

МІЖНАРОДНЕ ПРАВО ТА ПРАВО ЄВРОПЕЙСЬКОГО СОЮЗУ

УДК 349

DOI <https://doi.org/10.32782/2408-9257-2025-4-18>

Владикін О. Н.,

кандидат юридичних наук,

доцент кафедри інтелектуальної власності та приватного права факультету соціології і права

Національного технічного університету України

«Київський політехнічний інститут імені Ігоря Сікорського»

ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН У ЦИФРОВОМУ ПРОСТОРИ: ЗАРУБІЖНИЙ ДОСВІД

LEGAL REGULATION OF DIGITAL SPACE: FOREIGN EXPERIENCE

У статті здійснено комплексний аналіз підходів до правового регулювання цифрового простору в країнах Європейського Союзу, США, а також деяких азійських та арабських державах. Автор досліджує еволюцію національного законодавства в контексті глобальних інформаційних викликів, особливу увагу приділяє законодавчим актам, спрямованим на захист прав користувачів, неповнолітніх, персональних даних і об'єктів інтелектуальної власності. У сучасному суспільстві цифрові комунікації є не лише технологічною новацією, а й ключовим фактором трансформації соціально-політичного та економічного життя. Водночас цифрове середовище породжує нові юридичні виклики – захист персональних даних, протидія кіберзагрозам, контроль за онлайн-контентом, захист інтелектуальної власності. У різних країнах спостерігається значна варіативність правових моделей – від ліберальної саморегуляції до суворих адміністративних підходів. Отже, актуальним стає порівняльний аналіз міжнародного досвіду, що дасть змогу адаптувати найефективніші практики для вдосконалення українського законодавства у сфері інформаційних відносин.

Окрема увага приділяється впливу саморегулятивних механізмів, цифровій грамотності та інформаційній безпеці як основі стабільного функціонування цифрового середовища. Стаття містить порівняльний аналіз нормативно-правових підходів, їх ефективності та викликів для майбутньої гармонізації вітчизняного законодавства з міжнародними стандартами. У контексті глобальної цифровізації інформаційні відносини відіграють ключову роль у формуванні нових моделей взаємодії між державою, бізнесом і громадянами. Однак разом із позитивними змінами виникають і загрози – від порушення конфіденційності до поширення шкідливого контенту. Тому зростає необхідність у правовому врегулюванні як на національному, так і на міжнародному рівнях.

Вивчення зарубіжного досвіду (США, ЄС, КНР, Південна Корея тощо) дає змогу оцінити ефективність інструментів регуляції цифрового простору. Актуальними залишаються проблеми юридичної відповідальності онлайн-платформ, кіберзлочинності, авторських прав у цифровому середовищі та впровадження стандартів цифрової етики.

Ключові слова: цифрові правовідносини, правове регулювання, інформаційна безпека, персональні дані, інтернет-право, інтелектуальна власність, саморегуляція, кібербезпека, цифрові комунікації.

The article provides a comprehensive analysis of approaches to the legal regulation of the digital space in the countries of the European Union, the USA, as well as some Asian and Arab states. The author examines the evolution of national legislation in the context of global information challenges, paying special attention to legislative acts aimed at protecting the rights of users, minors, personal data and intellectual property. In modern society, digital communications are not only a technological innovation, but also a key factor in the transformation of socio-political and economic life. At the same time, the digital environment gives rise to new legal challenges – protection of personal data, countering cyber threats, control over online content, protection of intellectual property. In different countries, there is significant variability in legal models – from liberal self-regulation to strict administrative approaches. Therefore, a comparative analysis of international experience becomes relevant, which will allow adapting the most effective practices to improve Ukrainian legislation in the field of information relations.

Special attention is paid to the influence of self-regulatory mechanisms, digital literacy and information security as the basis for the stable functioning of the digital environment. The article contains a comparative analysis of regulatory approaches, their effectiveness and challenges for the future harmonization of domestic legislation with international standards. In the context of global digitalization, information relations play a key role in the formation of new models

of interaction between the state, business and citizens. However, along with positive changes, threats also arise – from violation of confidentiality to the spread of harmful content. Therefore, the need for legal regulation is growing both at the national and international levels.

