкоду чи приводять до інших негативних наслідків в рамках її національної юрисдикції. Такий підхід використовується в багатьох національних правових системах та є правомірним доти, доки держава не зобов'яже себе нормою міжнародного права, що закріплює протилежне [274, с. 1239-1240]. Саме тому, ми вбачаємо прогресивний розвиток

міжнародного права у сфері передачі та обробки персональних даних в уніфікації розрізнених національних та регіональних підходів як на рівні нормотворення, так і на рівні правозастосування.

Ще одним аргументом на користь універсального міжнародно-правового регулювання інформаційної сфери є необхідність створення ефективного механізму захисту персональних даних і приватного життя. Незважаючи на те, що США були чи не першою державою в світі, що законодавчо врегулювала приватне життя, обсяг захисту персональної інформації завжди залишався орієнтованим на потреби ринку та підпорядковувався принципу вільного потоку інформації, відображеному в Першій поправці до Конституції США [275, с. 91]. Таким чином, державне регулювання в даній сфері залишається вкрай обмеженим. Абсолютно протилежний підхід до режиму захисту даних використовується в ЄС. Так, Шварц та Райденберг стверджують, що європейське законодавство в цій сфері є найбільш досконалим, оскільки розглядає захист даних в якості громадянського права. Вони відзначають нормативне значення приватності в контексті демократичного управління [276, с. 39-42]. ЄС, Канада, Австралія, Нова Зеландія і Гонконг, на відміну від США, надають перевагу централізованому регулюванню захисту персональних даних. Обробка персональної інформації повинна здійснюватися у суворій відповідності з правовими приписами.

У таких регуляторних умовах міжнародне право покликане виконувати роль уніфікуючого фактору, спрямованого на імплементацію єдиних, універсальних стандартів правовідносин у сфері захисту персональних даних і приватності. У рамках міжнародних організацій та інтеграційних об'єднань також спостерігається функціональний розподіл відповідних компетенцій. Так, Міжнародний союз електрозв'язку займається питаннями інституційної інфраструктури та технічними аспектами транскордонного переміщення даних, у той час як інші організації більше сконцентровані на формуванні стандартів обробки таких даних, їх передачі та безпеки [277, с. 954].

На рівні ООН питання, пов'язані з приватністю та захистом персональних даних, регулюються Керівними принципами ООН щодо регламентації комп'ютеризованих картотек, які містять дані особистого характеру 1990 року. У 2006 році в довгострокову програму діяльності Комісії міжнародного права ООН було включене питання захисту

особистих даних при транскордонному переміщенні інформації.

У квітні 2015 року Рада з прав людини ООН прийняла Резолюцію 28/16 «Право на недоторканість приватного життя в цифрову еру». Відповідно до Резолюції права, якими люди володіють у звичайному житті, включаючи право на недоторканість приватного життя, повинні захищатися й у віртуальному середовищі. Крім того, вводиться посада Спеціального доповідача щодо питання про право на недоторканість приватного життя, термін повноважень якого складає три роки. Серед іншого Спеціальний доповідач повинен збирати відповідну інформацію, зокрема про міжнародні та національні правові норми, національну практику та національний досвід, виявляти можливі труднощі, що перешкоджають заохоченню та захисту права на недоторканість приватного життя, повідомляти про можливі порушення [278]. 3 липня 2015 року першим Спеціальним доповідачем з питань приватності був призначений представник Мальти Джозеф Каннатачі [279].

Основними нормативними актами ОЕСР у цій сфері є Керівні принципи, що регулюють захист приватності та транскордонні потоки персональних даних 2013 року, Декларація про транскордонні потоки даних 1985 року, Керівні принципи безпеки інформаційних систем 1992 року, Оттавська Міністерська декларація про охорону недоторканості приватного життя в глобальних мережах 1998 року. Документи не містять юридично обов'язкових норм, але широко використовуються у правозастосовній практиці держав.

У 2004 році в рамках Азійсько-Тихоокеанського економічного співробітництва (АТЕС) було затверджено Основи захисту приватності з метою уніфікації інформаційного захисту приватного життя в державах регіону. У 2007 році була запущена Програма-шукач персональних даних (*APEC Data Privacy Pathfinder*), спрямована на забезпечення відповідального ставлення до транскордонного обміну персональною інформацією в межах регіону АТЕС [280]. 2010 рік ознаменувався прийняттям Угоди АТЕС про дотримання транскордонної приватності. Відповідно до цієї багатосторонньої угоди правоохоронні органи отримують механізм обміну інформацією та сприяння транскордонному потоку даних [281]. Документ спрямований на посилення рівня охорони транскордонного обміну персональними даними.

У листопаді 2011 року лідери держав-членів АТЕС прийняли директиву, якою запроваджувалася Система правил транскордонної конфіденційності (CBPR) [282]. У цьому документі своє визнання отримала ідея про необхідність створення правової бази у сфері конфіденційності даних, яка б забезпечувала ефективний захист приватної інформації користувачів та при цьому не створювала бар'єрів на шляху інформаційних потоків. Дана система покликана забезпечити загальнорегіональну узгодженість політики конфіденційності, що повинно знизити витрати на дотримання нормативних вимог. Нагляд за управлінням системою правил транскордонної конфіденційності здійснює координаційна група АТЕС з питань електронної комерції. До системи АТЕС приєдналися також США та Мексика.

У січні 2014 року спільний Робочий комітет АТЕС та ЄС ухвалив Спільне роз'яснення щодо структури Системи обов'язкових корпоративних правил ЄС та Системи правил транскордонної конфіденційності АТЕС [283]. Даний документ покликаний слугувати своєрідним неформальним контрольним списком для компаній, що звертаються за авторизацією в Системі обов'язкових корпоративних правил ЄС та сертифікацією в Системі правил транскордонної конфіденційності АТЕС. У ньому містяться вимоги щодо відповідності обом системам, а також відзначаються спільні елементи та додаткові умови для кожної з них. У довгостроковій перспективі планується досягти максимальної сумісності двох систем.

У січня 2015 року була запроваджена система Визнання приватності процесорів (*The Privacy Recognition for Processors (PRP)*), що регулює роботу процесорів з персональною інформацією в контексті забезпечення відповідності діяльності контролерів відповідним зобов'язанням щодо приватності. У свою чергу контролери отримують можливість визначення кваліфікованих та надійних процесорів. Процесор, що звертається із запитом про визнання, повинен заповнити анкету, на основі оцінки якої відповідальна особа АТЕС приймає рішення про визнання.

Рада Європи закріплює основи захисту персональних даних у Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція № 108) [284]. Важливо відмітити, що це перший обов'язковий до виконання міжнародно-правовий договір щодо недоторканості приватного життя. У 2001 році до Конвенції № 108 був

прийнятий Додатковий протокол, що стосується наглядових органів та транскордонних потоків даних. У ньому міститься вимога до всіх держав-членів РЄ надати наглядовим органам повну незалежність. Він також передбачає створення національного наглядового органу, уповноваженого слідкувати за дотриманням законодавства в сфері захисту даних та вимагати від держав, що не є сторонами Конвенції, забезпечення адекватного рівня захисту даних, що їм передаються [285]. У 1999 році були також прийняті Керівні принципи щодо захисту особистості при збиранні та обробці персональних даних на інформаційних магістралях.

У рамках ЄС захист персональних даних здійснюється на основі Директиви 95/46/ЄС «Про захист даних», Директиви 2002/58/ЄС «Про недоторканість приватного життя та електронні комунікації».

Очевидно, що європейська система захисту персональних даних і приватності не відповідала інтересам американських компаній, що діяли відповідно до стандартів саморегулювання. У зв'язку з цим виникла необхідність узгодження позицій двох ключових суб'єктів у досліджуваній сфері, що призвело до появи так званої угоди про «безпечну гавань». Уся складність полягала в тому, що згідно зі статтею 2 Директиви 95/46/ЄС «Про захист персональних даних» передача персональних даних третій країні можлива за умови, що така третя країна гарантує адекватний рівень їх захисту [286]. Таким чином, екстериторіальна спрямованість вказаної статті практично унеможливлювала передачу персональних даних з держав-членів ЄС у США, оскільки вважається, що останні не надають належного рівня захисту такої інформації.

21 липня 2000 року у відповідь на Директиву 95/46/ЄС Міністерство торгівлі США прийняло Принципи відповідності вимогам інформаційної безпеки ЄС (*International Safe Harbor Privacy Principles*), запропонувавши компаніям дотримуватися їх [287]. У Рішенні Європейської Комісії 2000/520/ЄС визнається, що ці принципи забезпечують необхідний захист [288]. Крім того, з метою гармонізації було створено механізм затвердження міжнародними корпораціями спеціальних, єдиних корпоративних правил обробки даних. Таким чином, угода про «безпечну гавань», будучи інструментом «м'якого» права, донедавна залишалася найбільш ефективним механізмом регулювання співпраці США та ЄС у сфері захисту персональних даних.

Наразі відсутнє універсальне регулювання питань конфіденційності. Разом з тим, 89 країн світу мають чинні закони про приватність чи захист персональних даних. Більшість з них регулюють питання міжнародних обмінів даними у якості механізму захисту недоторканості приватного життя фізичних осіб та забезпечення виконання національної політики. Так, у Сполученому Королівстві суди звузили поняття персональних даних порівняно з іншими європейськими країнами, зазначивши, що такі дані повинні бути значною мірою біографічними та стосуватися конкретної фізичної особи, а не будь-якої іншої людини, угоди чи заходу.

У Франції Національна комісія з питань обробки даних застосовує попереджувальні заходи для забезпечення виконання Закону про обробку даних, файли даних та індивідуальні свободи. Комісія опублікувала керівництво щодо законної обробки персональних даних, яке зобов'язує контролерів даних виконувати вимоги щодо надання повідомлень та співробітництва, а також щодо забезпечення безпеки персональних даних та в окремих випадках отримувати попередню санкцію Комісії на обробку таких даних.

У Німеччині персональні дані повинні бути отримані безпосередньо від суб'єкта даних, за винятком тих випадків, коли дані вимагаються відповідно до закону в дійсних комерційних цілях або коли для отримання даних безпосередньо від суб'єкта вимагаються невиправдано великі зусилля та відсутні підстави вважати, що при цьому постраждають інтереси суб'єкта. Крім того, у Федеральному законі про захист даних особлива увага приділяється розробці систем захисту даних, спрямованих на мінімізацію об'ємів оброблюваних персональних даних, зокрема шляхом надання суб'єкту даних анонімного статусу чи використання псевдонімів [289].

Відповідно до Патріотичного акту США дозволяється спільне використання персональних даних будь-якого підозрюваного у причетності до тероризму чи відмивання грошей. Внаслідок такого законодавчого припису стало можливим отримання широкого доступу до персональної інформації та обміну нею. Верховний суд США визнав право на конфіденційність, посилаючись на Конституцію США, незважаючи на те, що на конституційному рівні відсутнє закріплення аналогічного права. Положення про захист конфіденційності містяться у конституціях багатьох штатів. Лише Каліфорнія розширила сферу захисту даних з виключно державного на приватний сектор.

У Канаді Хартія прав і свобод містить право «на захист від необґрунтованих обшуків та накладення арешту на майно», яке згодом було розширене судами до права на захист «розумного сподівання фізичної особи на недоторканість приватного життя». Канадські закони не обмежують міжнародну передачу персональних даних, однак відповідальність за таку передачу покладається на сторону, що розкриває дані.

В Україні забезпечення приватності кожного закріплене статтями 31 та 32 Основного закону. Так, кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо. Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. 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. 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 інформації [290]. Крім того, у статті 3 Цивільного кодексу України йдеться про неприпустимість свавільного втручання у сферу особистого життя людини [291]. Спеціальним законом, що регулює правовідносини у сфері захисту і обробки персональних даних осіб та спрямований на забезпечення права на невтручання в особисте життя, є Закон України «Про захист персональних даних».

У Бразилії спеціальні закони про захист даних наразі не прийняті, хоча в її Конституції закріплені основні права на конфіденційність та таємницю листування. У Цивільному кодексі відображено положення про те, що фізична особа може просити про допомогу у зв'язку з будь-якою загрозою її правам. Приватне життя визнається недоторканим. Широкий захист надає також Кодекс захисту прав споживачів. Він, зокрема,

передбачає права споживачів на доступ до будь-яких зареєстрованих персональних даних та на внесення змін до них.

Спеціальні закони відсутні і в Південній Африці, втім право на конфіденційність знайшло відображення у Конституції держави. Положення щодо персональної інформації закріплені також у Законі про захист прав споживачів 2008 року та Законі про електронні комунікації та угоди 2002 року.

У Саудівській Аравії за відсутності відповідних законодавчих приписів суди керуються нормами шаріату. Відповідно до останнього деліктний позов може бути пред'явлено внаслідок завдання шкоди, спричиненої незаконним розкриттям персональної інформації фізичної особи.

В Індії відсутнє конституційне право на конфіденційність, хоча Верховний суд постановив, що принцип конфіденційності необхідно вважати складовою права на життя та особисту свободу. Збирання та обробка персональних даних регламентуються Законом про інформаційні технології 2000 року, відповідно до якого компанії повинні вживати адекватні заходи безпеки при обробці персональних даних. Крім того, при отриманні таких даних згідно з договором їх забороняється розкривати без згоди суб'єкта даних, що у протилежному випадку становитиме порушення договору.

Японія, будучи членом АТЕС, дотримується його політики конфіденційності. Збирання та використання персональних даних регламентується також Законом про захист персональної інформації. Він регулює всі види обробки даних, однак застосовується лише тоді, коли йдеться про інформацію, що належить понад 5000 фізичних осіб. Цей закон встановлює загальні вимоги до дозволів, безпеки та надання інформації, а також додаткові вимоги щодо контролю за працівниками та третіми особами, що здійснюють обробку персональних даних [292, с. 153-160].

Обмеження міжнародних потоків даних з метою захисту права на конфіденційність не може бути виправданим у сучасному світі, особливо в умовах, коли глобалізація та технологічний прогрес охоплюють все більше сфер взаємодії держав та індивідів. Лише універсальні нормативно-правові акти здатні створити ефективні регуляторні рамки у сфері захисту приватності та обміну персональними даними. Засоби захисту повинні бути пропорційними перевагам співробітництва, побудованого за принципом відкритості.

Важливо дотримуватися послідовності при виробленні національних та міжнародних підходів до регулювання досліджуваної сфери. Багатосторонній діалог повинен стати основою розробки стандартів в умовах технологічно орієнтованого та динамічного глобального середовища. Особлива увага повинна приділятися країнам, що розвиваються, для яких надзвичайно актуальним є віднаходження оптимального балансу між ухваленням відповідних правових норм та розвитком інфраструктурного потенціалу. Урегулювання потребують також питання захисту приватності та розкриття персональної інформації в цілях безпеки. Наразі фрагментованість нормативного регулювання має очевидний негативний ефект в контексті налагодження міжнародного співробітництва та забезпечення безперешкодного транскордонного обміну інформацією у глобалізованому світі. У багатьох державах та регіональних об'єднаннях уже сформувалося розуміння необхідності перегляду більшості правових актів у сфері захисту приватності та обміну персональними даними. Втім, сам процес подолання консервативності регуляторного середовища виявився надзвичайно складним завданням. Таким чином, маємо ситуацію, коли розвиток ІКТ значно випереджає спроможність міжнародного права щодо його нормативного регулювання.

У 2009 році з метою активізації міжнародної співпраці була ухвалена Мадридська резолюція щодо міжнародних стандартів у сфері приватності [293]. У документі були закладені мінімальні стандарти захисту. Визначалися основні принципи та права, забезпечення яких є запорукою ефективного захисту приватності на міжнародному рівні та спрощення міжнародного обміну персональними даними. Широке визнання отримали принципи законності та справедливості, конкретизації мети, пропорційності, якісних даних, транспарентності та відповідальності. Транскордонний обмін інформацією не включений до базових принципів, однак виділений в окремий пункт. Крім того, у тексті резолюції йдеться про створення наглядових органів та посилення співпраці і координації між державами.

Останнім яскравим прикладом конфлікту юрисдикцій у сфері захисту персональних даних є рішення Суду Європейського Союзу від 6 жовтня 2015 року. Підставою для прийняття рішення стало звернення австрійця Максиміліана Шремса спочатку до Спеціального уповноваженого з питань захисту персональних даних, а згодом до

Верховного суду Ірландії зі скаргою проти *Facebook*. Він скаржився, що *Facebook* зберігає його персональні дані на серверах у США і просив заборонити передачу своїх даних у цю країну. Позивач заявляв, що в США не гарантується належний рівень захисту персональних даних від стеження з боку державних структур. Після того, як Спеціальний уповноважений відмовився задовольнити скаргу, керуючись відсутністю необхідних повноважень, Шремс звернувся до Верховного суду. Останній передав на розгляд Суду Європейського Союзу питання про те, чи може незалежний наглядовий орган держави-члена ЄС проводити власне розслідування щодо порушення прав користувачів при передачі їх персональних даних у США [294].

У своєму рішенні Суд ЄС вказав, що висновки Комісії ЄС про належний рівень захисту персональних даних у США, відображені у згаданому вище рішенні від 2000 року, жодним чином не впливають на обов'язок спеціально уповноважених органів у державах-членах ЄС слідкувати за охороною таких даних. Більше того, рішення Комісії не є обов'язковим для цих органів. Однак, при цьому Суд також розглянув і саме рішення Комісії та визнав його недійсним. Висновки Суду базуються на тому факті, що насправді Комісія, приймаючи це рішення, не вивчала положення законодавства США на предмет охорони персональних даних. Крім того, обов'язки, взяті на себе компаніями, ніяк не впливають на дії державних органів США. У дійсності державні структури США мають можливість практично необмеженого доступу до персональних даних. Іншим аргументом Суду став той факт, що законодавством США не передбачається можливість звернення користувачів з проханням змінити їх дані чи видалити їх, якщо вони є неточними чи недостовірними. Така політика США суперечить вимогам законодавства Європейського Союзу про охорону персональних даних та забезпечення доступу до правосуддя. На підставі рішення Суду ЄС Спеціальний уповноважений Ірландії з питань захисту персональних даних розгляне питання про те, чи може *Facebook* передавати персональні дані європейських користувачів у США [295].

Рішення у даній справі створило міжнародно-правовий вакуум у сфері трансатлантичної передачі персональних даних, що, однак, був заповнений укладенням у лютому 2016 року нової угоди – «Щит конфіденційності ЄС-США» (*EU-US Privacy Shield*). Структурно документ складається з обов'язкових для компаній принципів приватності та

зобов'язань щодо забезпечення виконання угоди з боку вищих посадових осіб США. Серед позитивних досягнень нової угоди – посилення зобов'язань американських компаній щодо захисту персональних даних громадян ЄС, а також запровадження механізмів моніторингу та примусового виконання з боку Міністерства торгівлі США та Федеральної торгової комісії, у тому числі через посилену співпрацю з органами захисту персональних даних у державах-членах ЄС. Крім того, угода містить зобов'язання США щодо встановлення чітких підстав, належних гарантій та контрольних механізмів доступу американських державних органів до персональних даних, отриманих з ЄС, з метою недопущення загального, неіндивідуалізованого доступу. Передбачається запровадження кількох механізмів правового захисту порушених прав, зокрема шляхом подачі індивідуальної скарги до відповідної компанії, звернення органу захисту персональних даних зі скаргою до Міністерства торгівлі США та Федеральної торгової комісії, використання безкоштовної процедури альтернативного вирішення спорів. Крім того, буде введенно посаду омбудсмана, що займатиметься питаннями доступу до персональних даних національних розвідувальних органів. Документ буде предметом щорічного перегляду з метою приведення його у відповідність з останньою практикою трансатлантичної передачі даних [296].

Крім того, на початку вересня 2015 року Європейський Союз та США завершили переговори щодо високих стандартів захисту персональних даних у діяльності правоохоронних органів. Надзвичайно важливою визнається співпраця ЄС та США з питань боротьби зі злочинністю та тероризмом. У той же час, обмін персональними даними, такими як досьє злочинця, імена чи адреси, повинен відбуватися при суворому дотриманні норм про захист даних. Таким цілям і буде слугувати Угода про захист персональних даних у зв'язку з попередженням, розслідуванням, розкриттям чи переслідуванням кримінальних злочинів, так звана «Парасолькова угода» (*Umbrella Agreement*). Вона покликана гарантувати високий рівень захисту всіх персональних даних при їх передачі правоохоронним органам через Атлантику. Зокрема, громадяни ЄС отримають право на захист своїх персональних даних в американських судах [297].

