УДК 342.7:004.738

https://doi.org/10.52058/2786-6300-2025-12(42)-1411-1419

Скоморовський Віталій Богданович доктор юридичних наук, професор, професор кафедри теорії та історії держави і права Університету економіки та права «КРОК», м. Київ, https://orcid.org/0000-0002-1020-2322

Корольова Вікторія Вікторівна кандидат юридичних наук, доцент, завідувач кафедри державно-правових дисциплін Університету економіки та права «КРОК», м. Київ, https://orcid.org/0000-0003-2998-6144

МІЖНАРОДНІ СТАНДАРТИ РЕГУЛЮВАННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ В ІНТЕРНЕТІ

Анотація. У статті проаналізовано міжнародний досвід юридичної регламентації відповідальності за правопорушення в мережі Інтернет, зокрема акцентується на важливості закріплення права доступу до Інтернету як одного з центральних аспектів сучасного правового регулювання. Розглянуто законодавчі ініціативи різних країн, таких як Греція, Непал, Іспанія та Бразилія, які чітко визначають право громадян на участь в інформаційному суспільстві та державний обов’язок сприяти доступу до інформації в електронному вигляді. Вивчено також питання прозорості та доступності інформації в контрактах, що підкреслює важливість даних аспектів для формування довіри користувачів до постачальників послуг. У статті проаналізовано питання інформаційної безпеки, зокрема нормативні акти США, що визначають концепти цілісності, конфіденційності та доступності інформації. Важливість цих аспектів акцентується у зв'язку з сучасними ризиками, пов'язаними із кіберзлочинністю та зловживанням інформацією.

Крім того, розглянуто важливість запозичення міжнародних практик для України, де питання впровадження відповідальності за правопорушення в інформаційних технологіях стає дедалі актуальнішим у контексті глобальних викликів. На основі аналізу зазначених тенденцій, автори обґрунтовують необхідність адаптації вітчизняного законодавства до міжнародних стандартів, що повинно включати імплементацію концепцій електронного урядування, а також обмін досвідом в питаннях інформаційної безпеки.

У статті окреслюється, що існування комплексної системи правового регулювання є критично важливим для забезпечення захисту прав і свобод користувачів в цифровому середовищі. Пропонуються рекомендації щодо розвитку правових механізмів, які сприятимуть забезпеченню балансу між правами

громадян та вимогами інформаційної безпеки, а також моніторингу за виконанням норм, що регулюють використання мережі Інтернет.

Ключові слова: юридична відповідальність, права людини, Інтернет, інформаційні технології, кібербезпека, правозастосування, правове регулювання, міжнародне співробітництво, міжнародне право.

Skomorovsky Vitalii Bohdanovych Doctor of Law, Professor, Professor of the Department of Theory and History of State and Law, University of Economics and Law "KROK", Kyiv, https://orcid.org/0000-0002-1020-2322

Korolova Viktoriia Viktorivna Candidate of Law, Associate Professor, Head of the Department of Public-Law Disciplines, University of Economics and Law "KROK", Kyiv, https://orcid.org/0000-0003-2998-6144

INTERNATIONAL STANDARDS REGULATING LEGAL LIABILITY FOR INTERNET OFFENSES

Abstract. The article analyzes the international experience of legal regulation of liability for offenses on the Internet, in particular, it emphasizes the importance of consolidating the right to access the Internet as one of the central aspects of modern legal regulation. Legislative initiatives of various countries, such as Greece, Nepal, Spain and Brazil, are considered, which clearly define the right of citizens to participate in the information society and the state's obligation to facilitate access to information in electronic form. The issue of transparency and accessibility of information in contracts is also studied, which emphasizes the importance of these aspects for building user trust in service providers. The article analyzes the issue of information security, in particular, US regulations that define the concepts of integrity, confidentiality and availability of information. The importance of these aspects is emphasized in connection with modern risks associated with cybercrime and information abuse.

In addition, the importance of borrowing international practices for Ukraine is considered, where the issue of introducing liability for offenses in information technologies is becoming increasingly relevant in the context of global challenges. Based on the analysis of these trends, the authors justify the need to adapt domestic legislation to international standards, which should include the implementation of e-government concepts, as well as the exchange of experience in information security issues.

The article outlines that the existence of a comprehensive system of legal regulation is critically important for ensuring the protection of users' rights and freedoms in the digital environment. Recommendations are offered for the development of legal mechanisms that will help ensure a balance between citizens'

rights and information security requirements, as well as monitoring compliance with the norms governing the use of the Internet.

Keywords: legal liability, human rights, Internet, information technologies, cybersecurity, legal regulation, international cooperation, international law.