Studying foreign experience (USA, EU, China, South Korea, etc.) allows us to assess the effectiveness of digital space regulation tools. The problems of legal liability of online platforms, cybercrime, copyright in the digital environment and the implementation of digital ethics standards remain relevant.

Key words: *digital legal relations, legal regulation, information security, personal data, Internet law, intellectual property, self-regulation, cybersecurity, digital communications.*

Постановка проблеми. У сучасному світі цифрові комунікації стали визначальним фактором трансформації суспільних, економічних та політичних процесів. Разом з цим зростає потреба у правовому регулюванні інформаційних відносин, що виникають у цифровому середовищі. У центрі уваги перебувають проблеми захисту прав користувачів, персональних даних, забезпечення кібербезпеки, боротьби з протиправним контентом і захисту інтелектуальної власності. Водночас практика різних країн демонструє широкий спектр підходів – від ліберальних моделей саморегуляції до жорстких адміністративно-каральних інструментів. Це обумовлює актуальність дослідження міжнародного досвіду з метою адаптації ефективних правових моделей для вдосконалення вітчизняного законодавства.

Аналіз останніх досліджень і публікацій. Теоретичні засади формування та еволюції цифрових відносин відображено у працях провідних зарубіжних дослідників, серед яких Е. Браун, Д. Белл, А. Тоффлер, Г. Паркер, П. Друкер та інші, які акцентували увагу на трансформаційних процесах в економіці під впливом інформаційних технологій. Вивченню міжнародного досвіду впровадження цифрової економіки та розвитку цифрових суспільств присвячено низку наукових напрацювань українських авторів, зокрема І. Грінько, С. Коляденка, О. Пухоменко-Куцевіл, А. Абрамової, В. Бещасного та А. Жаворонка. При підготовці дослідження також було проаналізовано офіційні публікації та аналітичні матеріали профільних державних і міжнародних інституцій, відповідальних за реалізацію цифрових стратегій у провідних країнах світу.

Виклад основного матеріалу дослідження. Інтернет не є юридичною особою або організаційною структурою з централізованим управлінням, а тому не може виступати як класичний суб'єкт правовідносин у правовій сис-

темі. Це унеможливорює встановлення безпосередніх юридичних відносин між Інтернетом як явищем і державою. Натомість у межах мережі функціонують окремі суб'єкти, які виступають учасниками правовідносин, пов'язаних із використанням інформаційних ресурсів. До структури таких ресурсів в Інтернеті входять: вебсайти традиційних медіа (телебачення, друковані ЗМІ, радіо тощо), інформаційні платформи, що існують виключно в цифровому просторі без аналогів у реальному медіапросторі, сторінки та сервіси приватних чи комерційних суб'єктів, які не мають статусу засобу масової інформації, але поширюють контент для широкої аудиторії.

З активним розвитком цифрових технологій та глобальної мережевої інфраструктури значно зросла роль інформаційних відносин у сучасному суспільстві. Більшість держав визнають необхідність правового врегулювання цих відносин, адже стрімке поширення електронних комунікацій спричиняє трансформаційні процеси в усіх сферах суспільного життя – від державного управління до освіти, культури та бізнесу. Інформаційні відносини стали потужним інструментом соціального поступу, сприяючи відкритості, мобільності знань та ліквідації бар'єрів у доступі до інформаційних ресурсів. Держава, громадяни й суб'єкти господарювання отримали нові можливості щодо створення, зберігання, використання й поширення інформації, обсяг і різноманіття якої постійно зростає.

Разом із тим, розширення інформаційного простору породжує низку актуальних викликів правового характеру. Мова йде про питання відповідальності за поширення інформації, забезпечення інформаційної безпеки, захисту персональних даних, дотримання авторських прав тощо. За відсутності належного правового регулювання ці проблеми можуть не лише ускладнювати функціонування інформацій-

ної інфраструктури, а й створювати загрози для основ демократичного устрою. Саме тому питання нормативного врегулювання інформаційних відносин набуває особливої важливості як на національному, так і на міжнародному рівнях. Аналіз зарубіжного досвіду у цій сфері дає змогу оцінити ефективність різних підходів до правового забезпечення цифрових процесів і визначити напрями подальшого розвитку законодавства України.