Сам текст «Парасолькової угоди» так і не був офіційно опублікований. При цьому документ не позбавлений недоліків. Так, передача даних між органами, відповідальними за

забезпечення національної безпеки, не знайшла відображення в угоді. Передбачається чимало виключень зі сфери її регулювання. «Парасолькова угода» залишає державі можливість обійти свої закони у сфері захисту приватності шляхом отримання від іншої держави інформації, збирання якої заборонене відповідно до власного національного законодавства. Крім того, в документі варто було б прописати чіткі принципи поводження з даними в правоохоронних цілях. Ця угода є ще одним прикладом узгодження політичної волі держав через використання регуляторних засобів «м'якого» права.

24 лютого 2016 року Президент США Б. Обама підписав ухвалений Конгресом Акт про судовий захист (*Judicial Redress Act*) [298], що було необхідною передумовою завершення підписання «Парасолькової угоди». Причиною прийняття цього акту стала наполегливість ЄС в питаннях надання його громадянам тих самих прав у сфері захисту приватності та засобів судового захисту, що й громадянам США. Однак, режим захисту при цьому не стає однаковим. Відповідно до Акту про судовий захист лише окремі положення Акту про захист приватності США 1974 року будуть застосовуватися до обміну даними між правоохоронними органами ЄС та США з метою розслідування злочинів. Так, розширення сфери дії деяких норм Акту про захист приватності можливе лише по відношенню до держави, що уклала зі США угоду про належний захист даних у кримінальних справах, як у випадку з «Парасольковою угодою». Альтернативною передумовою є активний обмін даними з відповідними органами США з метою попередження, розслідування чи кримінального переслідування злочинів. Для цього буде створений спеціальний список країн, що відповідають вимогам американського законодавства. Міністр юстиції США може виключити будь-яку країну з цього списку, якщо буде встановлено, що вона порушує домовленість по типу «Парасолькової угоди», приховує дані або перешкоджає передачі інформації в США приватними компаніями чи окремими фізичними особами.

Крім того, положення Акту про захист приватності не будуть застосовуватися до персональних даних громадян інших держав, якщо такі дані були зібрані органами США за власною ініціативою, навіть якщо вони використовуються в цілях розслідування чи переслідування злочинів. Поза сферою дії Акту залишаються також розвідувальні дані. Але ж обмін даними далеко не обмежується правоохоронними цілями. Уважне вивчення Акту

про судовий захист дає зрозуміти, що громадянам ЄС надається значно менше можливостей для судового захисту своїх прав. Безумовно, «Парасолькову угоду» складно назвати комплексним нормативним актом, тим не менше у ній робиться важлива спроба узгодження двох традиційно протилежних режимів захисту персональних даних.

15 грудня 2015 року в ЄС було погоджено пакет реформування сфери захисту персональних даних, що передбачає затвердження Регламенту про захист персональних даних та Директиви про захист персональних даних у сфері співпраці поліцейських та судових органів [299]. Реформа у сфері захисту персональних даних повинна посприяти формуванню єдиного цифрового ринку, що є пріоритетним напрямком діяльності Європейської Комісії. Передбачається введення єдиних правил захисту персональних даних у рамках ЄС, а також запровадження чітких та зрозумілих правил передачі персональних даних третім країнам. Задля цього Регламент містить деталізовані положення щодо оцінки Європейською Комісією належного рівня захисту, передбаченого законодавством третіх країн. Крім того, передбачається періодичний, принаймні кожні чотири роки, перегляд Комісією рішень щодо відповідності законодавства третіх країн праву ЄС. Регламент надає громадянам можливість більшого контролю за своїми персональними даними та спрощує регуляторне середовище для компаній. Іноземні компанії, що засновані в третій країні та надають послуги в Євросоюзі, будуть зобов'язані підпорядковуватися законам останнього. Національні органи із захисту персональних даних отримують право накладати санкції на іноземні компанії за недотримання законодавчих приписів ЄС при здійсненні діяльності в межах його території. Згідно з Директивою будуть застосовуватися гармонізовані правила міжнародної передачі персональних даних з метою полегшення правозастосування у кримінальній сфері. Офіційне затвердження пакету реформ Європейським парламентом та Радою очікується у першому півріччі 2016 року, після чого передбачається двохрічний перехідний період для набрання чинності новими правилами.

Отже, основна проблема сучасного нормотворення у досліджуваній сфері зводиться до балансування між доволі суперечливими інтересами ключових зацікавлених сторін. Так, приватний сектор зацікавлений у вільному потоці інформації. Індивіди теж отримують безперечні переваги від такого безперешкодного обміну інформацією, втім прагнуть зберегти ефективний контроль над передачею своїх персональних даних. Нормативно-

правове регулювання у сфері захисту приватності та вільного потоку інформації повинне, в першу чергу, враховувати технологічну складову. Можливості розвитку не повинні гальмуватися в силу надмірності правових приписів, адміністративних бар'єрів чи конфлікту юрисдикцій. Нормативно-правове регулювання повинно бути максимально сприятливим для приватного сектору, оскільки саме останній продукує та акумулює прибутки внаслідок використання досягнень сучасних ІКТ. У той же час, повинні бути враховані інтереси самих суб'єктів персональних даних, оскільки йдеться про передачу інформації, що безпосередньо стосується їх повсякденного життя. Крім того, часто запроваджуючи непропорційні обмеження для приватних компаній, держави залишають за собою право витребувати від останніх персональні дані фізичних осіб та використовувати їх на власний розсуд. За таких умов не доводиться говорити про ефективність державного регулювання досліджуваної сфери.

Європейський підхід традиційно ґрунтується на географічній прив'язці. Він покликаний попередити ризики, що можуть виникнути у зв'язку з передачею персональних даних до певної країни. Відповідно держава, до якої експортуються дані з ЄС, повинна надати їм належний рівень захисту. Європейську модель запозичили також Аргентина, Марокко та Росія. Натомість Канада та держави-члени АТЕС відмовилися від географічної прив'язки та покладають обов'язок охорони персональних даних на суб'єкта, що здійснює їх передачу.

Не менш складним залишається питання про право, застосовне до правовідносин, що виникли внаслідок порушення приватності чи неправомірного поводження з персональними даними. Навіть в рамках самого ЄС існує чимало нормативних приписів, що втрачають свою ефективність при регулюванні правовідносин, ускладнених технологічною складовою. Так, у Регламенті Рим II про право, застосовне до недоговірних зобов'язань закріплюється прив'язка до права держави, в якій настали наслідки прямої шкоди. Практичне застосування цього принципу ускладнюється тим, що негативні наслідки, пов'язані з використанням сучасних ІКТ, як правило, ніколи не обмежуються територією однією держави. Відтак, виникає конфлікт юрисдикцій та невизначеність щодо того, який правопорядок повинен вважатися компетентним у кожному конкретному випадку. В умовах глобальності та універсальності Інтернету територіальна прив'язка

втрачає свою ефективність у її теперішньому розумінні та потребує перегляду.

Еволюція регіональних міжнародно-правих режимів захисту персональних даних демонструє високий рівень адаптивності міжнародного права до розвитку глобального інформаційного суспільства. Вкотре підтверджується первинність правозастосовної практики та авторитет судових рішень, що стали підставою перегляду договірної основи співробітництва США та ЄС у сфері поводження та обробки персональних даних. Їх приклад свідчить про те, що вироблення універсального міжнародно-правового регулювання сфери захисту персональних даних можливе лише за умови застосування єдиної системи цінностей (напр., пріоритет безпеки чи вільного обміну інформацією), відмови від категоричності формулювань та надання мінімальних обов'язкових гарантій. Ухвалення єдиних стандартів обробки та передачі персональних даних дозволить усунути нормативні бар'єри на шляху до вільного потоку інформації, що є одним із основних принципів глобального інформаційного суспільства. Локалізація чи навіть регіоналізація регулювання з питань глобального інформаційного суспільства, по суті, є штучною перешкодою для прогресивного розвитку міжнародного права. Втім, як свідчить приклад сфери захисту персональних даних, еволюція міжнародного права продовжує відбуватися за класичною схемою трансформації регіональних режимів в універсальні. При цьому логічним було б уникати надлишкової і, як правило, обмежувальної нормативної активності та розробляти універсальне, глобальне регулювання для правовідносин глобального характеру в інформаційній сфері.

Зрештою, останній акцент у нашому дисертаційному дослідженні зробимо на питаннях безпеки у кіберпросторі. Безпека є необхідною передумою стабільності та передбачуваності розвитку глобального інформаційного суспільства. Роль міжнародного права полягає, відповідно, у створенні ефективних нормативних рамок та закріпленні належних гарантій як безпеки інфраструктури, так і безпеки самих правовідносин, що виникають в інформаційній сфері.

3.3. Міжнародно-правовий режим безпеки кіберпростору

У наш час кіберпростір відіграє вирішальну роль у забезпеченні благополуччя

населення, підтриманні політичної незалежності та територіальної цілісності держав. Інтернет розширює можливості людини, але в той же час містить у собі величезні загрози самому її існуванню. Сучасні інформаційно-комунікаційні технології у випадку недобросовісного та умисно шкідливого їх використання можуть призвести до катастрофічних наслідків глобального масштабу. Сучасний світ завдяки розвитку все тих же ІКТ являє собою надзвичайно тісно внутрішньо взаємопов'язаний механізм. Небезпека полягає у тому, що ризики та загрози розвиваються непропорційно швидко у порівнянні із засобами та механізмами протидії їм. Залежність повсякденного життя, науки, механізмів управління від автоматизованих систем підвищує їх вразливість до кібератак. Кіберзлочинність та кібертероризм загрожують мирному існуванню людства та використанню кіберпростору у суспільно корисних цілях. У зв'язку з чим вкрай актуальним постає питання міжнародного співробітництва з метою забезпечення кібермиру та підтримання кіберстабільності на основі норм та принципів міжнародного права.

Інформаційно-комунікаційні системи та мережі покладено в основу національної безпеки та економічної стабільності більшості держав світу. На них також базується робота бізнес структур та державних органів. Інформаційна інфраструктура відіграє важливу роль у сферах громадського здоров'я, безпеки та соціального забезпечення. Порушення рівноваги у кіберпросторі може призвести до серйозних збоїв та неполадок у життєво важливих сферах існування людини.

Сучасне суспільство користується перевагами глобального інформаційного простору, разом з якими приходять загрози кібератак, що можуть виникнути у будь-якому місці, в будь-який час та спричинити величезні збитки. Розмір збитків зростає за рахунок взаємозв'язку інформаційно-комунікаційних технологій з життєво важливими національними інфраструктурами.

Наразі межа між миром та війною у кіберпросторі не має чітких контурів. У той же час, захист мережевої інфраструктури є одним із ключових пріоритетів у сфері національної безпеки. Кіберпростір може використовуватись з метою завдання терористичного удару або ведення атаки, яка за своїми масштабами не поступатиметься звичайній військовій атаці. Втім, відсутні будь-які спеціальні

міжнародні договори, які б врегульовували дані питання. Розробка міжнародної конвенції з питань кіберпростору повинна стати ключовим пріоритетом міжнародного співтовариства.

Використання кіберпростору у цілях шпигунства та військових атак є предметом постійного та все зростаючого інтересу з боку збройних сил та розвідувальних служб різних держав. Здійснення усіх широкомасштабних атак приписують державам. Тим не менше, сама природа кіберпростору значно ускладнює можливості для виявлення виконавців таких атак. Такий стан речей створює серйозну загрозу для кібербезпеки і одночасно відкриває майже безмежні можливості для здійснення електронних атак.

Кібератаки стали невід'ємною складовою арсеналу зброї, що використовується на сучасному полі бою, розуміння якого зазнало значних трансформацій у XXI столітті. Останнім часом усе міжнародне співтовариство було свідком зростаючого числа загроз та підвищеної вразливості кіберпростору. Поширеною стала думка про те, що більшість збройних конфліктів у цифрову еру зачіпатимуть мирні відносини у кіберпросторі. Атаки у кіберпросторі мають далекосяжні наслідки й у реальному світі.

Протистояння між Росією та Грузією у 2008 році вперше продемонструвало одночасне використання традиційної та кіберзброї у міждержавному конфлікті. Після цього випадку повноцінного міжнародного збройного конфлікту багато кризових ситуацій містили кіберкомпонент.

Так, слід згадати комп'ютерний вірус *Stuxnet*, який у 2010 році атакував електростанцію та інші промислові об'єкти та значно сповільнив ядерну програму Ірану, вірус *Duqu*, який у 2011 році був спрямований проти комп'ютерних систем Ірану та, серед іншого, збирав інформацію про промислові системи країни, а також вірус *Flame*, який роком пізніше був запущений проти тієї ж іранської ядерної програми.

У відповідь на терористичні атаки 11 вересня 2001 року США оголосили війну проти тероризму, при цьому вони використовували традиційну зброю проти асиметричної загрози. Одночасно експерти з питань безпеки почали наголошувати

на тому, що інформаційні технології можуть також бути використані для здійснення атаки, яка за своїми наслідками не поступатиметься традиційному збройному конфлікту. Так само, як і у випадку з терористичним організаціями, традиційні правові норми, що регулюють збройний конфлікт, важко застосувати до кібератак. У той же час, не викликає сумнівів необхідність захисту електронних мереж, що є складовою частиною інфраструктури держави.

Для України питання кібербезпеки набули особливої актуальності в контексті триваючої агресії Російської Федерації, що супроводжує та посилює наслідки «традиційної» військової агресії. Досвід нашої держави яскраво продемонстрував, що неготовність до інформаційного протистояння та відсутність відповідного кіберпотенціалу можуть мати катастрофічні наслідки для держави, її суверенітету та територіальної цілісності.

Деякі держави уже заявили, що вони готові відбити найбільш складні кібератаки за допомогою традиційних військових озброєнь. Зокрема, аналогічне положення міститься в Стратегії з кіберпростору США від 2011 року. У Польщі було розроблено офіційну урядову програму з питань кібербезпеки на 2011-2016 роки. Поняття «кібератака» зустрічається також у стратегічних документах інших країн, включаючи Сполучене Королівство, Канаду, РФ. Спеціальні кіберпідрозділи було створено у США, Ізраїлі та КНР. Кіберпростір є середовищем без кордонів, що становить інтерес для всього людства. Тому він потребує відповідного міжнародно-правового регулювання.

Міжнародне право ще не виробило універсального поняття кібервійни, що породжує суперечності з приводу того, з якого моменту атаку слід вважати актом кібервійни: як вона починається та закінчується, як відбувається, а також імовірні правові наслідки. Тим не менше, ключова ідея, що лежить в основі дискусії з питань кібервійни, зводиться до забезпечення кібербезпеки в умовах невідповідної інфраструктури, недостатнього фінансування, нестачі людських ресурсів, застарілих методів національної політики та відсутності належного нормативно-правового забезпечення як на державному, так і на міжнародному рівні.

Основними цілями кібератак стають стратегічні інфраструктури країн

(ядерна, хімічна чи будь-яка інша промисловість, системи життєзабезпечення великих мегаполісів, фінансова, продовольча, енергетична національні системи, транспортні мережі, діяльність уряду, правоохоронних органів, армії тощо). Удари завдаються через інформаційно-телекомунікаційні системи, особливо, автоматизовані системи управління, які необхідні для функціонування повсякденного життя людей, структур економіки чи органів влади. Особливе місце в системі критичної інфраструктури сучасної держави займає інформаційна інфраструктура, ефективний захист якої виступає необхідним елементом забезпечення її національної безпеки.

Вважається, що концепція критичної інформаційної інфраструктури була сформульована та детально розроблена у США [300]. Переліки критично важливих інфраструктур є неоднаковими в різних країнах і визначаються у відповідності до традицій, суспільних та політичних уподобань, а також географічних та історичних особливостей кожної держави [301]. У Росії, як і в Україні, немає офіційного документа, який би визначав перелік критичних інфраструктур або напрями забезпечення їх безпеки.

Статут ООН визнає невід'ємне право на самооборону у випадку збройної атаки, яке може бути реалізоване до тих пір, доки Рада Безпеки ООН не застосує заходи для відновлення міжнародного миру та безпеки. Якщо кібератака загрожує безпеці держави, але ще не є атакою у розумінні статті 51 Статуту ООН, така держава може звернутися до Ради Безпеки з проханням втрутитися та застосувати санкції. Очевидно, що такий підхід є виправданим у випадку масштабних кібератак.

У той же час, деякі вчені стверджують, що якщо розглядати кіберпростір перш за все як простір для спілкування та ведення економічної активності, міжнародне право щодо використання сили виявляється повністю непридатним для регулювання питань кібербезпеки. Підходящим правом є право, що закріплює економічні права та право на невтручання, а не право самооборони. Хибність військової парадигми для кіберпростору полягає також у тому, що більшість вчених-міжнародників, які займаються питаннями кібербезпеки, з самого початку зародження Інтернету працювали у військовій сфері чи мали з нею тісні зв'язки. Український вчений І.

Забара у складі міжнародної інформаційної безпеки виділяє кримінальний, терористичний та військовий елементи [302, с. 70].

Той факт, що кібератака чи кібершпигунство не є збройним нападом ще не означає, що міжнародне право не містить норм, які б регулювали це питання. Втручання у сферу економіки держави, повітряний, морський чи територіальний простір, навіть у випадку відсутності міжнародного договору, який би забороняв таке втручання, не допускається відповідно до загального принципу невтручання. Даний принцип відображено у ряді міжнародних договорів, резолюціях ООН та рішеннях Міжнародного Суду ООН. Міжнародне право створює значні бар'єри для використання кіберзброї та захисту кіберпростору від кібератак за допомогою сили. У цілому, міжнародне право спрямоване на регулювання кіберпростору як економічної та комунікаційної сфери та має у своєму арсеналі засоби правомірного реагування на кіберпровокації будь-якого характеру. Примусові міри, що є правомірними у випадку економічних правопорушень та порушень угод про контроль над озброєнням, будуть також визнаватися правомірними у випадку кібератаки. У економічній сфері відповідь на порушення носить назву контрмір, у сфері контролю над озброєнням – санкцій [303].

Кіберзлочинність стає надзвичайно прибутковим видом злочинної діяльності. Злочини у кіберпросторі можуть стати ще більш небезпечними, враховуючи той факт, що ІКТ все частіше використовуються з метою контролю та моніторингу за критичними інфраструктурами, а держави стають все більше залежними від таких структур.

Чимало питань виникає щодо застосовності міжнародного гуманітарного права до регулювання правовідносин, пов'язаних з кіберзагрозам, кібератаками, кібервійною та кібертероризмом. Тут слід зауважити, що наразі відсутній єдиний підхід до тлумачення цих понять, що викликає труднощі вже на етапі кваліфікації відповідних діянь та пошуку ефективних регулівних механізмів. Правомірність звернення до самооборони та застосування збройної сили у відповідь на кібератаку встановлюється на основі принципів необхідності та пропорційності у кожному конкретному випадку. Таким чином, цілком очевидно, що кібератака, спрямована на критичну інфраструктуру держави, може бути визнана актом збройної агресії, що викличе відповідну реакцію з використанням традиційної зброї. Однак, свобода держав у веденні військових дій у кіберпросторі не є абсолютною. Держави як суб'єкти кіберпростору повинні дотримуватися певних правил, хоча наразі таким правилам ще бракує досконалості.

Зрештою, праву самооборони повинна відводитися незначна роль при обговоренні питань кібербезпеки. Навіть у випадку, коли кіберінцидент повністю підпадатиме під визначення збройної атаки, відповідь на таку атаку навряд чи буде правомірною чи розумною, якщо у якості контрмір застосовуватиметься сила. Наголос слід робити на невійськових методах подолання небезпек та атак у кіберсередовищі.

У розумінні міжнародного гуманітарного права кібероперація може бути визнана збройним конфліктом залежно від її руйнівних наслідків. При цьому, розуміння шкоди не обмежується виключно фізичними пошкодженнями, а поширюється також на випадки виведення з ладу об'єктів та порушення їх нормального функціонування [304]. Це відповідно тягне за собою серйозні наслідки. Гуманітарне право визначає захищені категорії осіб та майна в ході військових дій. Серйозні порушення законів, що застосовуються при збройному конфлікті, можуть призвести до індивідуальної кримінальної відповідальності окремих осіб за військові злочини. Так, незаконну кібератаку на об'єкти цивільної інфраструктури, що знаходяться під захистом, наприклад лікарні, слід розглядати як військовий злочин, а винні особи повинні бути притягнені до відповідальності, у тому числі

через Міжнародний кримінальний суд.