Постановка проблеми. У сучасному цифровому суспільстві Інтернет відіграє ключову роль у забезпеченні права на доступ до інформації, участі у публічному житті та розвитку соціальних відносин. Разом із тим, швидке поширення Інтернету породжує численні правові виклики, пов'язані з регулюванням доступу до мережі, захистом інформаційної безпеки, відповідальністю за правопорушення в кіберпросторі та забезпеченням балансу між свободою слова і безпекою. Зарубіжний досвід свідчить про різноманітні підходи до гарантування права на доступ до Інтернету: від конституційного закріплення цього права у Греції, Непалі та Іспанії до встановлення мінімальної швидкості підключення у Фінляндії та Естонії. Окремі держави, такі як США, Франція та Китай, поєднують доступ із жорсткими вимогами щодо інформаційної безпеки та контролю за контентом, що викликає дискусії щодо доцільності подібних обмежень.

В Україні питання правового забезпечення доступу до Інтернету та гарантування інформаційної безпеки поки що недостатньо врегульоване, що створює загрозу порушення прав користувачів та ускладнює ефективну протидію кіберзлочинності. Враховуючи глобальний характер Інтернету та його транснаціональні виклики, актуальною є проблема гармонізації національного законодавства із міжнародними стандартами у сфері цифрових прав та інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Варто виділити праці Д. Бойко, Д. Грибанова, М. Гури, Р. Дроб'язко, В. Жукова, В. Жарова, Р. Калюжного, А. Кананович, Є. Макарової, А. Незнамова, О. Пастухова, І. Рассолова, М. Стрелі, Є. Юркова та інших, у яких порушено широкий спектр актуальних проблем: від правової природи веб-сайту та специфіки правопорушень у мережі Інтернет до особливостей охорони об'єктів інтелектуальної власності та основних механізмів захисту прав у цифровому середовищі. Багато питань, пов'язаних із визначенням складу цифрових правопорушень, встановленням меж застосування існуючих інститутів юридичної відповідальності та адаптацією їх до специфіки кіберпростору, досі не отримали комплексного теоретико-методологічного вирішення. Зарубіжні дослідження зосереджуються на порівняльно-правовому аналізі гарантування права на доступ до Інтернету, регулюванні інформаційної безпеки, стандартах обслуговування та захисті прав користувачів. Досвід Бразилії, Фінляндії, Естонії, США, Франції та Китаю демонструє різноманітні підходи до балансу між свободою інформації та контролем за контентом,

що є важливим для формування міжнародних стандартів у сфері кібербезпеки та відповідальності за правопорушення в мережі даного дослідження.

Мета статті – здійснити комплексний аналіз зарубіжних підходів до правового регулювання доступу до Інтернету та забезпечення інформаційної безпеки з метою окреслення орієнтирів для подальшого вдосконалення національного законодавства України.

Виклад основного матеріалу. Одним з центральних аспектів регулювання мережі Інтернет у низці держав на порядку денному є закріплення права на доступ до Інтернету. Право на доступ до Інтернету регулюється законами кількох держав на національному рівні. Наприклад, Конституція Греції визначає право кожного громадянина на участь у інформаційному суспільстві та обов'язок держави сприяти доступу до інформації у електронній формі. У Конституції Непалу закріплено заборону закривати або скасовувати реєстрацію телебачення, Інтернету та інших цифрових та електронних засобів масової інформації через публікацію, трансляцію чи видання будь-яких матеріалів. У Королівстві Іспанії доступ до Інтернету регулюється Органічним законом «Про стійку економіку» (2011 р.) [90, с. 389].

Фінляндія прийняла Декрет Міністерства транспорту та комунікацій, який встановлює мінімальну швидкість функціонального Інтернет-доступу як універсальну послугу, що повинна бути надана з мінімальною швидкістю 1 Мб/с. Дотичну практику було упроваджено в Естонії у 2000 р: тутешній парламент запустив масову програму з розширення доступу для сільської місцевості. Інтернет, як стверджує уряд, має велике значення для життя в XXI ст. Уряд Іспанії гарантував своїм громадянам із 2011 р. загальний доступ до Інтернету на території всієї країни зі швидкістю передачі даних щонайменше 1 Мбіт/с за розумною ціною [91].

У законодавствах Франції, Албанії, Німеччини, Іспанії, Туреччини та Чорногорії гарантується право на доступ до Інтернету в цілому. У деяких інших країнах, таких як Грузія, Португалія, Кіпр та Україна, право на доступ до Інтернету пов'язане з правом на інформацію та зв'язок, що передбачені їхніми Основними законами.