До кінця XX століття в законодавстві Сполучених Штатів Америки сформувались ключові підходи до правового регулювання інформаційних відносин у цифровому просторі. Значний вплив на це мало прийняття Закону про телекомунікації 1996 року (*Telecommunications Act of 1996*), який доповнив федеральний закон 1934 року положеннями, спрямованими на регулювання взаємодії учасників інформаційних процесів у новому технологічному середовищі [1].

Зокрема, два положення акта стосувалися обмеження відповідальності за зміст інформації, що циркулює через інформаційні ресурси. Перше положення передбачало звільнення від відповідальності провайдерів та користувачів інтерактивних комп'ютерних послуг за контент, оприлюднений іншими суб'єктами. Друге – гарантувало інформаційним посередникам право на самостійне обмеження доступу до змісту, який вони вважають неприйнятним, без настання юридичних наслідків за такі дії. Незважаючи на ліберальну орієнтацію цих норм, реакція з боку громадськості виявилася неоднозначною. Значна частина цифрової спільноти сприйняла такі законодавчі ініціативи як загрозу свободі інформаційного самовираження та приклад потенційного державного втручання у процеси, які за своєю природою мають саморегулювальний характер.

Ці занепокоєння особливо яскраво були висловлені у Декларації незалежності кіберпростору Джона Перрі Барлоу, яка набула широкого розголосу як символ протесту проти надмірного контролю з боку держави над інформаційним середовищем. У цьому документі підкреслюється, що традиційні механізми державного регулювання не можуть бути безпосередньо перенесені на новий вимір інформаційних відносин, оскільки останні

мають іншу природу, логіку функціонування та етичні засади [2].

Барлоу наголошував, що нормативне втручання у формування інформаційних комунікацій без згоди користувачів є порушенням засадничих принципів свободи вираження. У декларації міститься заява про те, що владні структури не мають юрисдикції в інформаційному середовищі без прямої згоди його учасників, оскільки вони не були його творцями, не беруть участі в розбудові цифрової культури та не враховують особливостей етичного та неформального регулювання, яке вже склалося серед спільнот користувачів [4].

Таким чином, у контексті розвитку інформаційних відносин на межі XX–XXI століття вперше було публічно поставлено питання про обмеження державної юрисдикції над комунікаціями у цифровому просторі та необхідність врахування саморегулювальних механізмів, що виникають з ініціативи самих учасників цих відносин. У 1997 році Верховний Суд США визнав неконституційним окреме положення Закону про пристойність у засобах зв'язку, яке передбачало кримінальну відповідальність за розповсюдження матеріалів сумнівного змісту, що можуть бути доступні неповнолітнім. Суд дійшов висновку, що така норма суперечить Першій поправці до Конституції США, яка гарантує свободу слова. Водночас інші положення закону, що стосуються обмеження обігу матеріалів непристойного характеру, були залишені в силі [5].

Реакцією на суспільну дискусію щодо захисту дітей у цифровому інформаційному середовищі стало запровадження на рівні виконавчої влади стратегії, яка мала на меті формування «сімейно-дружнього простору» в системі інформаційних відносин. Зокрема, за ініціативи президента Білла Клінтона та віце-президента Альберта Гора було запропоновано комплекс заходів, що передбачав надання батькам і освітянам інструментів контролю за доступом неповнолітніх до цифрового контенту, а також спрямування їхньої уваги на якісні освітні ресурси. Представники галузі телекомунікацій та цифрового контенту підтримали цю ініціативу, домовившись про необхідність розвитку систем фільтрації, створення інструментів рейтингової оцінки матеріалів, а також проведення

просвітницьких кампаній з підвищення цифрової грамотності та безпеки. У цьому ж році президентом США було підписано указ, який визначив загальні принципи державної політики у сфері інформаційних відносин у цифровому середовищі. Основна увага в цьому документі приділялася обмеженню втручання держави у процеси, що відбуваються в електронному інформаційному просторі, лише до тих сфер, де це є необхідним. Таке втручання повинно бути мінімальним, прозорим і базуватися на простих правових механізмах. Пріоритет надавався захисту приватної власності, інтелектуальних прав, протидії шахрайству та забезпеченню умов для розвитку електронної комерції.