Пріоритетним завданням міжнародного права та ООН є підтримання міжнародного миру та безпеки, уникнення випадків їх порушення. Для того, щоб військове реагування на кібератаку було виправданим, необхідне дотримання кількох умов: атака має бути значною; вона повинна бути спрямована проти тієї держави, що застосовує міри самооборони; застосування сили повинно відбуватися в останню чергу та з великою вірогідністю повинно сприяти успішній обороні; таке застосування сили повинно бути необхідним та пропорційним завданій шкоді. На практиці дотримання усіх цих умов є неможливим, оскільки кібератаки здійснюються анонімно та дуже складно відслідковуються. Міжнародне право містить значні бар'єри на шляху до використання кіберзброї та захисту кіберпростору від кібератак через застосування сили.

Нагальною є потреба у прийнятті багатосторонньої конвенції з питань кіберпростору. Розробка чітких правових принципів, спрямованих на регулювання поведінки держав у кіберпросторі, відповідає інтересам усього міжнародного співтовариства. Зокрема, визначення потребують законні об'єкти для кібератаки, момент початку воєнних дій у кіберпросторі, захищені особи та об'єкти, заборонені види діяльності. Дана робота ведеться в рамках Міжнародного Комітету Червоного Хреста, Комісії з міжнародного права, НАТО та ЄС [305, с. 2].

У ході дослідження було виявлено відсутність єдиного підходу до вироблення універсального міжнародно-правового режиму безпеки у кіберпросторі. Так, США традиційно обмежувалися концепцією боротьби з тероризмом, а Європа зосередилася на кримінальних аспектах проблеми. Фрагментація правового регулювання сама по собі становить серйозний виклик міжнародній кібербезпеці. Досі складно було говорити навіть про наявність прагнення держав світу до вироблення універсального документу щодо кібербезпеки, що поступово призвело до регіоналізації відповідних обговорень. Саме тому нижче пропонуємо розглянути найбільш ефективні ініціативи щодо захисту критично важливої інфраструктури та забезпечення кібербезпеки, що були погоджені в рамках різних інтеграційних об'єднань. При проведенні аналізу спробуємо дотриматися справедливого

регіонального представництва та представити передові практики у досліджуваній сфері. Загалом 82 держави світу підписали або ратифікували хоч якийсь з обов'язкових до виконання документів з питань кіберзлочинності.

Резолюції Генеральної Асамблеї ООН 57/239 «Створення глобальної культури кібербезпеки» 2002 року [306] та 58/199 «Створення глобальної культури кібербезпеки та захист найважливіших інформаційних інфраструктур» 2003 року [307] є основними документами ООН, присвяченими питанню кібербезпеки. Вони наголошують на необхідності міжнародної співпраці у боротьбі з кіберзлочинністю. Технологічна відсталість окремих держав розглядається як гальмівний фактор вироблення універсального міжнародно-правового режиму безпеки у кіберпросторі. Резолюція ГА ООН 64/211 «Створення глобальної культури кібербезпеки та оцінка національних зусиль щодо захисту найважливіших інформаційних інфраструктур» 2009 року пропонує добровільний механізм самооцінки національних зусиль щодо захисту найважливіших інформаційних інфраструктур, а також заохочує держави оновлювати списки відповідних правових органів. Проблема кіберзлочинності обговорювалася також на кількох конгресах ООН щодо попередження злочинів та кримінального правосуддя.

У відповідь на ініціативу Росії щодо вирішення на міжнародному рівні питання забезпечення міжнародної інформаційної безпеки Генеральна Асамблея ООН щорічно, починаючи з 1998 року, публікує резолюцію «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки». Ухвалення резолюції стало свідченням визнання міжнародним співтовариством факту існування проблеми забезпечення інформаційної безпеки, а дане питання було включене в робочий план ГА ООН. У цей же період був запропонований проект Принципів міжнародної інформаційної безпеки, що фактично міг перетворитися на кодекс поведінки держав в інформаційному просторі. З метою практичного вирішення питань у сфері інформаційної безпеки у 2004 році була створена Група урядових експертів ООН. Глобальна програма кібербезпеки, прийнята Міжнародним союзом електрозв'язку у 2007 році, складається з п'яти основних елементів, зокрема нормативно-правової бази, технічних заходів, організаційних

структур, нарощування потенціалу та міжнародної співпраці [308]. МСЕ володіє мандатом на надання допомоги країнам, що розвиваються в контексті розробки законодавчих заходів щодо захисту від кіберзагроз. У рамках МСЕ було ухвалено ряд резолюцій, присвячених питанням кібербезпеки.

Понад 140 урядів та представників бізнес кіл беруть участь в ініціативі МСЕ та Міжнародного багатостороннього партнерства проти кіберзагроз, у рамках якого організовано Глобальний центр реагування, що забезпечує раннє попередження про кіберзагрози та надає підтримку у врегулюванні інцидентів. При технічній підтримці МСЕ та Форуму груп реагування на інциденти та забезпечення безпеки були створені національні групи реагування на інциденти у сфері комп'ютерної безпеки. Крім того, МСЕ публікує щорічний Глобальний індекс кібербезпеки, у якому дається оцінка потенціалу держав у контексті забезпечення кібербезпеки.

Порівняно нещодавно з'явилася ідея створення автономного миротворчого контингенту для кіберпростору в рамках ООН у цілях боротьби із все зростаючою кількістю кібератак. Це є свідченням високої важливості кібероперацій у системі миротворчих операцій ООН [309].

У 2013 році Група урядових експертів ООН представила доповідь «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки». У документі зазначалося, що «…всі держави зацікавлені у заохоченні використання ІКТ в мирних цілях. Держави також зацікавлені у попередженні конфліктів, що виникають у результаті використання ІКТ. Загальне розуміння норм, правил та принципів, що застосовуються державами у контексті використання ІКТ, та добровільні заходи зміцнення довіри можуть відігравати важливу роль у підтриманні миру та безпеки» [87].

Значна робота у сфері забезпечення кібербезпеки здійснюється Європейським Союзом. Так, у 2001 році Європейська комісія опублікувала повідомлення на тему «Створення безпечного інформаційного суспільства, підвищення безпеки інформаційних структур та боротьба з комп'ютерною злочинністю», у якому наголошувалося на необхідності забезпечення цілісності, доступності та надійності інформаційних систем та мереж. У цьому ж році Комісія видала комюніке «Мережа

та інформаційна безпека», відповідно до якого гармонізація законодавства у сфері боротьби з кіберзлочинністю визнавалася одним із пріоритетних напрямків правотворчої діяльності ЄС. Крім того, була прийнята Рамкова угода про боротьбу з шахрайством та підробкою негрошових платіжних засобів, що зачіпає питання вчинення цих злочинів з використанням комп'ютерів та спеціальних програм.

У 2004 році було створено Європейське агентство мережевої та інформаційної безпеки. Тоді в рамках ЄС почали активно обговорюватися питання захисту інфраструктури. У 2009 році з метою обміну інформацією було засновано Державно-приватне партнерство для підвищення сталості. У серпні 2013 року була оновлена Європейська програма захисту критично важливої інфраструктури та виділено три напрямки роботи: попередження, підвищення готовності та реагування. Цього ж року було прийнято Директиву про атаки на інформаційні системи, що доповнила правову основу боротьби з кіберзлочинністю в ЄС. 2013 рік ознаменувався прийняттям Стратегії кібербезпеки ЄС.

У грудні 2015 року, після двох років обговорень, було ухвалено проект Директиви ЄС «Про мережеву та інформаційну безпеку» [310]. Навесні 2016 року очікується остаточне затвердження тексту директиви Європарламентом та Радою ЄС. Після опублікування директиви держави-члени ЄС матимуть 21 місяць для її імплементації у національне законодавство та приведення в дію, а також 6 додаткових місяців для встановлення переліку операторів необхідних послуг у межах своєї території. Директивою передбачається вжиття відповідних заходів операторами критичної інфраструктури та провайдерами цифрових послуг з метою захисту мереж та даних від кіберінцидентів, мінімізації ризиків, а також повідомлення про найсерйозніші з них відповідним національним регуляторним органам. Діяльність операторів критичної інфраструктури є особливо активною у таких важливих секторах, як енергетика, транспорт, медицина та фінанси. Цифрові послуги охоплюють онлайнові ринки, пошукові системи та хмарні сервіси. Більш суворі вимоги передбачені для операторів критичної інфраструктури, що пов'язано з непропорційно великою шкодою, яка може бути завдана суспільству та економіці держави внаслідок порушення функціонування критичної інфраструктури. На

виконання директиви держави-члени ЄС повинні будуть ухвалити відповідні стратегії кібербезпеки та створити один чи кілька національних органів, відповідальних за координацію національної політики у цій сфері, а також групи швидкого реагування на інциденти, пов'язані з комп'ютерною безпекою (*Computer Security Incident Response Teams - CSIRTs*). Фактично, директива охоплює доволі значне коло приватних суб'єктів та встановлює обов'язкові рамки їх взаємодії з державними структурами з питань інформаційної безпеки, що свідчить про тенденцію до централізації. У той же час, директива є рамковим документом, що відображає компромісне рішення держав, які так і не змогли досягти згоди щодо конкретного переліку операторів, створивши тим самим передумови для подальшої фрагментації правового регулювання у сфері інформаційної безпеки. Подібний підхід негативно відобразиться на діяльності транснаціональних компаній, що мають представництва у кількох державах-членах ЄС, де відтепер вони можуть стати об'єктом різних регуляторних вимог у контексті забезпечення мережевої та інформаційної безпеки.

В ЄС розроблена також Інформаційна мережа попередження критично важливих інфраструктур, що спрямована на обмін ідеями, дослідженнями та передовим досвідом між державами-членами ЄС та їх установами. На виконання Цифрового порядку денного для ЄС під керівництвом Європейського агентства мережевої та інформаційної безпеки проводяться загальноєвропейські навчання кібербезпеки, у ході яких перевіряються системи забезпечення безпеки критично важливої інфраструктури на всій території ЄС. Крім того, були визначені мінімальні базові можливості, послуги та політичні рекомендації, необхідні для ефективного функціонування національних груп швидкого реагування на комп'ютерні інциденти.

Один із ключових документів у сфері кібербезпеки був розроблений у 2001 році в рамках Рада Європи та отримав назву Конвенції про кіберзлочинність. Остання набрала чинності у 2004 році, втім не була підписана та ратифікована, зокрема, Росією. Серед держав, що не є членами РЄ, Конвенцію ратифікували, зокрема, Канада, Японія та США. Станом на квітень 2016 року Конвенцію підписали лише 54 держави, шість з яких досі не ратифікували її [311]. Основним

предметом суперечок є небажання держав забезпечити безперешкодний доступ на свою територію правоохоронним органам інших країн. Таке небажання обґрунтовується тим, що подібна діяльність правоохоронних органів призведе до порушення державного суверенітету. Однак, надмірна територіальна прив'язка розслідування злочинів у кіберпросторі робить дану Конвенцію вкрай неефективним правовим інструментом. Розвиток ІКТ за останні 15 років пішов далеко вперед, і норми Конвенції більше не відповідають тим викликам, що існують у сфері забезпечення безпеки у кіберпросторі. Це свідчить про необхідність перегляду конвенційного механізму. Негативним фактором є також нехтування інтересами країн, що розвиваються та обмеження їх права на участь в обговореннях щодо внесення поправок до Конвенції. А приєднання до Конвенції потребує одностайної згоди держав-учасниць.

НАТО долучилася до захисту критично важливої інфраструктури у 2001 році. У 2006 році глави держав та урядів підтвердили роль Альянсу щодо захисту критично важливої інфраструктури в контексті охорони населення, території, інфраструктури та збройних сил країн-учасниць від наслідків терористичних атак, а також з метою захисту власних інтересів безпеки від переривання потоку життєво важливих ресурсів.

У відповідь на кібератаки в Естонії у 2007 році Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), Шанхайська організація співробітництва (ШОС) та НАТО заснували Спільний центр передового досвіду з кіберзахисту у Таллінні. А вже у новій Стратегічній концепції НАТО 2010 року йшлося про необхідність формування потенціалу з метою виявлення, попередження та захисту від кібератак, а також створення єдиної системи інформаційної безпеки всіх структур Альянсу [312]. Відповідно до концепції кібернетичної оборони НАТО ефективний захист кіберпростору повинен складатися з трьох взаємопов'язаних напрямків: розвиненої міжнародної співпраці, розробки коаліційної політики та посилення оборонного потенціалу у кіберпросторі.

У березні 2013 року з ініціативи Спільного центру передового досвіду з кіберзахисту був опублікований Талліннський посібник щодо міжнародного права,

яке застосовується до кібервійни [313]. Документ неофіційний і саме тому становить неабиякий інтерес. Фактично, посібник є найбільш комплексним експертним міжнародно-правовим аналізом військової складової кіберпростору, що охоплює як сферу *jus ad bellum*, так і питання *jus in bello*. Принципи ведення кібервійни об'єднані в 95 правил, кожне з яких детально описане. Серед правил є умови фізичної атаки на супротивника та перетворення цивільних об'єктів на військові тощо. Посібник детально розглядає юридичні проблеми, пов'язані з правом збройних конфліктів у кіберпросторі. Принципи, що містяться у ньому, можуть оформити юридичні рамки для військових дій у кіберпросторі, оскільки рекомендації, що покладені в основу документу, швидше за все будуть взяті до уваги при розробці національного законодавства із зазначеного питання. Основним досягненням посібника є те, що він вказує на прогалини у міжнародному праві, зокрема, щодо того як уникнути атак у кіберпросторі та з якого моменту відраховувати початок воєнних дій. Талліннський посібник наголошує на необхідності прийняття якісно нових міжнародно-правових норм, оскільки вже існуючі не враховують нових кіберобставин, хоча в окремих випадках можуть бути застосовані за аналогією.

Наразі відбувається процес обговорення Таллінського посібника 2.0, що охопить також питання застосування міжнародного права до кіберпростору в мирний час. Зокрема аналізуються такі питання, як права людини, дипломатичне право, відповідальність міжнародних організацій, право міжнародних телекомунікацій та мирні операції. Друга, розширена версія посібника вже не є виключно академічним дослідженням. У ній містяться посилання на відповідні міжнародно-правові документи та їх практичне застосування до кіберпростору. Відмінною рисою підготовчого процесу є так званий Гаазький процес, тобто залученість держав до обговорень в рамках експертної групи, що свідчить про зростаючу значимість Таллінського посібника. У тексті Посібника знаходять відображення ті норми поведінки у кіберпросторі, що на думку експертів є звичаєвою нормою міжнародного права. Остаточне затвердження документу очікується у другій половині 2016 року.

У квітні 2015 року НАТО задовольнила прохання України про надання допомоги у розробці планів дій у надзвичайних ситуаціях та антикризових заходів. З цією метою в Україну була направлена Консультативна група підтримки НАТО щодо захисту критично важливої інфраструктури та цивільного населення.

ОБСЄ вперше проявила інтерес до питань кібербезпеки ще у 1983 році, провівши дослідження щодо можливості міжнародної гармонізації кримінального законодавства з метою подолання комп'ютерної злочинності. У 2002 році були ухвалені Керівні принципи щодо забезпечення безпеки інформаційних систем і мереж, що лягли в основу культури кібербезпеки в регіоні. У грудні 2013 року було прийнято Рішення про першочерговий перелік заходів зміцнення довіри в рамках ОБСЄ з метою скорочення ризиків виникнення конфліктів у результаті використання інформаційних та комунікаційних технологій. До цього переліку, серед іншого, увійшли добровільне проведення консультацій на відповідному рівні для зниження ризику неправильного сприйняття та захисту критично важливої національної та міжнародної інфраструктури ІКТ, у тому числі забезпечення їх цілісності.

Питаннями захисту критично важливої інформаційної інфраструктури у державах арабського регіону займається Організація ісламського співробітництва. Вона консультує зацікавлені держави-члени з метою зміцнення їх потенціалу на національному рівні. У 2008 році Організація створила Групу екстреного реагування на комп'ютерні інциденти. У свою чергу, у рамках Ліги арабських держав було ухвалено Керівний закон про боротьбу зі злочинами у сфері інформаційних технологій 2003 року.

У січні 2012 року Африканський союз розробив проект Конвенції про зміцнення довіри та безпеки у кіберпросторі. Метою Конвенції є створення надійної основи для кібербезпеки в Африці. Документ планувався до прийняття у січні 2014 року, чого не сталося в силу заперечень Кенії щодо питання конфіденційності. У червні 2014 року було прийнято Конвенцію про кібербезпеку та захист персональних даних, що охоплює питання електронних операцій, захисту даних, кібербезпеки та кіберзлочинності [314].

У 2004 році члени Організації американських держав схвалили резолюцію, відповідно до якої Секретаріат розпочав роботу над питаннями кібербезпеки. Метою цієї роботи було створення Груп екстреного реагування на комп'ютерні інциденти в кожній державі-члені та аналогічної групи та рівні самої організації.

Іншою організацією, що включила питання кібербезпеки в сферу своєї компетенції, є Асоціація держав Південно-Східної Азії (АСЕАН). Вже у Сінгапурській декларації 2003 року містився заклик до створення інформаційної інфраструктури АСЕАН та Груп екстреного реагування на комп'ютерні інциденти у всіх державах-членах до 2005 року. У 2010 році був прийнятий Генеральний план розвитку зв'язку в країнах АСЕАН. А в 2011 році було погоджено Генеральний план розвитку ІКТ в АСЕАН до 2015 року. У 2012 році з метою підтримки Ради АСЕАН з питань мережевої безпеки державами-членами АСЕАН було прийняте рішення про продовження навчань під керівництвом Групи екстреного реагування на комп'ютерні інциденти АСЕАН. У 2013 році була оновлена програма співпраці щодо мережевої безпеки 2005 року.

Азійсько-Тихоокеанське економічне співробітництво (АТЕС) долучилося до обговорення питань кібербезпеки у 2002 році. У рамках об'єднання була прийнята Стратегія кібербезпеки 2005 року, у якій визнавалася важливість безпеки інфраструктури зв'язку і, зокрема, Інтернету в регіоні АТЕС.

Особливо слід відзначити діяльність Шанхайської організації співробітництва (ШОС). Так, у 2007 році держави-члени ШОС ухвалили спільний План дій щодо забезпечення інформаційної безпеки. Згодом, у 2009 році була прийнята Угода про співпрацю у сфері забезпечення міжнародної інформаційної безпеки, яка вперше на міжнародно-правовому рівні закріпила наявність конкретних загроз та визначила основні напрямки, принципи і форми співпраці у досліджуваній сфері. У 2013 році були підписані двосторонні угоди про боротьбу з використанням чи потенційним використанням комп'ютерних мереж у терористичних, сепаратистських чи екстремістських цілях. На рівні СНД діє Угода про співпрацю держав-членів СНД щодо боротьби зі злочинами у сфері комп'ютерної інформації 2001 року.

Між країнами світу існують серйозні протиріччя щодо класифікації кібератак,

що особливо помітно на прикладі США та Росії. У 2011 році Росія запропонувала концепцію Конвенції про забезпечення міжнародної інформаційної безпеки, у якій визначаються основні загрози міжнародному миру та безпеці в інформаційному просторі. В основу документу покладено принцип збереження державного суверенітету та юрисдикції у кіберпросторі. Натомість США послідовно критикують російські ініціативи та виступають за відкритість Інтернету. У концепції перелічуються принципи забезпечення міжнародної інформаційної безпеки. Окремо розглядаються заходи попередження і вирішення військових конфліктів, протидії терористичним актам та правопорушенням в інформаційному просторі [315]. Документ не отримав загального визнання та наразі існує у вигляді Декларації ШОС, що визначає основні принципи відповідальної поведінки у кіберпросторі.

У 2012 році Росія запропонувала прийняти угоду, яка б забороняла таємно вводити шкідливі коди чи схеми, які згодом можуть бути активовані з віддаленої точки світу у випадку війни. США виступили проти такої ініціативи, оскільки послідовно відстоюють ідею військового реагування на кібератаки [316]. Росія орієнтує міжнародне співтовариство на дослідження загроз у сфері інформаційної безпеки і можливих спільних заходів щодо їх усунення, у тому числі на створення міжнародно-правового режиму, що обмежує можливості створення і застосування інформаційної зброї. Крім того, Росія виступає ініціатором обговорення проблеми інформаційної безпеки на регіональному рівні в рамках таких організацій як ШОС, ОБСЄ, ОДКБ, НАТО тощо.