Досвід Бразилії в регулюванні права на доступ до Інтернету є цікавим та важливим для розгляду. Згідно з Біллем про Інтернет-права Бразилії, прийнятим у 2014 році, користувачам надаються певні права та гарантії, що стосуються доступу до Інтернет-мережі. Основні положення цього закону можуть бути проаналізовані наступним чином:

1. обслуговування Інтернет-з'єднання: Більшість користувачів має право на обслуговування Інтернет-з'єднання. Це означає, що постачальники послуг повинні забезпечити доступ до Інтернету користувачам.

2. Постійне підключення: Закон передбачає право користувачів на постійне підключення до мережі відповідно до якості, зазначеної у контракті з постачальником послуг. Це забезпечує стабільний доступ до Інтернету.

3. Інформація в контрактах: Користувачі мають право на чітку й повну інформацію в контрактах з постачальниками послуг. Це сприяє транспарентності та забезпечує, що користувачі розуміють умови свого контракту.

Ці права та гарантії спрямовані на забезпечення доступу до Інтернету для всіх громадян та користувачів і підкреслюють важливість цього доступу для участі в публічних справах, культурному житті та розвитку знань та інформації. Бразильський досвід підкреслює необхідність захисту прав користувачів Інтернету і сприяє розширенню доступу до цифрового середовища [92, с. 20; 93, с. 79].

Чільне місце у регламентації мережі Інтернет займає питання забезпечення інформаційної безпеки. Зокрема, одним з найбільш прогресивних прогнозовано у цьому питанні є досвід США. Закон США, відомий як «Про управління інформаційною безпекою», прийнятий у 2002 році, визначає інформаційну безпеку як захист інформації та інформаційних систем від незаконного доступу, використання, розкриття, поширення, зміни або знищення. Ця безпека також включає забезпечення цілісності інформації, щоб запобігти її незаконній зміні або знищенню, включаючи підтримку її автентичності. Також вона включає забезпечення конфіденційності, яка передбачає дотримання обмежень доступу і поширення інформації, включаючи збереження приватних даних та власності, і забезпечення доступності, що передбачає швидкий і надійний доступ до інформації. Багато інших країн також використовують аналогічні поняття, такі як «автентичність», «доступність», «цілісність» та «конфіденційність», при регулюванні питань інформаційної безпеки. Федеральний Закон США «Про захист інформації» від 1998 року використовує подібні поняття, і він розширюється на облікові записи, ведені як державними установами, так і приватними компаніями, та встановлює обмеження на використання персональних даних і доступ до облікових записів [94].

У цьому контексті в Швеції і Фінляндії існують юридичні обмеження на доступ до урядової інформації. Важливо відзначити, що в інших зарубіжних країнах, а також в Україні, існує схожа тенденція – це розробка та впровадження концепцій електронного уряду. Ця концепція базується на використанні інформаційних технологій для створення державних інформаційних ресурсів та полегшення доступу до інформації про діяльність державних органів влади, а також на розміщенні відкритих даних. Ця практика реалізується у країнах, таких як США, Сінгапур, Австралія, Нова Зеландія та інші.

Наприклад, в Австрії законодавчо встановлено право громадян на доступ до нормативно-правової бази, і при цьому ця інформація перебуває в розпорядженні державного сектору, а не комерційних структур. При цьому може стягуватися плата за копіювання та поширення цієї інформації.

Отже, аналіз зарубіжного досвіду в галузі правового регулювання доступу до інформації показує, що існують загальні тенденції, але різні підходи до забезпечення інформаційної безпеки [95].

Значний масив законодавчих та інших нормативних правових актів у галузі забезпечення інформаційної безпеки в багатьох зарубіжних державах стосується електронної торгівлі та використання електронних підписів. Це зокрема Закон Канади «Про електронні угоди» 1999 року, Федеральний закон США «Про електронні підписи в міжнародній і внутрішній торгівлі» 2000 року, Закон Ірландії «Про електронну торгівлю» 2000 року, Закон Іспанії «Про послуги інформаційного суспільства та електронної торгівлі» 2002 року, Закон Південної Кореї «Про електронну торгівлю» 2001 року, Закон Таїланду «Про електронні угоди і електронного підпису» 2002 року тощо [96; 97, с. 23].