Одним із важливих положень нової інформаційної політики стала теза про те, що традиційні норми, розроблені для телебачення, радіомовлення чи аналогових телекомунікацій, не можуть бути безпосередньо застосовані до цифрових інформаційних відносин. Відтак законодавство має бути переглянуто з урахуванням особливостей електронної комунікації та нових ризиків, які виникають у зв'язку з розвитком цифрової економіки.

Крім того, політичне керівництво США акцентувало увагу на важливості правового захисту в межах інформаційного обміну. Постачальники цифрових послуг мають бути впевнені у збереженні прав на створений контент і інтелектуальну власність, тоді як користувачі – у достовірності та легальності отриманої інформації. Такий підхід свідчить про формування нового розуміння інформаційних правовідносин, яке поєднує захист інтересів як творців, так і споживачів інформаційного продукту.

У США на державному рівні підтримується розвиток інфраструктур безпеки інформаційних відносин, які функціонують відповідно до ринкових механізмів і ґрунтуються на використанні криптографічних технологій. Ці інфраструктури покликані забезпечити базові принципи інформаційної безпеки, зокрема – автентифікацію учасників, збереження цілісності та конфіденційності інформаційного обміну. Задля досягнення цих цілей адміністрація США у співпраці з Конгресом здійснює розробку та удосконалення нормативно-право-

вих актів, спрямованих на стимулювання розвитку відповідних рішень.

У публічному дискурсі домінує підхід, згідно з яким інформаційні ресурси в цифровому середовищі не повинні підпадати під ті самі регуляторні рамки, що й традиційні медіа (радіо, телебачення). Такий підхід аргументується тим, що надмірне втручання держави може стримувати інноваційний розвиток цифрових комунікацій та обмежувати плюралізм джерел інформації.

У цьому контексті пріоритет надається саморегуляції учасників інформаційних правовідносин – через впровадження добровільних кодексів поведінки, рейтингових систем оцінювання контенту та гнучких технічних засобів обмеження доступу до певної інформації. Адміністративна політика орієнтована на створення умов для конкуренції серед цифрових рішень, які забезпечують баланс між свободою комунікації та захистом від небажаного чи шкідливого контенту, при цьому не порушуючи базових прав користувачів на інформацію.

Загалом, така стратегія відображає намагання США розвивати систему інформаційних відносин як відкриту, інноваційну і ринкову сферу, де ключову роль у забезпеченні правового порядку відіграє не стільки пряме державне регулювання, скільки механізми самоорганізації цифрового суспільства.

Інформаційна політика Сполучених Штатів Америки в умовах цифрової трансформації орієнтується на кілька основних напрямів регуляторного впливу, які охоплюють ключові правові аспекти функціонування інформаційних правовідносин. Серед пріоритетних сфер державного втручання виокремлюються: контроль за змістом цифрових інформаційних потоків; обмеження присутності іноземного інформаційного контенту; регулювання комерційної реклами в мережевому середовищі; протидія шахрайству та іншим формам правопорушень у сфері цифрових комунікацій. Особливе місце в нормативному забезпеченні займають механізми захисту неповнолітніх в умовах глобальної відкритості цифрових інформаційних каналів. Зокрема, прийнятий у 1998 році Закон про захист приватного життя дітей у мережі встановлює заборону на збір і поширення персональних даних осіб віком до 16 років без

попередньої згоди батьків або законних представників. Також обмежується можливість створення персоніфікованих інформаційних облікових записів та каналів цифрової комунікації для неповнолітніх осіб. Ухвалений згодом Закон про захист прав дітей у цифровому середовищі (Child Online Protection Act) передбачає значні штрафні санкції (до 50 тис. доларів США) і навіть позбавлення волі за розміщення у відкритому доступі контенту, що потенційно може зашкодити фізичному, психічному або моральному розвитку дітей [4].

Крім захисту неповнолітніх, американське законодавство також приділяє увагу правовим аспектам функціонування інформаційної економіки. Зокрема, йдеться про забезпечення дотримання авторських і суміжних прав в умовах спрощеного цифрового копіювання, регулювання електронної комерції, включаючи інструменти цифрової реклами, обігу електронних валют, електронного документообігу, контрактних зобов'язань та оподаткування трансакцій, пов'язаних з передачею інформації. Не менш значущим є вектор, пов'язаний із забезпеченням інформаційної безпеки. У сучасному правовому дискурсі вона трактується як здатність держави гарантувати безперервне функціонування життєво важливих інформаційних систем, недоторканність критичної цифрової інфраструктури та захист від кіберзагроз.