Першими документами у сфері кібербезпеки, прийнятими США, стали Національна стратегія боротьби з тероризмом, Національна стратегія захисту кіберпростору та Національна стратегія фізичного захисту критичної інфраструктури. Ці стратегії вперше офіційно визнали «повну залежність інфраструктури США від інформаційних систем і мереж» та передбачили створення Єдиної національної системи реагування на кібернетичні напади [317-318]. Відповідно до Стратегії щодо діяльності у кіберпросторі США зобов'язуються підтримувати тісні зв'язки зі своїми союзниками з метою захисту спільних інтересів у кіберпросторі та розробки заходів стримування потенційних агресорів [319]. Це, в

свою чергу, повинно сприяти поширенню американської моделі кібербезпеки.

У лютому 2014 року в США були представлені перші добровільні стандарти кібербезпеки для приватного сектору, спрямовані на захист їх критично важливої інфраструктури. Стандарти також заохочують більш широкий обмін інформацією між секторами бізнесу та відповідними державними органами. Міжнародна стратегія з кібербезпеки США спрямована на передачу державам, що прагнуть створити свій власний технічний потенціал та потенціал кібербезпеки, необхідного досвіду, знань та інших ресурсів. Така підтримка може мати найрізноманітнішу форму – від зміцнення національного потенціалу у сфері ліквідації наслідків інцидентів до створення державно-приватних партнерств, підвищення безпеки систем управління та допомоги у розробці ефективних законів про кібербезпеку [320].

На початку 2015 року США ухвалили нову Стратегію національної безпеки, у якій згадується й про кібербезпеку. У документі зазначається про зростаючу небезпеку підривної чи подекуди руйнівної кібератаки. З метою реагування на нові виклики пропонується збільшити інвестиції у цифровий потенціал, співпрацювати з власниками та операторами критичної інфраструктури, законодавчо супроводжувати цифрове регулювання, а також сприяти розвитку цифрових можливостей держав світу. Однак, кібербезпека не увійшла в число восьми головних стратегічних ризиків.

Стратегія закріплює положення про необхідність вжиття заходів для захисту американського бізнесу та мереж від кіберкрадіжок торговельних таємниць для отримання комерційної вигоди як з боку приватного сектору, так і зі сторони уряду Китаю. США, таким чином, декларують захист приватного сектору від кібершпіонажу. Показово, що в документі підтверджується застосовність міжнародного права до відносин у кіберпросторі [321].

На жаль, не виділяється ефективністю правового регулювання сфери кібербезпеки Україна. Вкрай негативною рисою національного законодавства є відсутність єдиного комплексного загальнообов’язкового документу та розпорошеність окремих питань у численних нормативно-правових актах різної

юридичної сили. При цьому, важливі питання закріплюються на рівні підзаконних нормативно-правових актів, що свідчить про те, що Україна до останнього часу не усвідомлювала усієї важливості інформаційної безпеки. Не менш важливою проблемою для ефективного забезпечення інформаційної безпеки України є неузгодженість нормативно-правових актів між собою та з чинною Конституцією. Характерною рисою національного інформаційного законодавства є декларативність значного масиву норм.

Відповідно до ч. 1 ст. 17 Конституції України захист інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу [290]. Крім того, інформаційна безпека України є невід'ємною складовою національної безпеки та критично важливою умовою для забезпечення суверенітету та територіальної цілісності держави.

Починаючи з 1999 року традиційно невдалими були спроби на законодавчому рівні врегулювати питання інформаційної безпеки та державної інформаційної політики. Чинними нормативно-правовими актами, що регулюють відносини у сфері інформаційної безпеки України є Закон України «Про основи національної безпеки України» від 2003 року [322] та Рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 2014 року [323]. В останньому документі нарешті наголошується на необхідності прийняття таких основоположних документів як Стратегія розвитку інформаційного простору України, Стратегія кібернетичної безпеки України, Закону про кібернетичну безпеку України, а також внесення численних змін до чинного законодавства. Пропонується також розробити заходи протидії інформаційній агресії іноземних держав та негативному інформаційно-психологічному впливу. Крім того, у березні 2016 року була затверджена Стратегія кібербезпеки України, написана у вкрай загальних формулюваннях. Залишається сподіватися, що в нашій державі зрештою будуть проведені необхідні законодавчі зміни, що у комплексі із реструктуризацією системи національної безпеки дозволять створити потужний механізм стримування та протидії зовнішньому агресору, зокрема, в інформаційній сфері, яка у сучасних

умовах перетворюється на вагомий чинник суспільного та державного розвитку.

Незважаючи на ті виклики та загрози, що несуть у собі кібератаки для світового миру та безпеки, деякі вчені та науковці продовжують вважати, що напади у кіберпросторі не становлять небезпеки для реального світу. Їх позиція є абсолютно невиправданою, хоча б тому, що сучасний світ є надзвичайно залежним від інформаційно-комунікаційних мереж та технологій середовищем. Держави вже сьогодні ведуть боротьбу за контроль та вплив у кіберпросторі, який відіграє надзвичайно значущу роль у перерозподілі світових сил.

Найкращим способом стримування кіберконфлікту є зниження національних та міжнародних ризиків, одночасно із дослідженням усіх можливостей використання кіберпростору. Держави повинні прагнути до зменшення гонки кіберозброєнь шляхом побудови взаємовідносин на основі довіри. В якості першого кроку у напрямку зниження ризику виникнення конфлікту кожна держава повинна провести внутрішню оцінку стану своєї захищеності від можливих атак. Це вимагає ретельного та досконалого огляду усіх сфер, в основі яких лежить критична інфраструктура. По-друге, держави повинні вжити заходів для підвищення безпеки устаткування і програмного забезпечення. По-третє, держави повинні співпрацювати між собою з метою поширення інформації, особливо в періоди криз, а також у цілях встановлення загальнообов'язкових норм поведінки.

Співпраця держав у кіберпросторі повинна відбуватися за принципом розумного стримування та обмеження розвитку кіберпотужностей. В основу універсального міжнародно-правового договору має бути покладена добровільна відмова держав від використання кіберозброєння, що може спричинити руйнівні наслідки. Подібні домовленості на міжнародному рівні уже мали місце, коли держави домовились про обмеження розвитку та поширення ядерної, хімічної та біологічної зброї. Однак, кіберпростір настільки ускладнює процес атрибуції суб'єктів, винних у вчиненні кіберзлочинів та завданні кібератак, що надзвичайно складно говорити про ефективність пристосування вже існуючих контрольних та каральних механізмів до правовідносин, що виникають внаслідок порушення кібербезпеки.

Саме тому наразі міжнародні організації активно працюють над питанням розробки заходів підвищення довіри у кіберпросторі. Так, у 2012 році з метою оцінки ролі заходів довіри в забезпеченні стабільності кіберпростору була проведена конференція ООН. У 2013 році ОБСЄ прийняла перші багатосторонні заходи зміцнення довіри у сфері кібербезпеки та безпеки ІКТ. Хоча подібні норми не мають обов'язкової сили, вони є свідченням розвитку дипломатичного діалогу щодо досягнення консенсусу з питання створення заходів довіри. Останні повинні задовольняти критерії прозорості, передбачуваності та перевірки [324].

Одна з ключових перешкод на шляху до створення універсального режиму кібербезпеки полягає у тому, що кожна держава прагне зайняти стратегічні позиції для кібервійни. Відбувається перегляд військових доктрин на предмет включення до них кібервійни як важливої сфери протиборства. Очевидно, що для вироблення єдиних стандартів кібербезпеки держави повинні, в першу чергу, довіряти одна одній. Але вкрай складно говорити про довіру в умовах, коли кожна з них намагається здобути першість у гонці кіберозброєнь.

Кібервійна розпочинається у кіберпросторі з використання ІКТ, втім вона може дуже швидко перекинутися за межі онлайнового світу, створюючи загрозу урядам, бізнес-середовищу та індивідам. Слід з усією серйозністю поставитися до потенційно можливих негативних наслідків кібервійни і кіберзлочинності для міжнародної безпеки та миру. Складність і взаємозалежність інформаційних систем веде до того, що наслідки порушення їх нормальної роботи можуть бути непередбачуваними і в найгіршому випадку викликати «ефект доміно».

Отже, незважаючи на відсутність єдиного розуміння того, що являє собою кібервійна чи кібертероризм, держави повинні бути впевнені у тому, що їх інфраструктури належним чином захищені від різних типів кіберзагроз, а також у тому, що їх правові та політичні норми дозволяють ефективно попередити, відбити та зменшити негативні наслідки можливих кібератак. Неспроможність виробити універсальне визначення ключових понять «кібератаки» та «кібервійни» не зменшує нагальності підвищення готовності держав до можливих кіберконфліктів [325].

Упродовж останніх десятиліть міжнародне право з перемінним успіхом

забезпечувало мирне співіснування держав, що, однак, не повинно нівелювати його ролі як інструмента підтримання кібермиру і кіберстабільності. Наразі більшість міжнародно-правових актів та обговорень зосереджені навколо військової складової кібербезпеки. Вважаємо за доцільне змістити акцент на мирне використання кіберпростору, зміцнення заходів довіри та культивування відповідальної поведінки держав у кіберпросторі. Така неагресивна риторика сприятиме досягненню компромісу з питань вироблення універсального міжнародно-правового режиму безпеки для кіберпростору. Модель підтримання кібермиру та створення системи захищеності суб'єктів у кіберпросторі потребує затвердження на універсальному рівні загальнообов'язкових норм та правил поведінки в інформаційному середовищі. Однак, як і у випадку із захистом персональних даних, намітилася чітка тенденція до регіоналізації обговорень з питань кібербезпеки. При цьому, значної гармонізації термінологічного апарату та норм і правил поведінки у кіберпросторі у військовий та мирний час вдалося досягти на рівні юридично незобов'язуючого документу _ Таллінського посібника. Фактично, державам залишилося лише перенести відповідні режими у юридично обов'язкову площину, якщо вони, все-таки, збережуть тенденцію до визнання своєї першості у питаннях міжнародної безпеки. З іншого боку, інтенсифікація співробітництва з іншими зацікавленими суб'єктами на основі багатостороннього діалогу дозволить створити максимально глобальний механізм забезпечення кібербезпеки, що охоплюватиме як нормативну, так і технологічну складову. Лише вироблення універсального міжнародно-правового режиму безпеки у кіберпросторі здатне забезпечити належний рівень захисту прав людини онлайн, у тому числі, що стосується передачі персональних даних.

Одним із семи принципів загального міжнародного права, закріплених у Декларації про принципи міжнародного права щодо дружніх відносин та співробітництва між державами 1970 року, визнається принцип співробітництва держав, що не втрачає своєї актуальності й у контексті правотворення та правозастосування з питань розвитку глобального інформаційного суспільства.

У цьому розділі дисертаційного дослідження були розглянуті приклади міжнародного співробітництва держав з питань розвитку глобального

інформаційного суспільства у сферах, що становлять найбільший інтерес, є найбільш нормативно розробленими та водночас викликають найбільше труднощів в аспекті вироблення універсальних міжнародно-правових режимів та регулювання. При цьому при виборі конкретних сфер співробітництва автором був застосований не стільки секторальний, скільки ціннісний підхід, передбачений підсумковими документами Всесвітнього саміту інформаційного суспільства. Обмежений обсяг дисертаційного дослідження не дозволяє охопити усі напрямки співробітництва з питань розвитку глобального інформаційного суспільства, втім найважливіші з них знайшли відображення в останньому розділі дисертації.

ВИСНОВКИ ДО РОЗДІЛУ 3

Природа глобального інформаційного суспільства сприяє формуванню міжнародно-правового регулювання, центром якого є людина. Саме тому аналіз взаємодії співробітництва і нормотворчих ініціатив держав та інших зацікавлених суб'єктів розпочинається з вивчення режиму та механізмів захисту прав людини онлайн. Так, встановлено, що чинне міжнародне право гарантує кожній людині однакові права онлайн та офлайн. При цьому найбільш прогресивним є регулювання в рамках Ради Європи, що активно займається розробкою концепції прав людини онлайн.

Запропоновано авторське визначення цифрових прав або прав людини онлайн, під якими пропонується розуміти права людини, реалізація та захист яких відбуваються в межах або у зв'язку з кіберпростором шляхом використання Інтернету та/або сучасних ІКТ. Концепція цифрових прав охоплює існуючі права людини у контексті їх застосування в Інтернеті, тим самим розширюючи їх обсяг та надаючи їм нового виміру. Нерозвиненими на міжнародно-правовому рівні залишаються механізми правового захисту та відновлення порушених прав онлайн.

Встановлено, що новими правами, поява яких обумовлена розвитком глобального інформаційного суспільства, є доступ до Інтернету та «право бути забутим». Вважаємо, що сучасне міжнародне право повинне містити як негативні,

так і позитивні зобов'язання держав щодо гарантування права на доступ до Інтернету.

Принцип мережевої нейтральності є необхідною передумою реалізації прав людини онлайн. Для того, щоб підкреслити його важливість та комплексність було надано авторське визначення принципу мережевої нейтральності, під яким пропонується розуміти право користувачів Інтернету отримувати доступ до інформації та послуг без дискримінації за типом інформації, її обсягом, характером послуги, технічним способом або технічними пристроями, що їх застосовує конкретний користувач, а також імунітет операторів мережі від притягнення до відповідальності за передачу третіми сторонами контенту та додатків, що вважаються незаконними або небажаними.

Обґрунтовано раціональність запровадження універсального міжнародно-правового регулювання сфери захисту персональних даних. Продемонстровано, що у даній сфері найбільш тісним чином переплетені інструменти «твердого» та «м'якого» права. Саме до останнього належить переважна частина домовленостей між США та ЄС. Еволюція регіональних міжнародно-правових режимів захисту персональних даних демонструє високий рівень адаптивності міжнародного права до розвитку глобального інформаційного суспільства. Вкотре підтверджується первинність правозастосовної практики та авторитет судових рішень, що стали підставою перегляду договірної основи співробітництва США та ЄС у сфері поводження та обробки персональних даних. Їх приклад свідчить про те, що вироблення універсального міжнародно-правового регулювання сфери захисту персональних даних можливе лише за умови застосування єдиної системи цінностей (напр., пріоритет безпеки чи вільного обміну інформацією), відмови від категоричності формулювань та надання мінімальних обов'язкових гарантій.

Ухвалення єдиних стандартів обробки та передачі персональних даних дозволить усунути нормативні бар'єри на шляху до вільного потоку інформації, що є одним із основних принципів глобального інформаційного суспільства. Локалізація чи навіть регіоналізація регулювання з питань глобального інформаційного суспільства, по суті, є штучною перешкодою для прогресивного

розвитку міжнародного права. Втім, як свідчить приклад сфери захисту персональних даних, еволюція міжнародного права продовжує відбуватися за класичною схемою трансформації регіональних режимів в універсальні. При цьому логічним було б уникати надлишкової і, як правило, обмежувальної нормативної активності та розробляти універсальне, глобальне регулювання для правовідносин глобального характеру в інформаційній сфері.

Безпека визнається необхідною передумою стабільності та передбачуваності розвитку глобального інформаційного суспільства. Роль міжнародного права полягає, відповідно, у створенні ефективних нормативних рамок та закріпленні належних гарантій як безпеки інфраструктури, так і безпеки самих правовідносин, що виникають в інформаційній сфері.

Крім того, потребують збалансування питання приватності та забезпечення кібербезпеки. І, хоча, більшість дослідників розглядають їх як взаємовиключаючі, у дисертації робиться наголос на їх комплементарності та критичній необхідності узгодження позицій держав та інших зацікавлених суб'єктів у рамках міжнародних форумів та організацій, що займаються розробкою відповідних міжнародно-правових стандартів.

Доведено, що правовий режим безпеки кіберпростору повинен бути універсальним за своєю природою, оскільки йдеться про такі ключові для людства цінності як міжнародний мир та стабільність. Фрагментація правового регулювання може призвести до посилення регіональної співпраці, що однак не вирішує проблему боротьби з кіберзлочинністю та забезпечення кібербезпеки, оскільки останні є глобальними явищами і потребують відповідного універсального механізму регулювання. З цією метою пропонується на міжнародному рівні прийняти універсальний договір, в якому погодити принципи встановлення юрисдикції щодо кіберзлочинів, єдині склади злочинів у кіберпросторі, правила використання електронних доказів при проведенні розслідування та посилення технічної допомоги і міжнародної співпраці у цій сфері. Такий універсальний документ повинен містити норми як матеріального, так і процесуального права, а також закладати основи міжнародного співробітництва у досліджуваній сфері. При

розробці міжнародного договору з питань кібербезпеки слід врахувати національні та регіональні нормативні підходи, вивчити передові практики та заповнити існуючі прогалини. В основу універсального режиму безпеки у кіберпросторі повинні бути покладені не лише єдині технічні стандарти, але й нормативні приписи.

Наразі більшість міжнародно-правових актів та обговорень зосереджені навколо військової складової кібербезпеки. Вважаємо за доцільне змістити акцент на мирне використання кіберпростору, зміцнення заходів довіри та культивування відповідальної поведінки держав у кіберпросторі. Така неагресивна риторика сприятиме досягненню компромісу з питань вироблення універсального міжнародно-правового режиму безпеки для кіберпростору.

Основі висновки розділу висвітлені в наукових працях автора [326-334].

ВИСНОВКИ

Проведене дослідження дозволило сформулювати та обґрунтувати наступні висновки, що підтверджують запропоновану у вступі гіпотезу про прогресивний розвиток міжнародного права як результат нормативного відображення питань розвитку глобального інформаційного суспільства:

1. На сучасному етапі прогресивний розвиток міжнародного права в інформаційній сфері став можливим, у тому числі, завдяки трансформуючому впливу глобального інформаційного суспільства. Доведено, що однією з найбільших труднощів міжнародно-правового регулювання досліджуваної сфери є випереджувальні темпи розвитку об'єкту регулювання порівняно із регуляторною спроможністю нормативної системи. На практиці реально сформувався і функціонує новий об'єкт міжнародно-правового регулювання – суспільні відносини, обумовлені появою глобального інформаційного суспільства, однак, досі недостатньо розвиненим залишається саме міжнародно-правове регулювання та механізми глобального управління інформаційним суспільством.

2. У доктрині міжнародного права та відповідних міжнародно-правових документах відсутнє єдине розуміння поняття «інформаційного суспільства» та його концептуального наповнення. З метою усунення термінологічної неоднозначності автором сформульовано власне визначення поняття глобального інформаційного суспільства у контексті міжнародного права, під яким пропонується розуміти не

просто нову суспільну формацію, а усю повноту правовідносин (правопорядок), що виникають в інформаційній сфері, а також унікальне поєднання демократичних інституцій, політичних режимів, сприятливого для інновацій середовища та активного і структурованого громадянського суспільства, що виникли та розвиваються в рамках глобального та інклюзивного кіберпростору, у якому відсутні фізичні кордони.

Іншою базовою категорією понятійного апарату дисертаційного дослідження є «кіберпростір», що в авторському визначенні означає специфічне середовище, в межах якого на основі використання Інтернету та відповідних інформаційно-комунікаційних технологій здійснюється обіг товарів та послуг, відбувається комунікація та реалізація прав людини, ведеться боротьба за розподіл сфер впливу та формуються власні механізми управління глобальним інформаційним суспільством. На нормативно-правовому рівні потребують врегулювання як питання використання та контролю над інформаційною інфраструктурою, так і самі суспільні відносини, що виникають у межах кіберпростору.

3. Стан сучасного міжнародного права означено поняттям нормативного індетермінізму, що зумовлює необхідність вдосконалення класичних міжнародно-правових концепцій суверенітету, кордонів, громадянства, територіальності та юрисдикції з метою відображення еволюційних змін, викликаних розвитком глобального інформаційного суспільства. Уявлення про кіберпростір як середовище у якому відсутні будь-які географічні кордони потребує нормативної реакції з боку міжнародного права. Однак, таке регулювання не може бути ефективним за умови застосування територіально орієнтованих правових актів до транскордонного глобального простору.