У Франції діють спеціальні закони, що забороняють публікацію матеріалів, що містять нацистську символіку, яка підтримує ідеї нацизму. Також привертає увагу французький Закон про обов'язкову реєстрацію власників сайтів країни і про кримінальну відповідальність провайдерів за надання хостингу ідентифікованим користувачам. Ще одним цікавим моментом даного нормативно-правового акту є встановлення вимоги до провайдерів про надання відомостей про авторів сайтів будь-яким третім особам, за порушення якої передбачена кримінальна відповідальність. Також даний вид відповідальності передбачений за надання неповних або недостовірних відомостей авторами французьких сайтів і за надання провайдерами місця на сервері ідентифікованим користувачем. Причому, по всіх сайтах, авторство яких не встановлено, відповідальність несе провайдер, а можливою мірою покарання є позбавлення волі строком на півроку. Будь-яка державна діяльність по встановленню контролю за громадянами апріорі є негативною, тому такий напрямок розвитку в частині інформаційної безпеки та протидії злочинності в мережі Інтернет не вважаємо доцільним. Однак, з огляду на останні тенденції розвитку вітчизняного законодавства, питання встановлення відповідальності за порушення правил авторизації в кібермережах рано чи пізно виявляться на порядку денному вітчизняного законодавця. За таких умов доцільним буде аналіз співставлення ретроспективи становлення зазначених законів і законодавства України [98].

Беручи до уваги вільний характер поширення інформації в Інтернеті, деякі країни впроваджують юридичні обмеження, спрямовані на зменшення або уникнення можливих загроз незалежності та забезпечення безпеки. Наприклад, в Індії у 2007 році було прийнято Закон про інформаційні технології, який ввів часткову цензуру на підставі терористичних актів у Мумбаї, зокрема обмеження стосувалися політичних та екстремістських ресурсів. У Єгипті в 2018 році було прийнято Закон про боротьбу з кіберзлочинністю, що посилив контроль держави над Інтернетом та блокуванням сайтів, а в Пакистані також блокуються ресурси через їхні етносепаратистські матеріали.

Слід відзначити, що проблеми з доступом до Інтернету також відзначаються у Китаї. Обмеження доступу в цій країні були введені поетапно. У 2000 році був затверджений документ «Адміністративні заходи, пов'язані з інформаційними послугами в мережі Інтернет», який містив перелік обмежень стосовно створення та розповсюдження інформації, що ставало підставою для її блокування. Більшість цих обмежень стосувалися авторитету, безпеки та підтримання порядку в державі. Також у той же рік була створена «Інтернет-поліція», яка відповідає за виявлення, фільтрацію та блокування контенту, що спричинює загрозу для держави.

У 2002 році в Китаї було заборонено доступ до пошукової системи Google, а в 2009 році в країні відбулися заворушення, організовані за допомогою соціальної мережі Facebook, що призвели до запровадження заборони на цю соціальну мережу. Також у 2009 році розпочався проект «Золотий щит», спрямований на блокування сайтів зі «шкідливим» вмістом. Сьогодні «Золотий щит» не обмежується лише блокуванням сайтів, а став комплексною системою ідентифікації користувачів, фільтрації контенту, відеомоніторингу та впровадження антивірусних систем [98, с. 34].

Висновки. Аналіз зарубіжного досвіду правового регулювання доступу до Інтернету та забезпечення інформаційної безпеки дає підстави стверджувати, що у світі сформувалися дві ключові тенденції: розширення гарантій доступу до Інтернету як необхідної умови реалізації прав людини та водночас посилення державного контролю з метою забезпечення безпеки інформаційного простору. Значна частина держав, зокрема країни ЄС, США, Бразилія, Фінляндія та Естонія, упроваджують нормативні механізми, спрямовані на забезпечення універсального доступу, встановлення мінімальних стандартів якості Інтернет-послуг та захист прав користувачів. У цих країнах Інтернет розглядається як інфраструктура, необхідна для участі громадян у суспільному, економічному та культурному житті.

Водночас у низці держав – Китаї, Індії, Пакистані, Єгипті – домінує підхід, зорієнтований на обмеження доступу до мережі на тлі безпекових викликів, що супроводжується різними формами цензури, фільтрації контенту та контролю за діяльністю користувачів. Така модель демонструє, що питання інформаційної безпеки часто набуває пріоритету над забезпеченням цифрових прав.

Особливе місце у регулюванні займають положення, які стосуються електронної торгівлі, електронного підпису та електронного урядування. Вони свідчать про перехід держав до цифрової моделі публічного управління, яка потребує належного правового забезпечення, захисту персональних даних та створення безпечної інфраструктури.

Важливою є також практика окремих країн щодо обмеження незаконного або шкідливого контенту, однак надмірний контроль за діяльністю користувачів,

як демонструє досвід Франції та деяких азійських держав, створює ризики для прав і свобод людини. Це потребує виваженого законодавчого підходу, аби уникнути надмірного втручання держави у приватну сферу.