У 2010 році законодавчий орган США розглядав проєкт Закон про захист кіберпростору як національного надбання, що надавав би Президенту США повноваження обмежувати або навіть тимчасово припиняти функціонування цифрових каналів комунікації (включаючи пошукові системи) у разі загроз національній безпеці. Цей підхід викликав суттєву критику через ризики порушення свободи слова та прав користувачів, тому в подальшому проєкт був модифікований і трансформований у виконавчий законопроект про координацію в кіберпросторі, з акцентом на міжвідомчу взаємодію та превентивні заходи. Таким чином, практика США демонструє послідовне розширення правового регулювання інформаційних відносин у цифровому середовищі, водночас балансуючи між захистом суспільних інтересів і дотриманням фундаментальних прав і свобод. Від-

критість інформаційного простору, характерна для американської моделі, поступово поєднується із жорсткішими підходами до регулювання вразливих сфер – дитячої безпеки, інтелектуальної власності та цифрової економіки [5].

У правовій системі США вже понад десятиліття діє спеціалізоване законодавство, спрямоване на врегулювання відносин у сфері використання інформації в цифровому середовищі – зокрема, Закон про авторське право в цифрову епоху (*Digital Millennium Copyright Act*, DMCA). Цей нормативний акт поєднує положення про відповідальність за порушення авторських прав у цифровому просторі з механізмами обмеження відповідальності для інформаційних посередників, зокрема провайдерів, за дії третіх осіб. За умови, що такі суб'єкти не знали і об'єктивно не могли знати про порушення прав, вони звільняються від юридичних наслідків [6].

Аналітика американських дослідницьких центрів демонструє, що ефективне правове реагування на порушення прав у сфері інформаційних відносин у цифровому середовищі позитивно впливає на національну економіку, загальну безпеку та навіть на рівень розвитку системи охорони здоров'я. Відтак у США активно формуються інституційні та процедурні механізми контролю за дотриманням законодавства у сфері обігу інформації, зокрема:

- розробляються методики збору електронних доказів,
- удосконалюються механізми притягнення до відповідальності за цифрові правопорушення,
- створюється система державного нагляду за законністю функціонування цифрових інформаційних платформ.

Схожі тенденції простежуються і в країнах Європейського Союзу, де правове регулювання інформаційних відносин також набуває обмежувальних рис з огляду на потребу дотримання принципу законності та забезпечення публічних інтересів.

Зокрема, Франція стала однією з перших держав ЄС, яка на рівні законодавства передбачила обмеження доступу до цифрових ресурсів, що порушують встановлені норми. Починаючи з 2000 року, у країні діє інститут кримінальної відповідальності для провайдерів, які надають

послуги хостингу без ідентифікації користувачів. Зобов'язання перевіряти особу користувача покладається як на посередників, так і на самих учасників інформаційного обміну [7].

Питання протидії порушенням у сфері інтелектуальної власності в онлайн-середовищі закріплено в Законі про боротьбу з цифровим піратством, чинному з 2010 року. Його реалізацію координує спеціалізований підрозділ Міністерства внутрішніх справ Франції – Центральне управління з протидії ІТ-злочинності, яке здійснює контроль за змістом цифрових ресурсів. У рамках Закону LOPPSI 2 (фр. «Loi du 14 mars 2011 d'orientation et de programmation pour la performance de la securite interieure»), поліції було надано право вимагати від цифрових платформ (провайдерів) негайного блокування доступу до ресурсів, які містять заборонений контент – зокрема, дитячу порнографію – без необхідності отримання попередньої санкції суду [8]. Водночас сформовано так звані «чорні списки» – переліки сумнівних ресурсів, які підлягають обмеженню в доступі. Механізм оскарження таких рішень фактично не передбачено. Зазначені практики демонструють перехід від абсолютної свободи обміну інформацією в цифровому середовищі до правової моделі, що балансує між свободою вираження, правами авторів та необхідністю забезпечення публічного порядку.