Доведено, що відображення на нормативному рівні змін у суспільних відносинах, зумовлених формуванням глобального інформаційного суспільства, сприятиме прогресивному розвитку міжнародного права. Наразі правова та соціальна системи досягли того рівня синергії, коли очевидним є не лише трансформуючий вплив глобального інформаційного суспільства на міжнародне

право, але й стає невідворотним нормативне закріплення правових основ та стандартів функціонування та еволюції такого суспільства.

4. Розроблено авторську періодизацію еволюції адаптивності міжнародного права до відображення змін у суспільних відносинах, зумовлених формуванням глобального інформаційного суспільства. Прогресивний розвиток міжнародного права проявляється у розширенні його регуляторної спроможності за рахунок поступового охоплення все більш широкого кола питань розвитку глобального інформаційного суспільства.

Автором пропонується розпочинати періодизацію з моменту прийняття документів з питань розбудови нового світового інформаційно-комунікаційного порядку (НСІКП) (1970-ті – 1990-ті рр. XX ст.). Наступний етап конвергенції датується 2003 роком та пов'язується з початком проведення Всесвітнього саміту інформаційного суспільства (ВСІС). Оцінка здобутків цього історичного періоду та перехід до наступного етапу відбувається наприкінці 2015 року із ухваленням Фінального документу ВСІС+10. Підведення підсумків цього етапу очікується у 2025 році. Крім того, паралельним поступом розвивається імплементація Плану дій «*Connect 2020*» та Цілей сталого розвитку ООН на період до 2030 року.

Встановлено історичну спадковість відображення питань розвитку глобального інформаційного суспільства у міжнародному праві. Питання захисту прав людини та розширення можливостей участі у глобальному нормотворенні усіх зацікавлених сторін є спільними для усіх досліджених етапів.

5. Запропоновано розрізняти два типи інституційних моделей, у рамках яких відбувається формування політики та стандартів управління глобальним інформаційним суспільством. Перша модель ґрунтується на традиційному міждержавному механізмі, прикладом якого може бути співпраця в рамках ООН. В основі іншої моделі – принцип багатосторонньої участі, що передбачає залучення різноманітних недержавних суб'єктів. На даному принципі побудована діяльність, зокрема, ICANN та IGF.

Доведено, що множинність інституційних механізмів, які подекуди задають протилежні напрямки розвитку глобального інформаційного суспільства, створює

загрозу фрагментації Інтернету і міжнародно-правового регулювання. Встановлено, що в умовах розбудови глобального інформаційного суспільства функцію задоволення суспільного інтересу найбільш ефективно здійснюють багатосторонні інституційні механізми, більшість з яких виконують обмежену у розумінні міжнародного права нормотворчу функцію. З огляду на глобальний та інклюзивний характер інформаційного суспільства в основу його інституційного механізму повинні бути покладені принципи відкритості, транспарентності та рівних можливостей, а у його структурі повинні бути представлені усі зацікавлені сторони як з розвинених країн, так і з країн, що розвиваються.

6. Продемонстровано, що роль держав як суб'єктів глобального інформаційного правопорядку чи не вперше за всю історію міжнародного права перестає бути лідируючою. Обґрунтовано перехід від державоцентричної до людиноцентричної системи міжнародно-правового регулювання. Крім того, визнання концепцій розподіленого суверенітету та багатосторонньої участі повинно стати органічним відображенням відповідних трансформацій у нормотворчій активності суб'єктів, спрямованій на регулювання інформаційних правовідносин.

Розвиток глобального інформаційного суспільства не просто вимагає розширювального тлумачення чинного міжнародного права, а сприяє його прогресивному розвитку.

7. Міжнародне право в силу швидкого розвитку сучасних ІКТ характеризується постійним відставанням від прогресуючих суспільних відносин в інформаційній сфері, що потребують відповідного нормативного врегулювання. У глобальному інформаційному суспільстві міжнародне право поступово втратило свою попереджувальну функцію та перетворилося із регулювання *ex ante* на регулювання *ex post*.

Встановлено, що в умовах глобального інформаційного суспільства відбувся фактичний перерозподіл владних та нормотворчих функцій, що зумовило зростання ролі «м'якого» права та судових рішень у якості «допоміжних» нормативних регуляторів суспільних відносин, опосередкованих використанням Інтернету.

8. Доведено, що у силу недостатньої розвиненості договірного міжнародно-правового регулювання питань розвитку глобального інформаційного суспільства зростає роль звичаю як джерела нормативного впорядкування правовідносин в інформаційній сфері. Отримала подальший розвиток концепція *diritto spontaneo*, тобто миттєвого звичаєвого міжнародного права, що ґрунтується на елементі *opinio juris* та не вимагає існування тривалої практики застосування норми поведінки. Формою закріплення такої норми може бути її відображення у тексті правовстановлюючої резолюції. Більшість договірних режимів не є універсальними, натомість звичаєві норми інколи мають більше охоплення за колом суб'єктів, що вважають себе зобов'язаними цією нормою. Різний рівень технологічного розвитку держав світу свідчить про більшу ймовірність формування регіональних звичаєвих норм з питань розвитку глобального інформаційного суспільства, аніж універсальних стандартів.

9. Протягом останніх трьох десятиліть у теорії міжнародного права сформувалася концепція «м'якого» права як компромісу між «твердим» правом та відсутністю нормативного регулювання. Встановлено, що «м'яке» право характеризується гнучкістю та високим ступенем адаптивності до змін, пов'язаних з виокремленням та ускладненням питань розвитку глобального інформаційного суспільства. Крім того, «м'яке» право передбачає максимально гнучкий механізм перегляду нормативних актів та внесення до них відповідних змін та поправок. Міжнародне право слід розглядати як еволюціонуючий механізм, ефективність якого вимірюється здатністю відповідати на суспільні потреби. У XXI столітті такі потреби найбільш повно та оперативно задовольняються через застосування «м'якого» права.

10. Глобальність інформаційного суспільства формує потребу у такому ж глобальному міжнародно-правовому регулюванні та правовиконанні. Прогресивний розвиток міжнародного права з питань розвитку глобального інформаційного суспільства проявляється у формуванні окремої комплексної галузі – міжнародного інформаційного права. При цьому, якщо розглядати глобальне інформаційне суспільство у широкому розумінні як воно запропоноване у авторському визначенні,

тобто як усю повноту правовідносин (правопорядок), що виникають в інформаційній сфері, то за предметною сферою воно охоплює усі напрями міжнародно-правового регулювання в інформаційній сфері. У вузькому розумінні міжнародно-правові питання розвитку глобального інформаційного суспільства можна виділити у якості окремої підгалузі міжнародного інформаційного права зі специфічним предметом регулювання. Так, до питань розвитку глобального інформаційного суспільства, що потребують врегулювання на нормативному рівні, пропонується включати наступні: а) інформаційна та комунікаційна інфраструктура; б) використання ІКТ у цілях розвитку; в) управління Інтернетом; г) інституційні механізми посиленої та багатосторонньої співпраці; ґ) права людини онлайн; д) кібербезпека та відповідальна поведінка держав у кіберпросторі. Наведений перелік не є вичерпним та підлягає постійному перегляду і доповненню з метою приведення його у відповідність із технологічним прогресом та відповідними змінами в інформаційних правовідносинах.

11. Розроблено класифікацію чинних нормативно-правових актів з питань розвитку глобального інформаційного суспільства за предметною сферою дії. Групування регуляторних актів у досліджуваній сфері покликане полегшити їх використання у правозастосовній діяльності. Першу групу становлять акти, спрямовані на регулювання глобального інформаційного суспільства як самостійного феномену. Другу групу формують міжнародно-правові акти з питань кіберпростору. Міжнародно-правові акти, що увійшли до третьої групи, сфокусовані на питаннях управління та функціонування Інтернету. Класифікуючою ознакою наступної категорії є заборона сексуальної експлуатації дітей та дитячої порнографії. Окрему групу становлять міжнародно-правові акти щодо використання ІКТ у цілях розвитку людства. Самостійним предметом міжнародно-правового регулювання є питання інтелектуальної власності.

12. Виявлено зростаючу роль міжнародних судових установ, зокрема Європейського суду з прав людини та Суду ЄС, у процесах стандартоутворення з питань глобального інформаційного суспільства. Саме суди виявилися здатними найбільш оперативно реагувати на зміни у правовідносинах у рамках глобального

інформаційного суспільства та закладати тенденції розвитку відповідного міжнародно-правового регулювання. Крім того, судова практика формує основи правозастосування в аспекті розширювального тлумачення чинних міжнародно-правових норм по відношенню до питань розвитку глобального інформаційного суспільства.

13. Доведено, що найбільш вдалими прикладами адаптації міжнародного права до швидко прогресуючих інформаційних правовідносин та правопорядку є права людини онлайн, захист і транскордонна передача персональних даних та кібербезпека, які, крім того, є найбільш нормативно розробленими та становлять основу багатостороннього діалогу з питань розвитку глобального інформаційного суспільства.

14. Природа глобального інформаційного суспільства сприяє формуванню міжнародно-правового регулювання, центром якого є людина. Встановлено, що чинне міжнародне право гарантує кожній людині однакові права онлайн та офлайн. При цьому найбільш прогресивним порівняно з іншими регіональними системами права є регулювання в рамках Ради Європи, що активно займається розробкою концепції прав людини онлайн. Доведено, що недостатньо просто закріпити однаковий режим захисту прав онлайн та офлайн, натомість окрім загальних принципів необхідно прописати конкретні способи та засоби такого захисту, що підлягають застосуванню відповідно до контексту правовідносин. Для сучасного міжнародного права характерне перманентне відставання в аспекті створення ефективних правових механізмів захисту прав людини онлайн.

Запропоновано авторське визначення цифрових прав або прав людини онлайн, під якими пропонується розуміти права людини, реалізація та захист яких відбуваються в межах або у зв’язку з кіберпростором шляхом використання сучасних інформаційно-комунікаційних технологій, зокрема Інтернету. Концепція цифрових прав охоплює існуючі права людини у контексті їх застосування онлайн, тим самим розширюючи їх обсяг та надаючи їм нового виміру. Нерозвиненими на міжнародно-правовому рівні залишаються механізми правового захисту та відновлення порушених прав онлайн.

15. Принцип мережевої нейтральності є необхідною передумовою реалізації прав людини онлайн. Для того, щоб підкреслити його важливість та комплексність надано авторське визначення принципу мережевої нейтральності, під яким пропонується розуміти право користувачів Інтернету отримувати доступ до інформації та послуг без дискримінації за типом інформації, її обсягом, характером послуги, технічним способом або технічними пристроями, що їх застосовує конкретний користувач, а також імунітет операторів мережі від притягнення до відповідальності за передачу третіми сторонами контенту та додатків, що вважаються незаконними або небажаними.

16. Удосконалено раціональність запровадження універсального міжнародно-правового регулювання у сфері захисту і транскордонної передачі персональних даних. Продемонстровано, що у даній сфері найбільш тісним чином переплетені інструменти «твердого» та «м'якого» права. Саме до останнього належить переважна частина домовленостей між США та ЄС. Еволюція регіональних міжнародно-правових режимів захисту персональних даних демонструє високий рівень адаптивності міжнародного права до розвитку глобального інформаційного суспільства. Вкотре підтверджується первинність правозастосовної практики та авторитет судових рішень, що стали підставою перегляду договірної основи співробітництва США та ЄС у сфері захисту і транскордонної передачі персональних даних. На їх прикладі доведено, що вироблення універсального міжнародно-правового регулювання сфери захисту персональних даних можливе лише за умови застосування єдиної системи цінностей (напр., пріоритет безпеки чи вільного обміну інформацією), відмови від категоричності формулювань та надання мінімальних обов'язкових гарантій.

17. Безпека визнається необхідною передумовою стабільності та передбачуваності розвитку глобального інформаційного суспільства. Роль міжнародного права полягає у створенні ефективних нормативних рамок та закріпленні належних гарантій як безпеки інфраструктури, так і безпеки самих правовідносин, що виникають в інформаційній сфері.

Крім того, потребують збалансування питання приватності та забезпечення кібербезпеки, що носять комплементарний характер по відношенню один до одного. Доведено, що правовий режим безпеки кіберпростору повинен бути універсальним за своєю природою, оскільки йдеться про такі ключові для людства цінності як міжнародний мир та стабільність. Фрагментація правового регулювання може призвести до посилення регіональної співпраці, що не вирішує проблему боротьби з кіберзлочинністю та забезпечення кібербезпеки, оскільки останні є глобальними явищами і потребують відповідного універсального механізму регулювання. Універсальний документ повинен містити норми як матеріального, так і процесуального права, а також закладати основи міжнародного співробітництва у досліджуваній сфері. При розробці міжнародного договору з питань кібербезпеки слід врахувати національні та регіональні нормативні підходи, вивчити передові практики та заповнити існуючі прогалини. В основу універсального режиму безпеки у кіберпросторі повинні бути покладені не лише єдині технічні стандарти, але й нормативні приписи.

18. Визначено, що інтеграція України в європейський та глобальний інформаційний простір можлива лише за умови приведення національного законодавства у відповідність зі світовими стандартами. Від правильності визначення геостратегічних пріоритетів в інформаційній сфері значною мірою залежатиме, чи стане Україна сильним та повноправним гравцем у сучасних міжнародних відносинах. Наразі національне нормативно-правове регулювання України не встигає враховувати зміни в розвитку інформаційно-комунікаційних технологій, застосування яких так чи інакше зачіпає сферу стратегічних інтересів нашої держави. Нові законодавчі акти у сфері інформаційної політики та безпеки розробляються лише у відповідь на реальні загрози, однак все одно залишаються рамковими та прописуються у доволі загальних формулюваннях. У законодавчих ініціативах, спрямованих на захист національної безпеки почала прослідковуватися тенденція до обмеження права на свободу вираження поглядів. Важливим геостратегічним пріоритетом України залишається поглиблення співробітництва з

НАТО, адаптація національного законодавства до Цифрового порядку денного для Європи та виконання приписів Угоди про асоціацію з ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Castells M. The Rise of the Network Society. The Information Age: Economy, Society and Culture / Manuel Castells. – Volume I. – 2nd edition. – Wiley-Blackwell, 2009. – Pp. 656.

2. Pinter R. Towards Getting to Know Information Society / Robert Pinter // Information Society: From Theory to Political Practice. Coursebook. – Budapest: Gondolat - Uj Mandatum, 2008. – Pp. 11-28.

3. Stonier T. The Wealth of Information: Profile of the Post-industrial Society / Tom Stonier. – London: Mandarin, 1983. – 176 p.

4. Florini A. M. The Third Force: The Rise of Transnational Civil Society / Ann M. Florini. – Washington DC: Carnegie Endowment for International Peace, 2000. – 295 p.

5. Скринька Д. В. Проблема екстерналій (зовнішніх ефектів) в міжнародному публічному праві / Д. В. Скринька // Актуальні проблеми міжнародних відносин. – Вип. 93. – Ч. ІІ. – 2010. – С. 103-110.

6. Karvalics L. Z. Information Society – what is it exactly? The meaning, history and conceptual framework of an expression / Laszlo Z. Karvalics // Information Society: From Theory to Political Practice. - Budapest: Gondolat-Uj Mandatum, 2008. – Pp. 29-47.

7. Pickard V. Neoliberal visions and revisions in global communications policy from NWICO to WSIS / Victor Pickard // Journal of Communication Inquiry. – 2007. – Vol. 31. – Pp. 118-139.

8. Scholte J. A. Global Civil Society: Changing the World? / Jan Aart Scholte // CSGR Working Paper. – University of Warwick, UK. – 1999. – Issue 31. – Pp. 1-35.

9. Price R. Reversing the Gun Sights: Transnational Civil Society Targets Land Mines / Richard Price // International Organization. – Vol. 52. – No. 3. – MIT Press, 1998. – Pp. 613-644.

10. Mitrani M. Global Civil Society and International Society: Compete or Complete? / Mor Mitrani // Alternatives: Global, Local, Political. – 2013. – Vol. 38. – Issue 2. – Pp. 172-188.

11. Held D. Democracy and the Global Order / David Held. – Cambridge: Polity Press, 1995. – 336 p.

12. Kaldor M. Governance, Legitimacy, and Security: Three Scenarios for the Twenty-first century / Mary Kaldor // Principled World Politics: The Challenge of Normative Relations [ed. Wapner P. and Ruiz L.]. – New York: Rowman & Littlefield Publishers Inc., 2000. – 284 p.

13. Risse T. The Power of Human Rights: International Norms and Domestic Change / Thomas Risse, Stephen C. Ropp, Kathryn Sikkink. – New York: Cambridge University Press, 1999. – 336 p.

14. Colas A. International Civil Society: Social Movements in World Politics / Alejandro Colas. – Cambridge: Polity Press, 2002. – 232 p.

15. Filho F. Introducao ao direito comunitario / Franca Filho, Marcilio Toscano. – Sao Paulo: Oliveira Mendes, 2002.

16. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace [Електронний ресурс]. – UNESCO, Paris. – 17 October 2003. – 10 p. – Режим доступу: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf.

17. Matias E. A humanidade e suas fronteiras: do Estado soberano a socidedade global / Eduardo Felipe Perez Matias. – Sao Paulo: Paz e Terra, 2005. – 556 p.

18. Pinheiro R., Tsang S. Advanced Intelligent Networks // Service Provision: Technologies for Next Generation Communications [ed. Kenneth J. Turner, Evan H. Magill, David J. Marples]. – New York: John Wiley & Sons Ltd., 2004. – Pp. 53-71.

19. Kazuto S. «Borderless» Activities Happen Only in a «Borderful» World: Ontological Borders and Institutional Borders in Integrated Europe / Suzuki Kazuto // International Relations. – Vol. 162 (2010). – Pp. 9-23.

20. Johnson D. Law and Borders – The Rise of Law in Cyberspace / David R. Johnson, David G. Post // Stanford Law Review. – No. 48. – May 1, 1996. – Pp. 1367-1402.

21. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти): дис. … д-ра юр. наук: 12.00.11/ Пазюк Андрій Валерійович; Київ. нац. ун-т ім. Тараса Шевченка. – 2016. – 467 с.

22. Ginsburg J. Global Use / Territorial Rights: Private International Law Questions of the Global Information Infrastructure / Jane C. Ginsburg // J. Copyright Society. – No. 42. – USA, 1995. – 318-336.

23. Sandel M. America's Search for a New Public Philosophy / Michael J. Sandel // Atlantic Monthly. – Mar. 1996. – Pp. 57-74.

24. Hudgins-Bonafield C. The grass roots of a global Internet rebellion / Christy Hudgins-Bonafield // Network Computing. – 15 October 1997. – Vol. 8. – No. 19. – 26 p.

25. Ó Siochrú S. Will the real WSIS please stand-up? The Historic Encounter of the «Information Society» and the «Communication Society»» / Seán Ó Siochrú // Gazette: The International Journal for Communication Studies. – 2004. – Vol. 66.– No. 3-4. – Pp. 203-224.

26. Скринька Д. В. Право як фактор економічного розвитку (інституційний підхід): автореф. дис. … канд. юр. наук: 12.00.01 / Скринька Дмитро Васильович; Київ. нац. ун-т ім. Тараса Шевченка. – К., 2004. – 21 с.

27. The 2015 BCG e-Intensity Index [Електронний ресурс]. – 2015. – November 18. – Режим доступу: https://www.bcgperspectives.com/content/interactive/telecommunications_media_entertainment_bcg_e_intensity_index/.

28. Digital Dividends. World Development Report 2016 [Електронний ресурс] // The World Bank. – Режим доступу: http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/01/13/090224b08405ea05/2_0/Rendered/PDF/World0developm0000digital0dividends.pdf.

29. Europe and the global information society. Recommendations to the European Council [Електронний ресурс]. – May 1994. – Режим доступу: http://ec.europa.eu/archives/ISPO/docs/basics/docs/bangemann.pdf.

30. Green Paper. Living and Working in the Information Society: People First. European Commission [Електронний ресурс]. – Belgium. – 1996. – Режим доступу: http://ec.europa.eu/employment_social/knowledge_society/green_en.pdf.

31. Чернов А. А. Основные историко-теоретические этапы развития концепций глобального информационного общества / А. А. Чернов // Информация. Дипломатия.

Психология. Сборник материалов «круглого стола» и лекций преподавательской кафедры массовой коммуникации и связей с общественностью Дипломатической академии МИД России. – М., 2002. – С. 31–50.