Для України узагальнений зарубіжний досвід може слугувати основою для подальшого вдосконалення національної моделі цифрового регулювання. Зокрема, актуальним є закріплення чітких гарантій доступу до Інтернету, розвиток електронного урядування, удосконалення нормативної бази щодо електронних послуг, а також формування збалансованої системи інформаційної безпеки, яка поєднуватиме захист державних інтересів із дотриманням прав і свобод громадян.

Література:

1. Попович Т. Право на доступ до Інтернету: зарубіжний досвід правового регулювання. *Науковий вісник Ужгородського національного університету.* 2021. № 5. С. 376-385.

2. Швидка Т.О. Законодавче закріплення права на доступ до Інтернету. *Підприємництво, господарство і право.* 2021. № 5. С. 145-150.

3. Brazil's Internet Bill of Rights: A Closer Look / C.A. Souza, M. Viola, R. Lemos. Rio de Janeiro: Institute for Technology and Society of Rio de Janeiro, 2017. 140 p.

4. Мукомела І.В. Право на доступ до Інтернету: проблеми визначення та забезпечення. *Вісник Національної академії правових наук України*. 2016. № 4 (87) С. 77-82.

5. Скалацький В.М. Інформаційне суспільство: сучасні теорії та моделі (соціально-філософський аналіз): дис.: 09.00.03. Київ: Київ. нац. ун-т ім. Тараса Шевченка, 2006. 181 с.

6. Бусакевич А.В., Стець О.М. Проблеми сучасного регулювання відносин в мережі Інтернет. https://doi.org/10.25313/2520-2308-2023-8.

7. Building the Information Society: Moving Canada into the 21st Century [Нормативний документ Міністерства Постачання та Послуг Канади] / Ministry of Supply and Services. Ottawa, 1996.

8. Грабар Н.С. Зарубіжний досвід правового регулювання забезпечення інформаційної безпеки. *Теорія та практика державного управління і місцевого самоврядування.* 2020. № 1. С. 20-41.

9. Турута О. Інтернет і право на свободу слова (порівняльно-правовий аспект). *Публічне право*. 2012. № 4. С. 31-35.

References:

1. Popovych, T. (2021). Pravo na dostup do Internetu: zarubizhnyi dosvid pravovoho rehuliuvannia [The right to Internet access: Foreign experience of legal regulation]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*, (5), 376–385. [in Ukrainian]

2. Shvydka, T.O. (2021). Zakonodavche zakriplennia prava na dostup do Internetu [Legislative consolidation of the right to Internet access]. *Pidpryiemnytstvo, hospodarstvo i pravo*, (5), 145–150. [in Ukrainian]

3. Souza, C.A., Viola, M., & Lemos, R. (2017). *Brazil's Internet Bill of Rights: A Closer Look*. Rio de Janeiro: Institute for Technology and Society of Rio de Janeiro. 140 p. [in English]

4. Mukomela, I.V. (2016). Pravo na dostup do Internetu: problemy vyznachennia ta zabezpechennia [The right to Internet access: Problems of definition and ensuring]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*, 4(87), 77–82. [in Ukrainian]

5. Skalatskyi, V.M. (2006). *Informatsiine suspilstvo: suchasni teorii ta modeli (sotsialno-filosofskyi analiz)* [Information society: Modern theories and models (socio-philosophical analysis)] (PhD dissertation, Taras Shevchenko National University of Kyiv). 181 p. [in Ukrainian]

6. Busakevych, A.V., & Stets, O.M. (2023). Problemy suchasnoho rehuliuvannia vidnosyn v merezhi Internet [Problems of modern regulation of relations on the Internet]. https://doi.org/10.25313/2520-2308-2023-8. [in Ukrainian]

7. Ministry of Supply and Services Canada. (1996). *Building the Information Society: Moving Canada into the 21st Century* [Government normative document]. Ottawa. [in English]

8. Hrabar, N.S. (2020). Zarubizhnyi dosvid pravovoho rehuliuvannia zabezpechennia informatsiinoi bezpeky [Foreign experience of legal regulation of information security]. *Teoriia ta praktyka derzhavnoho upravlinnia i mistsevoho samovriaduvannia*, (1), 20–41. [in Ukrainian]

9. Turuta, O. (2012). Internet i pravo na svobodu slova (porivnialno-pravovyi aspekt) [Internet and the right to freedom of speech (comparative legal aspect)]. *Publichne pravo*, (4), 31–35. [in Ukrainian]