У межах протидії кіберзлочинності деякі держави запроваджують спеціальні правові режими контролю за інформаційними відносинами. Зокрема, Закон LOPPSI 2 у Франції передбачає можливість втручання правоохоронних органів у цифрові системи користувачів за згодою прокуратури. Це включає застосування шкідливого програмного забезпечення (зокрема, троянських програм) для збору доказів під час розслідування тяжких кримінальних правопорушень, таких як незаконний обіг зброї, наркотичних засобів, легалізація коштів, одержаних злочинним шляхом тощо.

У Великобританії, незважаючи на відсутність окремого закону, що комплексно регламентує сферу інформаційних відносин, застосовується усталена судова практика, сформована ще до епохи цифровізації, для вирішення спірних ситуацій у цій галузі. Розслідування правопорушень у сфері високих

технологій здійснює Національний підрозділ з протидії кіберзлочинності. Крім того, певні форми контролю реалізуються через діяльність громадянського суспільства. Закон «Про цифрову економіку» (Digital Economy Act, 2010) надає можливість обмеження доступу користувачів до інформаційних ресурсів у разі систематичного порушення авторських прав – зокрема, без потреби у судовому рішенні, та передбачає блокування ресурсів, причетних до цифрового піратства [9].

Країни Перської затоки, зокрема Саудівська Аравія, також активно регулюють сферу інформаційних відносин. Починаючи з 2001 року, державна політика передбачає жорсткий контроль усіх видів інформаційного обміну. Весь вхідний і вихідний трафік проходить через державні проксі-сервери, а пошукові запити та приватне листування підлягають автоматичному фільтруванню. Остаточні рішення щодо блокування доступу до окремих ресурсів ухвалюються на рівні урядових органів – зокрема, Радою міністрів [10].

У ряді держав активно застосовуються механізми обмеження доступу до інформаційних ресурсів задля контролю над інформаційними відносинами у цифровому середовищі. Так, у деяких країнах Близького Сходу заборонено приблизно 90% вебресурсів, переважна більшість із яких мають порнографічне спрямування. Основним аргументом для введення таких обмежень декларується захист релігійних та морально-етичних цінностей. Водночас блокування охоплює також ресурси правозахисного спрямування, дискусійні платформи, блоги, сайти з інформацією про психоактивні речовини, алкоголь, азартні ігри та виготовлення вибухових засобів. Нерідко блокуванню підлягають навіть освітні, медичні або розважальні ресурси.

Попри суворі обмеження, у межах національних сегментів цифрової інфраструктури зберігається певна ступінь свободи. Наприклад, у Саудівській Аравії користувачі мають змогу перевірити доступність того чи іншого ресурсу через офіційні сервіси, а альтернативний доступ до заблокованих сайтів можливий через мобільні пристрої певного типу (зокрема, BlackBerry). Соціальні мережі, зокрема Facebook, залишаються відкритими для широ-

кого загалу. Подібна модель регулювання інформаційного середовища спостерігається і в Об'єднаних Арабських Еміратах. Тут також діють численні заборони на пошукові запити, а доступ до ресурсів, що містять інформацію про алкоголь, наркотики та інші заборонені теми, блокується на рівні провайдерів. Повноцінний доступ до глобальних інформаційних потоків можливий лише в спеціалізованих зонах, таких як Дубайський Теком, де зосереджені провідні ЗМІ, технологічні компанії та наукові установи. Соціальні мережі (Twitter, Facebook, YouTube), а також сервіси збереження контенту (Flickr) і комунікаційні платформи (Skype, «ВКонтакте») тривалий час залишалися недоступними [10].

У Південній Кореї, незважаючи на високий рівень цифровізації, держава також здійснює контроль за інформаційними потоками. Зокрема, посилюється законодавче регулювання у сфері захисту персональних даних, упроваджується обов'язкова ідентифікація користувачів, а також приймаються заходи для недопущення поширення небажаного контенту. Разом із тим, комплексність проблеми й досі не дозволяє досягти повного дотримання правових стандартів у сфері інформаційних відносин.