32. 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: http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_(body).pdf.

33. Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15 травня 2013 р. № 386-р [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/386-2013-%D1%80.

34. Okinawa Charter on Global Information Society [Електронний ресурс] // Okinawa Summit. – 2000. – July 22. – Режим доступу: http://www.ioc.u-tokyo.ac.jp/~worldjpn/documents/texts/summit/20000722.O1E.html.

35. Забара І. М. Сучасний міжнародний інформаційний правопорядок: концептуальні підходи і питання періодизації / І. М. Забара // «Інформація і право». – 2015. – № 1(13). – С. 38-46.

36. Борисов И. С. Идейно-пропагандистская экспансия империализма на Арабском Востоке и борьба арабских стран за новый международный информационный порядок: дис. … канд. истор. наук: 07.00.05 / Борисов Игорь Сергеевич; Дипломатическая академія МИД СССР. – 1984. – 203 с.

37. Вачнадзе Г. Н. Международный обмен информацией. Его сторонники и противники / Г. Н. Вачнадзе, Ю. Б. Кашлев. – Тбилиси: Сабчота Сакартвелою, 1980. – 390 с.

38. Declaration on Fundamental Principles concerning the Contribution of the Mass Media to Strengthening Peace and International Understanding, to the Promotion of Human Rights and to Countering Racialism, Apartheid and Incitement to War [Електронний ресурс]. – 1978. – 28 November. – Режим доступу: http://portal.unesco.org/en/ev.php-URL_ID=13176&URL_DO=DO_TOPIC&URL_SECTION=201.html.

39. Schiller H. Communication and Cultural Domination / Herbert I. Schiller. – New York: M.E. Sharpe Inc., 1976. – 128 p.

40. Many Voices One World, Report of the MacBride Commission [Електронний ресурс]. – Paris. – 1979. – Режим доступу: http://unesdoc.unesco.org/images/0004/000400/040066eb.pdf.

41. Carlsson U. The Rise and Fall of NWICO. From a Vision of International regulation to a Reality of Multilevel Governance / U. Carlsson // Nordicom. – 2003. – Vol. 24. – No. 2. – Pp. 31-67.

42. Виноградова С. М. Проблемы преодоления неравенства в международном информационном обмене / С. М. Виноградова, Г. С. Мельник // Гуманитарный вектор. – Чита, Забайкальский гуманитарно-педагогический университет им. Н. Г. Чернышевского. – 2012. – № 2. – С. 239-246.

43. Nordenstreng K. The Context: Great Media Debate // Towards equity in global communication: MacBride update [eds. R. C. Vincent, K. Nordenstreng, M. Traber]. – Cresskill, NJ: Hampton Press, 1999. – Pp. 263–305.

44. Tehranian M. Where is the New World Order? At the End of history or a Clash of Civilizations? // Towards equity in global communication: MacBride update [eds. R. C. Vincent, K. Nordenstreng, M. Traber]. – Cresskill, NJ: Hampton Press, 1999. – Pp. 23–63.

45. Resolution 73 of the ITU Plenipotentiary Conference [Електронний ресурс]. – Minneapolis. – 1998. – Режим доступу: https://www.itu.int/net/wsis/docs/background/resolutions/73.html.

46. UN General Assembly Resolution A/RES/56/183 «World Summit on the Information Society» dated 31 January 2002 [Електронний ресурс]. – Режим доступу: https://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf.

47. Raboy M. The World Summit on the Information Society and its Legacy for Global Governance / Marc Raboy // Gazette: The International Journal For Communication Studies, 2004. – Vol. 66. – No. 3-4. – Pp. 225–232.

48. Singh P. J. Framing a Global Information Society Discourse / Parminder Jeet Singh, Anita Gurumurthy // Economic and Political Weekly. – Vol. 41. – No. 10. – 2006. – March 11. – Pp. 876-878.

49. Geneva Declaration of Principles dated 12 December 2003 [Електронний ресурс] // ITU. – Режим доступу: http://www.itu.int/wsis/docs/geneva/official/dop.html.

50. WSIS: Plan of Action dated 12 December 2003 [Електронний ресурс] // ITU. – Режим доступу: http://www.itu.int/wsis/docs2/tunis/off/7.html.

51. WSIS: Tunis Commitment dated 18 November 2005 [Електронний ресурс] // ITU. – Режим доступу: http://www.itu.int/wsis/docs2/tunis/off/7.html.

52. WSIS: Tunis Agenda for the Information Society dated 18 November 2005 [Електронний ресурс] // ITU. – Режим доступу: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

53. Mueller M. Revisiting «roles»: On the agenda for Brazil [Електронний ресурс] / M. Mueller // Blog of the Internet Governance Project (IGP). – 2013. – December 18. – Режим доступу: http://www.internetgovernance.org/2013/12/18/revisiting-roles-on-the-agenda-for-brazil/.

54. Hamelink C. Did WSIS Achieve Anything at All? / C. Hamelink // Gazette: The International Journal For Communication Studies. – 2004. – Vol. 66. – No. 3-4. – Pp. 281-290.

55. McLaughlin L. «No investment, no information society»: Cosmopolitan corporatism and the World Summit on the Information Society / Lisa McLaughlin // Television and New Media. – 2006.

56. Padovani C. The World Summit On The Information Society. Setting the Communication Agenda for the 21st Century? An Ongoing Exercise / C. Padovani // Gazette: The International Journal for Communication Studies. – 2004. – Vol. 66. – Issue 3–4. – Pp. 187–191.

57. Padovani C. From the MacBride Report to the World Summit on the Information Society. Legacies and transformations in global debates around communication imbalances / C. Padovani // *Quaderns del CAC*. International Communication and Communication Policies – XXV Anniversary of the MacBride Report. – 2005. – Issue 21. – Pp. 65-69.

58. Padovani C. From NWICO to WSIS: another world information and communication order? / C. Padovani, K. Nordenstreng // Global Media and Communication. SAGE Publications. – 2005. – Vol. 1(3). – Pp. 264–272.

59. Резолюция ГА ООН A/RES/68/302 «Порядок проведения Генеральной Ассамблеей общего обзора хода осуществления решений Всемирной встречи на высшем

уровне по вопросам информационного общества» от 31 июля 2014 года [Электронный ресурс] // ООН. – Режим доступа: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/302&referer=/english/&Lang=R.

60. GA Resolution A/RES/70/125 «Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society» dated 13 December 2015 [Електронний ресурс] // United Nations General Assembly. – Режим доступу: http://digitalwatch.giplatform.org/printpdf/4428.

61. Summary Report From the UN GA WSIS Review Meeting [Електронний ресурс] // GIP Digital Watch. – Режим доступу: http://digitalwatch.giplatform.org/sites/default/files/WSIS10SummaryReport.pdf.

62. Connect 2020 Agenda for Global Telecommunication / ICT Development [Електронний ресурс] // ITU. – Режим доступу: http://www.itu.int/en/connect2020/Pages/default.aspx.

63. General Assembly Resolution A/RES/70/1 «Transforming our world: the 2030 Agenda for Sustainable Development» dated 25 September 2015 [Електронний ресурс]. – Режим доступу: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.

64. Raboy M. Globalization and Information Society / Marc Raboy // The World Summit on the Information Society: Moving from the Past into the Future [eds. Daniel Stauffacher, Wolfgang Kleinwächter]. – New York, United States: United Nations ICT Task Force, 2005. – Pp. 131-134.

65. Nye J. Governance in a Globalizing World / Joseph S. Nye, John D. Donahue. – Brookings Institution Press, 2000. – 368 p.

66. Padovani C. Communication Governance and the Role of Civil Society: Reflections on Participation and the Changing Scope of Political Action / C. Padovani, A. Tuzzi // Towards a Sustainable Information Society. Deconstructing WSIS. – Bristol UK: Intellect Books, 2006. – Pp. 51-79.

67. Arrangements and Practices for the Interaction of Non-Governmental Organizations in All Activities of the United Nations System [Електронний ресурс] // Report of the Secretary-

General. – 1998. – July 10. – UN Doc. A/53/170. – Режим доступу: http://www.un.org/documents/ga/docs/53/plenary/a53-170.htm.

68. Kleinwächter W. IGF, WSIS 10+ & WIC: Three World Conferences for One Internet [Електронний ресурс] / Wolfgang Kleinwächter. – 2015. – December 21. – Режим доступу: http://www.circleid.com/posts/20151221_igf_wsis_10_wic_three_world_conferences_for_one_internet/.

69. Levinson N. Co-creating Processes in Global Governance: the Case of the Internet Governance Forum [Електронний ресурс] / Nanette S. Levinson. – 2008. – 35 p. – Режим доступу: http://cdm16457.contentdm.oclc.org/cdm/ref/collection/p15430coll1/id/23.

70. Drake W. Multistakeholderism: External Limitations and Internal Limits / W. Drake // MIND: Multistakeholder Internet Dialog, Collaboratory Discussion Paper. – Series No. 2, Internet Policymaking. – Berlin: Collaboratory, 2011. – Pp. 68-72.

71. Final Acts of the World Conference on International Telecommunications [Електронний ресурс] // International Telecommunication Union. – Dubai. – 2012. – Режим доступу: http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.

72. Final Acts of the Plenipotentiary Conference [Електронний ресурс] // ITU. – Busan. – 2014. – Режим доступу: https://www.itu.int/en/plenipotentiary/2014/Documents/final-acts/pp14-final-acts-en.pdf.

73. Kehl D. Final Dispatch From Busan: Closing the Books on the 2014 ITU Plenipotentiary Conference [Електронний ресурс] / Danielle Kehl // New America Weekly. – 2014. – November 10. – Режим доступу: https://www.newamerica.org/oti/final-dispatch-from-busan-closing-thebooksonthe2014ituplenipotentiary-conference/.

74. UNESCO and WSIS Action Lines [Електронний ресурс]. – Режим доступу: http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/unesco-and-wsis/implementation-and-follow-up/unesco-and-wsis-action-lines/.

75. Keystones to Foster Inclusive Knowledge Societies. Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet [Електронний ресурс] // UNESCO. – 2015. – Режим доступу:

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Events/internet_draft_study_simple_version.pdf.

76. The Commission on Science and Technology for Development (CSTD). Mandate and Institutional Background [Електронний ресурс]. – Режим доступу: http://unctad.org/en/Pages/CSTD/CSTD-Mandate.aspx.

77. Working Group on Enhanced Cooperation Note on Membership [Електронний ресурс]. – 2013. – March 22. – Режим доступу: http://unctad.org/Sections/un_cstd/docs/cstd2013d04_Membership.pdf.

78. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [Електронний ресурс] // Note by the Secretary-General A/70/174. – 2015. – Режим доступу: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=E.

79. Resolution A/RES/70/237 «Developments in the field of information and telecommunications in the context of international security» [Електронний ресурс] // General Assembly. – 2015. – December 23. – Режим доступу: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf.

80. Gross R. World Intellectual Property Organisation (WIPO) [Електронний ресурс] / Robin Gross // GISWatch. – 2007. – Режим доступу: https://www.giswatch.org/institutional-overview/civil-society-participation/world-intellectual-property-organisation-wipo.

81. Geneva Declaration on the Future of the World Intellectual Property Organization [Електронний ресурс]. – Режим доступу: http://www.futureofwipo.org/futureofwipodeclaration.pdf.

82. Development Agenda for WIPO [Електронний ресурс]. – Режим доступу: http://www.wipo.int/ip-development/en/agenda/.

83. What Is The Open Government Partnership? [Електронний ресурс]. – Режим доступу: http://www.opengovpartnership.org/about.

84. Freedom Online Coalition. About Us [Електронний ресурс]. – Режим доступу: https://www.freedomonlinecoalition.com/about/.

85. London Conference on Cyberspace – Chairman's summary [Електронний ресурс]. – 2011. – Режим доступу: https://www.gccs2015.com/sites/default/files/documents/London%20Conference%20on%20Cyberspace%20-%20Chair%27s%20Summary%20-%201-2%20Nov%202011%20_1_.pdf.

86. Seoul Framework for and Commitment to Open and Secure Cyberspace [Електронний ресурс]. – 2013. – Режим доступу: http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf.

87. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98 dated 24 June 2013 [Електронний ресурс]. – Режим доступу: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

88. Global Conference on Cyberspace 2015. Chair's Statement [Електронний ресурс]. – Режим доступу: https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf.

89. Remarks by H. E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference [Електронний ресурс]. – Wuzhen. – 2015. – December 16. – Режим доступу: http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

90. The 2nd WIC Organizing Committee proposes the Wuzhen Initiative [Електронний ресурс]. – 2015. – December 18. – Режим доступу: http://www.wuzhenwic.org/2015-12/18/c_48241.htm.

91. Wuzhen Declaration dated 21 November 2014 [Електронний ресурс]. – Режим доступу: http://www.theregister.co.uk/2014/11/22/china_wuzhen_world_internet_conference_overview/?page=2.

92. Wuzhen Summit Community Statement dated 20 November 2014 [Електронний ресурс]. – Режим доступу: http://www.circleid.com/posts/20141120_community_statement_presented_at_wuzhen_summit/.

93. Wuzhen 2015: Evaluating China's Competing Vision of the Internet [Електронний ресурс]. – 2016. – January 21. – Режим доступу: https://ccgnludelhi.wordpress.com/2016/01/21/wuzhen-2015-evaluating-chinas-competing-vision-of-the-internet/.

94. Mozur P. To Reach China, LinkedIn Plays by Local Rules [Електронний ресурс] / Paul Mozur, Vindu Goeloct // New York Times. – 2014. – October 5. – Режим доступу: http://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html?_r=0.

95. Internet freedom faces new attack as China seeks to shape global web rules [Електронний ресурс]. – 2014. – November 18. – Режим доступу: https://www.amnesty.org/en/latest/news/2014/11/internet-freedom-faces-new-attack-china-seeks-shape-global-web-rules/.

96. China Freedom on the Net 2015 [Електронний ресурс]. – Режим доступу: https://freedomhouse.org/report/freedom-net/2015/china.

97. Передача координирующей роли NTIA в осуществлении функций IANA [Электронный ресурс]. – Режим доступа: https://www.icann.org/ru/stewardship.

98. Malcolm J. Appraising the Success of the Internet Governance Forum [Електронний ресурс] / J. Malcolm. – 2008. – November 21. – Режим доступу: http://www.internetgoverance.org.

99. Принципи NETmundial [Електронний ресурс]. – Режим доступу: https://www.netmundial.org/ru/%D0%BF%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D1%8B-netmundial.

100. Remark by member of ICANN Board of Directors Sébastien Bachollet at Third International Forum «Media for information society». – Kyiv, Ukraine. – 2014. – October 02.

101. Кирилюк О. В. Концепція глобального інформаційного суспільства в міжнародному праві / О. В. Кирилюк // Український часопис міжнародного права. – 2013. – № 4. – С. 120-125.

102. Кирилюк О. В. Основні етапи становлення міжнародно-правового регулювання розвитку глобального інформаційного суспільства / О. В. Кирилюк // Актуальні проблеми

міжнародних відносин: Збірник наукових праць. – К.: КНУ ІМВ, 2014. – Вип. 122. – Ч. ІІ. – С. 45-56.

103. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства / О. В. Кирилюк // Актуальні проблеми міжнародних відносин: Збірник наукових праць. – К.: КНУ ІМВ, 2015. – Вип. 126. – Ч. ІІ. – С. 77-90.

104. Кирилюк О. Міжнародно-правове регулювання розвитку глобального інформаційного суспільства / О. Кирилюк // Шевченківська весна: Матеріали міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених. К.: КНУ ІМВ, 2014. – Ч. 1. – С. 183-188.

105. Goldsmith J. Who controls the Internet: illusions of a borderless world / Jack Goldsmith, Tim Wu. – New York: Oxford University Press, 2006. – 240 p.

106. Schmitt M. The Nature of International Law Cyber Norms [Електронний ресурс] / Michael N. Schmitt, Liis Vihul // Tallinn Paper. – 2014. – No. 5. – Special Expanded Issue. – 35 p. – Режим доступу: https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf.

107. Developments in the field of information and telecommunications in the context of international security [Електронний ресурс] // Report of the Secretary-General A/68/156. – 2013. – July 16. – Режим доступу: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/156.

108. Chart of signatures and ratifications of Treaty 185 – Convention on Cybercrime [Електронний ресурс]. – Status as of April 05, 2016. – Режим доступу: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VMZitgWl.

109. Pagallo U. The Realignment of the Sources of the Law and their Meaning in an Information Society / Ugo Pagallo // Philosophy & Technology. – March 2015. – Vol. 28. – Issue 1. – Springer Netherlands. – Pp. 57-73.

110. Ago R. Science juridique et droit international / R. Ago // Recueil des cours. – 1956. – Vol. 90. – Pp. 851-958.

111. North Sea Continental Shelf Cases (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands) [Електронний ресурс] // ICJ Reports of Judgments, Advisory Opinions and Orders. – Judgment as of 20 February 1969. – Режим доступу: http://www.icj-cij.org/docket/files/52/5561.pdf.

112. Cheng B. United Nations Resolutions on Outer Space: «Instant» International Customary Law? / Bin Cheng // Studies in International Space Law. – Oxford: Clarendon Press, 1997. – Pp. 125-150.

113. Wiegandt J. Internationale Rechtsordnung oder Machtordnung? Eine Anmerkung zum Verhältnis von Macht und Recht im Völkerrecht / Jan Wiegandt // Zeitschrift fur auslandisches offentliches Recht und Volkerrecht. – 2011. – No. 21. – Pp. 31-76.

114. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World [Електронний ресурс] // The White House. – 2011. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cybers pace.pdf.

115. Chik W. «Customary Internet-ional Law»: Creating a Body of Customary Law for Cyberspace. Part 1: Developing Rules for Transitioning Custom into Law / Warren B. Chik // *Computer Law and Security Review*. – 2010. – Vol. 26. – Issue 1. – Pp. 3-22.

116. McDougal M. Theories about International Law: Prologue to a Configurative Jurisprudence / Myres S. McDougal, Harold D. Lasswell, W. Michael Reisman // Virginia Journal of International Law. – 1968. – Vol. 8. – Issue 2. – Pp. 188-299.

117. Ochoa C. The Individual and Customary International Law Formation / Christiana Ochoa // Virginia Journal of International Law. – 2007. – Vol. 48. – Issue 1. – Pp. 119-186.

118. Weber R. Overcoming the Hard Law / Soft Law Dichotomy in Times of (Financial) Crises / Rolf H. Weber // Journal of Governance and Regulation. – 2012. – Vol. 1. – Issue 1. – Pp. 8–14.

119. Gadbaw R. Systemic Regulation of Global Trade and Finance: A Tale of Two Systems / R. Michael Gadbaw // Journal of International Economic Law. – 2010. – Vol. 13. – Pp. 551–574.

120. Демин А. В. «Мягкое право» в эпоху перемен: опыт компаративного исследования. Монография / А. В. Демин. – Изд-во «Проспект», 2015. – 233 с.

121. Нешатаева Т. Н. Международные организации и право. Новые тенденции в международно-правовом регулировании / Т. Н. Нешатаева. – М.: Дело, 1998. – 272 с.

122. Snyder F. Soft law and institutional practice in the European Community / Francis Snyder // The Construction of Europe. Essays in Honour of Emile Noël. – Springer Netherlands, 1994. – Pp. 197-225.

123. Лукашук И. И. Международное «мягкое» право / И. И. Лукашук // Государство и право. – 1994. – № 8-9. – С. 159-167.

124. Yanaga M. Standards and Statutes: 'Soft' Law and 'Hard' Law / Masao Yanaga // Cybernics: Fusion of human, machine and information systems [eds. Y. Sankai, Ke. Suzuki, Y. Hasegawa]. – Springer Japan, 2014. – P. 315-333.

125. Бігун В. С. Євген Ерліх: життя і правознавча спадщина (актуальний наукознавчий нарис) / В. С. Бігун // Проблеми філософії права. – 2005. – Т. 3. – С. 105-126.

126. Lessig L. Code: Version 2.0. / Lawrence Lessig. – New York: Basic Books, 2006. – 424 p.

127. Lodge M. Comparing non-hierarchical governance in action: The open method of co-ordination in pensions and information society / M. Lodge // Journal of Common Market Studies. – 2007. – Vol. 45. – No. 2. – Pp. 343–365.

128. Simpson S. Governing information infrastructures and services: states, markets and the public interest in telecommunications / S. Simpson // Aslib Proceedings. – 2010. – Vol. 62. – No. 1. – Pp. 46–56.

129. Директива 2000/31/ЄС Європейського парламенту та Ради «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку» (Директива про електронну комерцію) від 8 червня 2000 року [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_224.

130. Kesan J. P. Why are the United States and the European Union failing to regulate the internet efficiently? Going beyond the bottom-up and top-down alternatives /

Jay P. Kesan, Andres A. Gallo // European Journal of Law and Economics. – May 2006. – Vol. 21. – Issue 3. – Pp. 237-266.

131. Jessup P. Transnational law / Philip C. Jessup. – New Haven: Yale University Press, 1956. – 113 p.

132. Solum L. B. Models of Internet governance / L. B. Solum // Internet governance: infrastructure and institutions [eds. L. A. Bygrave, J. Bing]. – New York: Oxford University Press, 2009. – Pp. 48–91.

133. Halliday T. C. Globalization of law / T. C. Halliday, P. Osinsky // Annual Review of Sociology. – 2006. – Vol. 32. – Pp. 447–470.

134. Pagallo U. Cracking down on autonomy: three challenges to design in IT law / U. Pagallo // Ethics and Information Technology. – 2012. – Vol. 14. – Issue 4. – Pp. 319–328.

135. Reed C. Making laws for cyberspace / C. Reed. – Oxford University Press, 2012. – 228 p.

136. Загальна декларація прав людини від 10 грудня 1948 року [Електронний ресурс] // Офіційний веб-портал Верховної Ради України. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/995_015.

137. OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions [Електронний ресурс] // IMF. – 2001. – September 18. – 47 p. – Режим доступу: https://www.imf.org/external/np/gov/2001/eng/091801.pdf.

138. Kellman B. The Soft Law of Nuclear Materials Protection / Barry Kellman // Commitment and Compliance: the Role of Non-Binding Norms in the International Legal System [ed. D. Shelton]. – Oxford University Press, 2000. – Pp. 486-505.

139. Abbott K. Hard and Soft Law in International Governance / Kenneth W. Abbott, Duncan Snidal // International Organization. – 2000. – Vol. 54. – Issue 3. – Pp. 421–456.

140. Віденська конвенція про охорону озонового шару від 22.03.1985 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/995_088.

141. Роттердамська конвенція про процедуру Попередньої обґрунтованої згоди відносно окремих небезпечних хімічних речовин та пестицидів у міжнародній торгівлі від

10 вересня 1998 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/995_a35.

142. Вассенаарська домовленість щодо контролю за експортом звичайних озброєнь та товарів і технологій подвійного використання від 01 липня 1996 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/998_177.

143. Armstrong D. Law, Justice and the Idea of a World Society / David Armstrong // International Affairs. – July 1999. – Vol. 75. – Issue 3. – Pp. 547-561.

144. McGoldrick D. Sustainable development and human rights: an integrated conception / Dominic McGoldrick // International and Comparative Law Quarterly. – October 1996. – Vol. 45. – Issue 04. – Pp. 796-818.

145. Bellia P. Cyberlaw: Problems of Policy and Jurisprudence in the Information Age / Patricia L. Bellia, Paul Schiff Berman, David G. Post. – West Group, 2007. – 803 p.

146. Holmes O. The Path of the Law: Conflicting Views of the Legal World / Oliver Wendell Holmes Jr. // The American Journal of Legal History. – July 1985. – Vol. 29. – No. 3. – Pp. 235-250.

147. The mapping of international Internet public policy issues [Електронний ресурс] // Intersessional Panel of the Commission on Science and Technology for Development. – 2014. – November 21. – Режим доступу: http://unctad.org/meetings/en/SessionalDocuments/CSTD_2014_Mapping_Internet_en.pdf.

148. Braman S. Change of State: Information, Policy, and Power / Sandra Braman. – Cambridge, MA: The MIT Press, 2006. – 545 p.

149. Rustad M. Legal Resources for Lawyers Lost in Cyberspace / Michael L. Rustad // Suffolk University Law Review. – 1996. – Vol. 30.

150. Marsden C. T. Introduction: information and communication technologies, globalisation and regulation / C. T. Marsden // Regulating the Global Information Society. – London: Routledge, 2000. – Pp. 1-40.

151. Chander A. The Electronic Silk Road: How the Web Binds the World Together in Commerce / Anupam Chander. – Yale University Press, 2013. – 296 p.

152. Easterbrook F. Cyberspace and the Law of the Horse / Frank H. Easterbrook // The University of Chicago Legal Forum. – 1996. – Pp. 207-216.

153. Sommer J. Against Cyberlaw / Joseph H. Sommer // Berkeley Technology Law Journal. – September 2000. – Vol. 15. – Issue 3. – Pp. 1145-1232.

154. Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

155. Benkler Y. From Consumers to Users: Shifting Deeper Structures of Regulation Toward Sustainable Commons and User Access / Yochai Benkler // Federal Communications Law Journal. – 2000. – Vol. 52. – Issue 3. – Article 9. – 561-579.

156. Mueller M. Networks and States: the Global Politics of Internet Governance / Milton L. Mueller. – The MIT Press, 2013. – 320 p.

157. Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations [Електронний ресурс] // ITU. – 1998. – Режим доступу: http://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf.

158. Конвенция о правах ребенка от 20 ноября 1989 года [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/childcon.shtml.

159. Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии от 25 мая 2000 года [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/conventions/rightschild_protocol2.shtml.

160. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) dated 25.10.2007 [Електронний ресурс]. – Режим доступу: http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084822.

161. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093.

162. Charter on the Preservation of the Digital Heritage [Електронний ресурс] // UNESCO. – Paris. – 2003. – October 17. – 4 p. – Режим доступу:

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/charter_preservation_digital_heritage_en.pdf.

163. Convention on Information and Legal Co-operation concerning «Information Society Services» dated 04.10.2001 [Електронний ресурс]. – Режим доступу: http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080625.

164. Recommendation CM/Rec(2015)6 on the free, transboundary flow of information on the Internet [Електронний ресурс]. – Режим доступу: https://edoc.coe.int/en/internet/6806-free-transboundary-flow-of-information-on-the-internet-recommendation-cmrec20156.html.

165. Internet Governance - Council of Europe Strategy 2016-2019. Democracy, human rights and the rule of law in the digital world dated 30 March 2016 [Електронний ресурс]. – Режим доступу: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c1b60.

166. Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999D0276.

167. eEurope: an information society for all. Communication on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000. COM (99) 687 final, 8 December 1999 [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24221.

168. Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Asi0016.

169. Концепция формирования информационного пространства Содружества Независимых Государств от 18 октября 1996 [Электронный ресурс]. – Режим доступа: http://zakon3.rada.gov.ua/laws/show/997_185.

170. Санкт-Петербургская декларация «Обеспечение доверия и безопасности в использовании ИКТ для содействия экономическому росту и процветанию» от 8 августа 2012 года [Электронный ресурс]. – Режим доступа: http://minsvyaz.ru/ru/documents/3705/.

171. G8 Declaration: Renewed Commitment for Freedom and Democracy [Електронний ресурс] // G8 Summit of Deauville. – 2011. – May 26-27. – Режим доступу: http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html.

172. G20 Leaders' Communiqué Antalya Summit of 15-16 November 2015 [Електронний ресурс]. – Режим доступу: http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

173. Communique on Principles for Internet Policy-Making [Електронний ресурс] // OECD High Level Meeting «The Internet Economy: Generating Innovation and Growth». – 2011. – June 28-29. – Режим доступу: http://www.oecd.org/dataoecd/33/12/48387430.pdf.

174. Gruenwald J. Intellectual Property Organization Stumped / Juliana Gruenwald // Interactive Week. ZD News. – 2001. – 01 February.

175. Товарные знаки и Интернет [Электронный ресурс] // ВОИВ. – 11 февраля 2011 года. – Режим доступа: http://www.wipo.int/edocs/mdocs/sct/ru/sct_25/sct_25_3.pdf.

176. Montreux Declaration «The protection of personal data and privacy in a globalised world: a universal right respecting diversities» [Електронний ресурс] // 27th International Conference of Data Protection and Privacy Commissioners. – 2005. – Режим доступу: https://www.itu.int/net/wsis/docs2/pc3/contributions/misc/montreux-declaration.pdf.

177. Ufa Declaration [Електронний ресурс] // VII BRICS Summit. – 9 July 2015. – Режим доступу: http://mea.gov.in/Uploads/PublicationDocs/25448_Declaration_eng.pdf.

178. IPU Resolution: Democracy in the Digital Era and the Threat to Privacy and Individual Freedoms [Електронний ресурс] // GIP Digital Watch. – 21 October 2015. – Режим доступу: http://digitalwatch.giplatform.org/instruments/ipu-resolution-democracy-digital-era-and-threat-privacy-and-individual-freedoms.

179. Alexander A. Digital surveillance 'worse than Orwell', says new UN privacy chief [Електронний ресурс] / Adam Alexander // The Guardian. – 24 August 2015. – Режим доступу: http://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief.

180. The Snowden Treaty: A new International Treaty on the Right to Privacy, Protection against Improper Surveillance and Protection of Whistleblowers [Електронний ресурс]. – Режим доступу: http://media.wix.com/ugd/fb845b_89e20fe385844f348fbc79a6ede39a4d.pdf.

181. Fidler D. The Proposed Snowden Treaty: More of the Same Rather than Really Radical [Електронний ресурс] / David Fidler // Council on Foreign Relations. – 2015. – October 12. – Режим доступу: http://blogs.cfr.org/cyber/2015/10/12/the-proposed-snowden-treaty-more-of-the-same-rather-than-really-radical/.

182. Milanovic M. Human Rights Treaties and Foreign Surveillance [Електронний ресурс] / Marko Milanovic // EJIL: Talk! Blog of the European Journal of International Law. – 2015. – September 28. – Режим доступу: http://www.ejiltalk.org/human-rights-treaties-and-foreign-surveillance/.

183. Leidel S. Some governments don't want to discuss mass surveillance [Електронний ресурс] / Steffen Leidel // Deutsche Welle. – 2015. – November 13. – Режим доступу: http://www.dw.com/en/some-governments-dont-want-to-discuss-mass-surveillance/a-18848685.

184. Farrell H. Promoting Norms for Cyberspace [Електронний ресурс] / Henry Farrell // Council on Foreign Relations. – April 2015. – Режим доступу: http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358.

185. Талимончик В. П. Международно-правовое регулирование отношений информационного обмена / В. П. Талимончик. – М.: Юридический центр Пресс, 2015. – 384 с.

186. Jayasuriya K. Globalization, Law, and the Transformation of Sovereignty: The Emergence of Global Regulatory Governance / Kanishka Jayasuriya // Indiana Journal of Global Legal Studies. – Spring 1999. – Vol. 6. – Issue 2. – Article 3. – Pp. 425-455.

187. 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.

188. Bogdandy A., Venzke I. Beyond Dispute: International Judicial Institutions as Lawmakers / Armin von Bogdandy, Ingo Venzke // International Judicial Lawmaking. – Springer Berlin Heidelberg, 2012. – Pp. 3-33.

189. Dolzer R., Schreuer C. Principles of International Investment Law / Rudolf Dolzer, Christoph Schreuer. – Oxford University Press, 2012. – 456 p.

190. Koskenniemi M. Constitutionalism as Mindset: Reflections on Kantian Themes about International Law and Globalization / Martti Koskenniemi // Theoretical Inquiries in Law. – Vol 8. – No. 1. – 2007. – Pp. 9-36.

191. Kelsen H. Reine Rechtslehre: Einleitung in die rechtswissenschaftliche Problematik [herausgeben von M. Jestaedt] / Hans Kelsen. – Mohr Siebeck, 2008 (Studienausg. 1934). – 181 s.

192. Brandom R. B. Some Pragmatist Themes in Hegel's Idealism: Negotiation and Administration in Hegel's Account of the Structure and Content of Conceptual Norms / Robert B. Brandom // European Journal of Philosophy. – Vol. 7. – Issue 2. – August 1999. – Pp. 164–189.

193. Kirchner C. Zur konsequentialistischen Interpretationsmethode / Christian Kirchner // Internationalisierung des Rechts und seine ökonomische Analyse. – Gabler Wiesbaden, 2008. – P. 37-49.

194. Reidenberg J. R. Technology and Internet Jurisdiction / Joel R. Reidenberg // University of Pennsylvania Law Review. – Vol. 153. – No. 6. – June 2005. – Pp. 1951-1974.

195. Report of the Director General to the WIPO Assemblies 2015 [Електронний ресурс] // WIPO. – Режим доступу: http://www.wipo.int/edocs/pubdocs/en/wipo_pub_1050_15.pdf.

196. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [Електронний ресурс] / Judgment of the Court (Grand Chamber) as of 13 May 2014 // EUR-Lex: Access to European Union law. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

197. Right to delisting: Google informal appeal rejected [Електронний ресурс] // Commission Nationale de l'Informatique et des Libertés (CNIL). – 21 September 2015. – Режим доступу: https://www.cnil.fr/fr/node/15814.

198. Fleischer P. Implementing a European, not global, right to be forgotten [Електронний ресурс] / Peter Fleischer // Google Europe Blog. – 2015. – July 30. – Режим доступу: http://googlepolicyeurope.blogspot.com/2015/07/implementing-european-not-global-right.html.

199. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána

[Електронний ресурс] / Judgment of the Court (Grand Chamber) as of 8 April 2014 // InfoCuria - Case-law of the Court of Justice. – Режим доступу: http://curia.europa.eu/juris/document/document.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=150642&occ=first&dir=&cid=99319%20(judgment,%20advisory%20opinions,%20resolutions,%20dissenting%20opinions).

200. Weltimmo S. R. O. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [Електронний ресурс] // InfoCuria - Case-law of the Court of Justice. – 1 October 2015. – Режим доступу: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddaeee4666aaf8474e8ec3817bab8f982e.e34KaxiLc.3qMb40Rch0SaxuRb3j0?text=&docid=168944&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=305205.

201. BestWater International GmBH v. Mebes [Електронний ресурс] / ECJ. – 2014. – October 21. – Режим доступу: https://globalfreedomofexpression.columbia.edu/cases/bestwater-international-gmbh-v-mebes/.

202. Svensson v. Sverige AB [Електронний ресурс] / ECJ. – 2014. – February 13. – Режим доступу: https://globalfreedomofexpression.columbia.edu/cases/svensson-v-sverige-ab/.

203. Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [Електронний ресурс] / ECJ. – 2011. – November 24 // EUR-Lex: Access to European Union law. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070.

204. Vorlage an den EuGH in Sachen ‘Speicherung von dynamischen IP-Adressen’ [Електронний ресурс] // Pressestelle des Bundesgerichtshofs. – Nr. 152/2014. – Режим доступу: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=69184&pos=0&anz=152.

205. Joined Cases «eDate Advertising GmbH v. X» and «Olivier Martinez and Robert Martinez v. MGN Limited» [Електронний ресурс] / ECJ. – 2011. – October 25 // EUR-Lex: Access to European Union law. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009CJ0509:EN:HTML.

206. Delfi AS v. Estonia [Електронний ресурс] / ECHR. – 2015. – June 16. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-155105.

207. Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary [Електронний ресурс] / ECHR. – 2016. – February 2. – Режим доступу: http://hudoc.echr.coe.int/eng#{"itemid":["001-160314"]}.

208. Affaire Cengiz et Autres c. Turquie [Електронний ресурс] // Cour européenne des droits de l'homme. – 2015. – December 01. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-158948.

209. Akdeniz c. Turquie [Електронний ресурс] // Cour européenne des droits de l'homme. – 2014. – March 11. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-142383.

210. Ahmet Yıldırım v. Turkey [Електронний ресурс] // ECHR. – 2012. – December 18. – Режим доступу: http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115705#{"itemid":["001-115705"]}.

211. Copland v. the United Kingdom [Електронний ресурс] // ECHR. – 2007. – April 03. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-79996.

212. Bărbulescu v. Romania [Електронний ресурс] // ECHR. – 2016. – December 01. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-159906.

213. Roman Zakharov v. Russia [Електронний ресурс] // ECHR. – 2015. – December 04. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-159324.

214. Editorial Board of Pravoye Delo and Shtekel v. Ukraine [Електронний ресурс] // ECHR. – 2011. – May 05. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-104685.

215. Gazeta Ukraina-Tsentr v. Ukraine [Електронний ресурс] // ECHR. – 2010. – July 15. – Режим доступу: http://hudoc.echr.coe.int/fre-press?i=003-3199714-3564889.

216. Order Compelling Apple Inc. to Assist Agents in Search [Електронний ресурс]. – No. ED 15-0451M. – US District Court for the Central District of California. – 2016. – February 16. – Режим доступу: https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf .

217. Amicus Briefs in Support of Apple [Електронний ресурс] // Apple Press Info. – Режим доступу: https://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html.

218. McLaughlin J. New Court Filing Reveals Apple Faces 12 Other Requests to Break Into Locked iPhones / Jenna McLaughlin // The Intercept. – 2016. – February 23. – Режим доступу: https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/.

219. Memorandum and Order 15-MC-1902 (JO) / United States District Court Eastern District of New York. – 2016. – February 29. – Режим доступу: https://drive.google.com/file/d/0B7EX8WXpPipGQ2xCclNzb1JoQnM/view?pref=2&pli=1.

220. National Association of the Deaf, et al. v. Harvard University [Електронний ресурс]. – United States District Court District of Massachusetts. – 09 February 2016. – Режим доступу: http://creeclaw.org/wp-content/uploads/2016/02/2016-02-09-50-Report-and-Rec-re-MTD.pdf.

221. United States v. Cotterman [Електронний ресурс]. – United States Court of Appeals for the Ninth Circuit. – No. 09-10139. – 08 March 2013. – Режим доступу: http://cdn.ca9.uscourts.gov/datastore/opinions/2013/03/08/09-10139.pdf.

222. Lulu Chang Germans granted right to be left alone as court rules FB's Friend Finder illegal [Електронний ресурс] // Digital Trends. – 2016. – January 17. – Режим доступу: http://www.digitaltrends.com/social-media/facebook-friend-finder-illegal-in-germany/#ixzz41vm2q1ZQ.

223. Cour D'Appel De Paris [Електронний ресурс]. – 2016. – Fevrier 12. – No. 2016-58. – Режим доступу: http://www.cottineau.net/wp-content/uploads/2016/02/facebook-jugement-cour-appel-paris-12-fevrier-2016.pdf.

224. Yahoo! Inc. v. LICRA and UEJF // United States Court of Appeals, Ninth Circuit. – 433 F.3d 1199. – 2006. – January 12.

225. R v. Graham Waddon [Електронний ресурс]. – Southwark Crown Court. – 1999. – June 30. – Режим доступу: http://www.out-law.com/page-8683.

226. Dow Jones & Company Inc. v Gutnick [Електронний ресурс]. – HCA 56. – 2002. – December 10. – Режим доступу:

http://www.kentlaw.edu/perritt/courses/civpro/Dow%20Jones%20&%20Company%20Inc_%20v%20Gutnick%20%5B2002%5D%20HCA%2056%20(10%20December%202002).htm.

227. EMI Records (Ireland) Ltd & ors v. Eircom Ltd [Електронний ресурс]. – High Court of Ireland. – 16.04.2010. – Режим доступу:http://www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d884080257707003508 2f?OpenDocument.

228. Кирилюк О. В. Международно-правовые основы саморегулирования в киберпространстве / О. В. Кирилюк // Право. Журнал Высшей школы экономики. – М., 2016. – № 1. – С. 177–188.

229. Кирилюк О. В. М'яке право як нормативна основа глобального інформаційного суспільства / О. В. Кирилюк // Актуальні проблеми міжнародних відносин: Збірник наукових праць. – К.: КНУ ІМВ, 2015. – Вип. 125. – Ч. І. – С. 106-117.

230. Кирилюк О. Саморегулювання як спосіб міжнародної правотворчості в інформаційній сфері / О. Кирилюк // Актуальні проблеми міжнародних відносин: Матеріали міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених. – К.: КНУ ІМВ, 2015. – Ч. 1. – С. 123-126.

231. Кирилюк О. Перспективи універсального нормативно-правового регулювання Інтернету / О. Кирилюк // Актуальні проблеми міжнародних відносин: Матеріали міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених. – К.: КНУ ІМВ, 2014. – Ч. 1. – С. 177-180.