У 2011 році Південна Корея зазнала одного з найбільших витоків персональних даних в історії країни, внаслідок чого, за оцінками експертів, інформація про понад 30 мільйонів громадян – більш ніж половину населення – опинилася в розпорядженні іноземних зловмисників. Цей інцидент засвідчив вразливість держав у сфері інформаційної безпеки та нагальну потребу в належному правовому регулюванні інформаційних відносин, що охоплюють як збирання, обробку й зберігання персональних даних, так і доступ до них.

У низці держав здійснюється жорстке регулювання функціонування інформаційного простору, що включає як технічні, так і правові механізми обмеження доступу до окремих ресурсів. Зокрема, в Китайській Народній Республіці діє розгалужена система контролю інформаційних потоків, яка передбачає багаторівневу фільтрацію пошукових запитів, блокування закордонних веб-ресурсів, обмеження функціонування соціальних мереж та активний моніторинг цифрової активності громадян.

Основною метою таких обмежень з боку державних органів влади є забезпечення національної безпеки та інформаційної стабільності в умовах загроз екстремізму й тероризму. Контроль за інформаційними відносинами реалізується через провайдерів, які несуть відповідальність за дотримання встановлених фільтрів та модераційного режиму на громадських платформах. Додатково, з метою посилення державного контролю, у 2011 році в Пекіні було запроваджено обов'язкові вимоги для суб'єктів господарювання, таких як кафе, книгарні та готелі, щодо встановлення спеціалізованого програмного забезпечення, яке дозволяє відстежувати дії користувачів, що підключаються до мережі Wi-Fi. Невиконання цих вимог тягло за собою значні штрафні санкції або анулювання ліцензії на ведення діяльності. Висока вартість програмного забезпечення у поєднанні з адміністративними обмеженнями спричинила відмову багатьох закладів від надання безкоштовного доступу до мережі, що вказує на обмеження інформаційних прав громадян навіть у публічному просторі [11].

У сучасних умовах функціонування глобального інформаційного простору особливої актуальності набуває питання державного регулювання інформаційних відносин, що виникають у цифровому середовищі. Розвиток національних систем контролю, обмеження доступу до інформаційних ресурсів і створення альтернативних платформ свідчать про прагнення окремих держав до формування замкненого інформаційного середовища.

Так, правоохоронні органи Китайської Народної Республіки успішно реалізують заходи з протидії нелегальній азартній діяльності у цифровому просторі. У 2011 році Міністерство оборони КНР створило спеціалізовану структуру – так звану «онлайн армію блакитних мундирів», діяльність якої, за оцінками експертів, спрямована на підвищення рівня державної фільтрації та контролю над комунікаційними потоками в національному сегменті інформаційних відносин. Крім того, в рамках удосконалення нормативно-правового регулювання інформаційної безпеки, у КНР з 2011 року набули чинності зміни до законодавства, що передбачають кримінальну відповідальність за

незаконний доступ до персональних даних – з максимальним строком покарання до семи років позбавлення волі.

Своєрідним прикладом радикального обмеження інформаційної взаємодії є політика Північної Кореї, де відсутня технічна інфраструктура для вільного функціонування інформаційних відносин із глобальним середовищем. Окремі вебресурси, що належать уряду, розміщуються за межами країни, тоді як на її території діє ізольована внутрішня мережа «Кванмен», не пов'язана із зовнішніми каналами зв'язку.

На Кубі обмеження стосуються переважної більшості населення: доступ до глобального інформаційного середовища дозволений лише вузькому колу фахівців, зокрема лікарям, тоді як для решти громадян існує пряма заборона на рівні законодавства.

Подібна практика має місце й в Ісламській Республіці Іран. Із грудня 2006 року було заблоковано низку вебресурсів, зокрема енциклопедію Wikipedia, платформу YouTube та базу даних IMDb. Обмеження пояснювались необхідністю протидії деструктивному культурному впливу. У 2012 році Іран перейшов до використання власної національної інформаційної мережі (інтранету), відокремленої від глобального інформаційного простору [11].

Наразі інформаційні відносини в Україні залишаються однією з ключових сфер, що потребують посиленого нормативного регулювання, зокрема у частині запобігання кіберзлочинності та збереження цифрових доказів. З огляду на транснаціональний характер цифрових правопорушень, Україна активно інтегрується в міжнародну систему реагування на кіберінциденти. Одним із важливих кроків є участь у ініціативі «Мережа 24/7», яка функціонує в межах співробітництва країн G7 та дозволяє на постійній основі обмінюватися

інформацією між національними контактними пунктами.

Це забезпечує можливість оперативного збереження цифрових слідів злочинів, навіть якщо сервери чи вебресурси, пов'язані з порушеннями, розміщені за межами держави. В Україні така взаємодія реалізується через канали Національного центрального бюро Інтерполу. З урахуванням сучасних викликів, подальше вдосконалення міжвідомчої співпраці та міжнародно-правових інструментів вважається необхідним кроком для ефективного реагування на загрози в інформаційній сфері, зокрема у частині захисту персональних даних, цифрової ідентичності та прав інтелектуальної власності в онлайн-середовищі.

Висновки. Отже, аналіз практики державного втручання у сферу інформаційних відносин дає змогу виокремити коло ключових загроз, які викликають занепокоєння на міжнародному рівні. Серед них:

- ризики для національної безпеки;
- розповсюдження забороненого контенту, зокрема пов'язаного з експлуатацією дітей, наркотичними речовинами;
- порушення прав інтелектуальної власності та загроз комп'ютерній безпеці;
- обмеження прав і свобод учасників інформаційних відносин;
- втручання у режим конфіденційності персональних даних;
- торгівля фальсифікованими лікарськими засобами через цифрові платформи.

Враховуючи транснаціональний характер інформаційних правопорушень, зростає актуальність посилення міждержавної координації та правозастосовного потенціалу відповідних інституцій. Ефективне функціонування таких механізмів є передумовою належного захисту суб'єктів інформаційного права в умовах глобалізованого цифрового простору.

ЛІТЕРАТУРА:

1. Telecommunications Act of 1996. Public Law 104–104, USA. [Електронний ресурс]. Режим доступу: <https://www.fcc.gov/general/telecommunications-act-1996#:~:text=The%20Telecommunications%20Act%20of%201996,any%20market%20against%20any%20other.>
2. United Nations. Roadmap for Digital Cooperation. Report of the Secretary-General, 2023.
3. Барлоу, Дж. Пеппі. Декларація незалежності кіберпростору // Electronic Frontier Foundation. – 1996. [англ. Declaration of the Independence of Cyberspace].
4. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506. [Електронний ресурс]. Режим доступу: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

5. OECD. Global Forum on Digital Security for Prosperity. Reports 2022–2024. [Електронний ресурс]. Режим доступу: <https://www.oecd-events.org/global-forum-digital-security-for-prosperity/eventagenda>
6. Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512. [Електронний ресурс]. Режим доступу: <https://www.copyright.gov/legislation/dmca.pdf>
7. European Commission. Digital Services Act (DSA). Regulation (EU) 2022/2065. [Електронний ресурс]. Режим доступу: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065>
8. H.R.3261- Stop Online Piracy Act [Електронний ресурс] // The Library of Congress. – 2011. – Режим доступу до ресурсу: <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3261>.
9. Digital Economy Act 2010 [Електронний ресурс] // Parliament of the United Kingdom. – 2010. – Режим доступу до ресурсу: http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf.
10. Залєвська, І., Удренас, Г. (2022). Інформаційна безпека України в умовах російської військової агресії. Південноукраїнський правничий часопис, 1–2, с.20–26. [Електронний ресурс]. Режим доступу: <http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf>
11. Detektor Media. Вірусні новини. Історія Асіна Торабі... – 2025. URL: <https://detector.media> Березовська І. С., Русак, Д. М. Державна інформаційна політика України та основні напрями її вдосконалення // Міжнародні відносини. Серія «Економічні науки». 2014. № 4. [Електронний ресурс]. Режим доступу: http://journals.iir.kiev.ua/index.php/ec_n/issue/view/132.
12. Samuels J. An Alternative to SOPA: An Open Process Befitting an Open Internet [Електронний ресурс] / Samuels // Electronic Frontier Foundation. – 2011. – Режим доступу до ресурсу: <https://www.eff.org/ru/deeplinks/2011/12/alternative-sopa-open-process-befittingopen-internet>.

Дата першого надходження рукопису до видання: 25.07.2025

Дата прийнятого до друку рукопису після рецензування: 25.08.2025

Дата публікації: 26.09.2025