232. Кирилюк О. Роль судової практики у формуванні основ міжнародно-правового регулювання глобального інформаційного суспільства / О. Кирилюк // Шевченківська весна: Матеріали міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених. – К.: КНУ ІМВ, 2016. – Ч. 1. – С. 123-126.

233. Кирилюк О. В. Нормативно-правові засади розвитку світового інформаційного суспільства: регіональний та глобальний вимір / О. В. Кирилюк // Інтеграція України в європейський інформаційний простір: виклики та завдання. Колективна монографія. – К.: ФОП Клименко, 2014. – С. 45-74.

234. Facebook says governments demanding more and more user data [Електронний ресурс]. – 2015. – November 12. – Режим доступу:

http://www.theguardian.com/world/2015/nov/12/facebook-says-governments-seek-more-and-more-user-data-and-takedowns.

235. Bobbio N. Presente e avvenire dei diritti dell'uomo [Електронний ресурс] / N. Bobbio. – 1988. – Режим доступу: http://www.giuffre.it/age_files/dir_tutti/strenne/1988/Presente%20e%20avvenire%20dei%20diritti%20dell'uomo%20-%20Norberto%20Bobbio.pdf.

236. O'Brien D. Governments Taking Techies Offline: 2015 in Review [Електронний ресурс] / Danny O'Brien // Electronic Frontier Foundation. – 2016. – January 1. – Режим доступу: https://www.eff.org/deeplinks/2015/12/too-familiar-story-technologists-jail-2015-review.

237. HRC Resolution A/HRC/20/L.13 «The Promotion, Protection and Enjoyment of Human Rights on the Internet» dated 29 June 2012 [Електронний ресурс]. – Режим доступу: http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement.

238. Kettemann M. C. UN Human Rights Council Confirms that Human Rights Apply to the Internet [Електронний ресурс] / Matthias C. Kettemann // EJIL: Talk!. – 2012. – July 23. – Режим доступу: http://www.ejiltalk.org/un-human-rights-council-confirms-that-human-rights-apply-to-the-internet/#more-5207.

239. Kopstein J. Digital rights are human rights [Електронний ресурс] / J. Kopstein. – 2016. – February 3. – Режим доступу: http://america.aljazeera.com/opinions/2016/2/digital-rights-are-human-rights.html.

240. Gawrońska M. Human Rights in the Digital World [Електронний ресурс] / M. Gawrońska. – 2015. – November 13.– Режим доступу: http://www.gmfus.org/blog/2015/11/13/human-rights-digital-world.

241. Sartor G. Human Rights in the Information Society / G. Sartor // Philosophical Dimensions of Human Rights. – Springer Netherlands, 2012. – Pp. 293-307.

242. Berger C. Human rights aren't enough anymore - we need a new strategy [Електронний ресурс] / C. Berger. – 2015. –December 17. – Режим доступу: https://www.opendemocracy.net/wfd/cathleen-berger/human-rights-aren-t-enough-any-more-we-need-new-strategy.

243. McDiarmid A., Shears M. The Importance of Internet Neutrality to Protecting Human Rights Online / A. McDiarmid, M. Shears // Net Neutrality Compendium. – Springer International Publishing, 2016. – Pp. 31-41.

244. McKune S. Blog #6 Utilizing the UN Human Rights Mechanisms for the Advancement of Digital Rights [Електронний ресурс] / S. McKune // WG 1 – An Internet Free and Secure: Blog Series. – 2015. – April 24. – Режим доступу: https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog-6/.

245. Cerf V. Internet Access Is Not a Human Right [Електронний ресурс] / Vinton G. Cerf // The New York Times. – 2012. – January 04. – Режим доступу: http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=1.

246. Rampton J. Is Internet Access a Human Right? Mark Zuckerberg Thinks So [Електронний ресурс] / J. Rampton. – 2015. – October 23. – Режим доступу: http://www.entrepreneur.com/article/251942.

247. 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] // EUR-Lex: Access to European Union law. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

248. Code of EU Online Rights, European Commission [Електронний ресурс]. – Luxembourg. – 2012. – Режим доступу: https://ec.europa.eu/digitalagenda/sites/digitalagenda/files/Code%20EU%20online%20rights%20EN%20final%202.pdf.

249. Regina v. Smith & Others [Електронний ресурс]. – EWCA Crim 1772 § 20. – England and Wales' Court of Appeal. – 2011. – Режим доступу: http://www.bailii.org/ew/cases/EWCA/Crim/2011/1772.html.

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

251. Michael Karanicolas on Digital Citizens, Human Rights, and Internet Freedom [Електронний ресурс] // The Digital Public Square. – 2015. – September 17. – Режим доступу: https://digitalpublicsquare.com/2015/09/17/interview-with-michael-karanicolas/.

252. Jarvis J. A Bill of Rights in Cyberspace [Електронний ресурс] / Jeff Jarvis // BuzzMachine. – Режим доступу: http://www.buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/.

253. Freedom on the Net 2015 [Електронний ресурс] // Freedom House. – October 2015. – Режим доступу: https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf.

254. Ukraine: Country Report [Електронний ресурс] / Freedom on the Net 2015 // Freedom House. – October 2015. – Режим доступу: https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Ukraine.pdf.

255. The right to privacy in the digital age [Електронний ресурс] // Report of the Office of the United Nations High Commissioner for Human Rights. – 2014. – June 30. – Режим доступу: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

256. Wong C. Internet at a Crossroads. How Government Surveillance Threatens How We Communicate [Електронний ресурс] / Cynthia Wong. – Режим доступу: https://www.hrw.org/world-report/2015/essays/internet-crossroads.

257. Toward a Social Compact for Digital Privacy and Security [Електронний ресурс] / Global Commission on Internet Governance. – 15 April 2015. – Режим доступу: https://www.chathamhouse.org/publication/toward-social-compact-digital-privacy-and-security.

258. Ülgen S. Governing Cyberspace: A Road Map for Transatlantic Leadership [Електронний ресурс] / Sinan Ülgen. – Carnegie Europe. – 2016. – Режим доступу: http://carnegieendowment.org/files/Sinan_Cyber_Final.pdf.

259. National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law [Електронний ресурс] / European Parliament. – 2013. – Режим доступу: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

260. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users dated 16 April 2014 [Електронний ресурс]. – Режим доступу: https://wcd.coe.int/ViewDoc.jsp?id=2184807.

261. Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality dated 13 January 2016 [Електронний ресурс]. – Режим доступу: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2016)1&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

262. Renewing dialogue, rebuilding trust, restoring security [Електронний ресурс] // Speech by Dr Frank-Walter Steinmeier, Chairperson-in-Office, to the OSCE Permanent Council. – Vienna. – 2016. – January 14. – Режим доступу: http://www.osce.org/pc/216716?download=true.

Marco Civil da Internet (unofficial English translation) [Електронний ресурс] // Cultura Digital e Democracia. – Режим доступу: https://thecdd.files.wordpress.com/2014/10/marco-civil-lei-nc2ba-12-965-2014-unnoficial-mirrored-english-translation.pdf.

263. Rossini C., Cruz F., Doneda D. The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet / C. Rossini, F. Brito Cruz, Danilo Doneda // Paper Series: No. 19. – September 2015. – Режим доступу: https://www.cigionline.org/sites/default/files/no19_0.pdf.

264. Country Report: Brazil's Marco Civil da Internet [Електронний ресурс] / ARTICLE 19. – 2015. – November 05. – Режим доступу: https://www.article19.org/resources.php/resource/38175/en/country-report:-brazil's-marco-civil-da-internet.

265. Указ Президента України «Про Стратегію сталого розвитку «Україна – 2020»» від 12 січня 2015 року № 5/2015 [Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/5/2015.

266. The Queen v. Minister of Agriculture, Fisheries & Food, ex parte Trevor Robert Fisher and Penny Fisher, trading as ‘TR and P Fisher’ [Електронний ресурс] / ECJ // InfoCuria - Case-law of the Court of Justice. – No. C-369/98. – 2000. – September 14.

267. Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v. Österreichischer Rundfunk [Електронний ресурс] / ECJ // InfoCuria - Case-

law of the Court of Justice. – Joined cases C-465/00, C-138/01 and C-139/01. – 2003. – May 20. – Режим доступу: http://curia.europa.eu/juris/document/document.jsf?text=&docid=48330&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=405872.

268. Amann v. Switzerland [Електронний ресурс] / ECHR. – No. 27798/95. – 2000. – February 16. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-58497.

269. Leander v. Sweden [Електронний ресурс] / ECHR. – No. 9248/81. – 1987. –March 26. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-57519.

270. Rotaru v. Romania [Електронний ресурс] / ECHR. – No. 28341/95. – 2000. – May 04. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-58586.

271. Turek v. Slovakia [Електронний ресурс] / ECHR. – No. 57986/00. – 2006. – February 14. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-72354.

272. Lessig L. The Law of the Horse: What Cyberlaw might teach / Lawrence Lessig // Harvard Law Review. – Vol. 113. – 1999-2000. – Pp. 501-549.

273. Goldsmith J. L. Against Cyberanarchy [Електронний ресурс] / Jack L. Goldsmith // University of Chicago Law Occasional Paper. – No. 40. – 1999. – Режим доступу: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1001&context=occasional_papers.

274. Solove D. The Digital Person: Technology and Privacy in the Information Age / Daniel J. Solove. – New York: New York University Press, 2004. – 283 p.

275. Schwartz P. M., Reidenberg J. R. Data Privacy Law: A Study of United States Data Protection / Paul M. Schwartz, Joel R. Reidenberg. – Lexis Law Pub, 1996. – 486 p.

276. Bothe M. Data, Transborder flow and Protection / Michael Bothe // Encyclopedia of Public International Law. – Vol. 1. – London, 1992. – Pp. 950-961.

277. Резолюция Совета по правам человека 28/16 «Право на неприкосновенность частной жизни в цифровой век» от 1 апреля 2015 года [Электронный ресурс] // Официальный сайт Верховной Рады Украины. – Режим доступа: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/068/80/PDF/G1506880.pdf?OpenElement.

278. Appointments Made at the 29th Session of the Human Rights Council (15 June - 3 July 2015) [Электронный ресурс] // The Office of the United Nations High Commissioner for Human Rights. – Режим доступа: http://www.ohchr.org/EN/HRBodies/SP/Pages/HRC29.aspx.

279. APEC Data Privacy Pathfinder [Електронний ресурс] // APEC Agreements and Declarations. – Sydney, Australia. – 2-3 September 2007. – Режим доступу: http://www.asianlii.org/apec/other/agrmt/adpp221/.

280. APEC Cooperation Arrangement for Cross-Border Privacy Enforcement [Електронний ресурс]. – August 2009. – Режим доступу: http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf.

281. APEC Cross-Border Privacy Rules System [Електронний ресурс]. – Режим доступу: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

282. APEC/EU Referential for the Structure of the EU Binding Corporate Rules and APEC Cross Border Privacy Rules System – DRAFT Endorsement Request [Електронний ресурс]. – Ningbo, China. – 20 February 2014. – Режим доступу: http://mddb.apec.org/Documents/2014/ECSG/ECSG1/14_ecsg1_013.pdf

283. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера № 108 от 1981 года [Электронный ресурс] // Официальный сайт Совета Европы. – Режим доступа:http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=RUS&NT=108.

284. Дополнительный протокол к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера, касаясь властей контроля и граничных потоков данных от 2001 года [Электронный ресурс] // Официальный сайт Совета Европы. – Режим доступа:http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=8&CL=RUS.

285. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Электронный ресурс] // Access to European Union law. – Режим

доступа: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

286. Safe Harbor Privacy Principles [Электронный ресурс]. – Режим доступа: http://www.export.gov/safeharbor/eu/eg_main_018475.asp.

287. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [Электронный ресурс] // Access to European Union law. – Режим доступа: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000D0520.

288. Защита данных и конфиденциальность в облаке. Облако чье же оно? [Электронный ресурс] // ITU News. – No. 1. – 2013. – Режим доступа: https://itunews.itu.int/ru/Note.aspx?Note=3690.

289. Конституція України від 28 червня 1996 року [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/print1385029031111268.

290. Цивільний кодекс України від 16 січня 2003 року [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/435-15.

291. Trends in Telecommunication Reform 2013. Transnational Aspects of Regulation In a Networked Society. Summary [Електронний ресурс] // ITU. – May 2013. – Режим доступу: http://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-TTR.14-2013-SUM-PDF-E.pdf.

292. International Standards on the Protection of Privacy with regard to the processing of Personal Data. The Madrid Resolution [Електронний ресурс] // International Conference of Data Protection and Privacy Commissioners. – 5 November 2009. – Режим доступу: http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf.

293. Maximillian Schrems v. Data Protection Commissioner [Електронний ресурс] // InfoCuria - Case-law of the Court of Justice. – C-362/14. – 6 October 2015. – Режим доступу: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

294. Передача персональных данных из Европы в США больше не разрешается? [Электронный ресурс] // «pvsm.ru» – новости информационных технологий. – 09 октября 2015. – Режим доступа: http://www.pvsm.ru/digital/100458.

295. EU-U.S. Privacy Shield: Frequently Asked Questions [Электронный ресурс] // European Commission Press Releases Database. – Brussels. – 29 February 2016. – Режим доступа: http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

296. Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection «Umbrella Agreement» [Электронный ресурс] // European Commission Official Website. – Brussels. – 08 September 2015. – Режим доступа: http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm.

297. An Act to Extend Privacy Act Remedies to Citizens of Certified States, and for Other Purposes [Електронний ресурс] // 114th Congress of the United States of America. – 04 January 2016. – Режим доступу: https://www.gpo.gov/fdsys/pkg/BILLS-114hr1428enr/pdf/BILLS-114hr1428enr.pdf.

298. Reform of EU Data Protection Rules [Електронний ресурс] // Офіційний сайт Єврокомісії. – Режим доступу: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

299. Леваков А. Информационная безопасность в США: проблемы и решения [Электронный ресурс]. – Режим доступа: https://goo.gl/Gv39jD.

300. Brunner E. M., Suter M. International Critical Information Infrastructure Protection Handbook 2008/2009 / Elgin M. Brunner and Manuel Suter. – Center for Security Studies - ETH Zurich, 2009. – 652 p.

301. Забара І. М. Інститут міжнародної інформаційної безпеки: правові аспекти [Електронний ресурс] / І. М. Забара // Правова інформатика. – № 1(41)/2014. – С. 64-71. – Режим доступу: http://ippi.org.ua/sites/default/files/14zimbpa.pdf.

302. O'Connell M. Cyber Security without Cyber War [Електронний ресурс] / Mary Ellen O'Connell // Journal of Conflict and Security Law. – Vol. 17. – Issue 2. – Pp. 187-209. – Режим доступу: http://jcsl.oxfordjournals.org/content/17/2/187.full.

303. What limits does the law of war impose on cyber attacks? [Електронний ресурс] // ICRC. – 28 June 2013. – Режим доступу: https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

304. Tarnogórski R. Time for an International Law on Cyber Conflicts / Rafał Tarnogórski // Bulletin of the Polish Institute of International Affairs. – No. 32 (485). – 26 March 2013. – 2 p.

305. Creation of a global culture of cybersecurity dated 20 December 2002 [Електронний ресурс]. – Режим доступу: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239.

306. Creation of a global culture of cybersecurity and the protection of critical information infrastructures dated 23 December 2003 [Електронний ресурс]. – Режим доступу: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/199.

307. Global Cybersecurity Agenda (GCA) [Електронний ресурс] // ITU. – Режим доступу: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

308. Watts S. Call for Cyberwar «Peacekeepers» Force [Електронний ресурс] / Susan Watts // BBC. – 26 January 2012. – Режим доступу: http://news.bbc.co.uk/2/hi/programmes/newsnight/9687338.stm.

309. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Електронний ресурс] // EUR-Lex - Access to European Union law. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

310. Convention on Cybercrime No. 185 dated 23 November 2001 [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

311. Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon. – 19 November 2010 [Електронний ресурс] // NATO. – Режим доступу: http://www.nato.int/cps/en/natohq/official_texts_68580.htm.

312. Schmitt M. Tallinn Manual on the International Law Applicable to Cyber Warfare / Michael N. Schmitt. – Cambridge University Press, 2013. – 300 p.

313. African Union Convention on Cyber Security and Personal Data Protection dated 27 June 2014 [Електронний ресурс]. – Режим доступу: http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf.

314. Конвенция об обеспечении международной информационной безопасности (концепция) [Электронный ресурс] // Официальный сайт Совета Безопасности Российской Федерации. – Режим доступа: http://www.scrf.gov.ru/documents/6/112.html.

315. US Cyber Command Fact Sheet dated 21 May 2010 [Електронний ресурс] // US Department of Defense. – Режим доступу: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-038.pdf.

316. The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets as of February 2003 [Електронний ресурс] // The White House, Washington. – Режим доступу: http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

317. The National Strategy to Secure Cyberspace as of February 2003 [Електронний ресурс] // The White House, Washington. – Режим доступу: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

318. Department of Defense Strategy for Operating in Cyberspace as of July 2011 [Електронний ресурс] // Department of Defense United States of America, Washington. – Режим доступу: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

319. инфраструктуры [Электронный ресурс] // Digital Report. – 02 сентября 2015. – Режим доступа: http://digital.report/zashhita-infrastrukturyi/.

320. National Security Strategy as of February 2015 [Електронний ресурс] // The White House, Washington. – Режим доступу: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

321. Закон України «Про основи національної безпеки України» від 19 червня 2003 року [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15.

322. 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 травня 2014 року [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/n0004525-14.

323. Sanjay Goel об адаптации права к конфликтам в киберпространстве [Электронный ресурс] // Digital Report. – 11 сентября 2015. – Режим доступа: http://digital.report/adaptatsiya-prava-k-konfliktam-v-kiberprostranstve/.

324. Talihärm A. M. Towards Cyberpeace: Managing Cyberwar through International Cooperation [Електронний ресурс] / Anna-Maria Talihärm // UN Chronicle. – Vol. L. – No. 2. – August 2013. – Режим доступу: http://www.un.org/wcm/content/site/chronicle/home/archive/issues2013/security/towardscyberpeacemanagingcyberwarthroughinternationalcooperation.

325. Кирилюк О. В. Становление универсального международно-правового регулирования в сфере защиты персональных данных / О. В. Кирилюк // Международный научно-практический правовой журнал «Legea si Viata». – Кишинёв. – 2015. – № 11. – С. 65-69.

326. Кирилюк О. В. Відкритий доступ до знань в інформаційному суспільстві / О. В. Кирилюк // Український часопис міжнародного права. – 2014. – № 1-2. – С. 78-87.

327. Кирилюк О. В. Міжнародно-правові аспекти використання кіберпростору у військових цілях / О. В. Кирилюк // Український часопис міжнародного права. – 2014. – Спецвипуск: Нові імена в науці міжнародного права. – С. 80-86.

328. Кирилюк О. Забезпечення інформаційної безпеки в умовах розбудови інформаційного суспільства в Україні / О. Кирилюк // Актуальні проблеми держави і права. Збірник наукових праць. – Одеса: «Юридична література», 2014. – Випуск 74. – С. 159-164.

329. Кирилюк О. Нормативно-правове забезпечення функціонування та безпеки критичної інформаційної інфраструктури / О. Кирилюк // Студентський юридичний журнал. – К.: Редакція журналу «Право України», 2013. - № 1. – С. 110-119.

330. Кирилюк О. Відповідність законодавства України стандартам Ради Європи щодо захисту прав людини в онлайн середовищі // Шевченківська весна: Матеріали

міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених. – К.: КНУ ІМВ, 2015. – Ч. 1. – С. 168-171.

331. Кирилюк О. Нормативно-правові основи інформаційної політики України // Геостратегічні пріоритети України в політичній, економічній, правовій та інформаційній сферах: Матеріали наукової конференції. – К.: КНУ ІМВ, 2015. – С. 210-213.

332. Кирилюк О. В., Пазюк А. В. Виклики національній безпеці в добу глобального інформаційного суспільства / О. В. Кирилюк, А. В. Пазюк // Українська Революція гідності, агресія РФ і міжнародне право. Колективна монографія. – К.: «К.І.С.», 2014. – С. 837-838.

333. Кирилюк О. В. Загальна характеристика національного законодавства у сфері захисту та відновлення прав і свобод людини онлайн // Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для Інтернет-користувачів. – К.: ФОП Клименко, 2015. – С. 33-72.