DOI: https://doi.org/10.37634/efp.2026.1.12
УДК 343.013

Антон Володимирович ***ЧУБ***
д.ю.н., завідувач кафедри, Національна академія управління
ORCID: https://orcid.org/0000-0002-6900-4865
e-mail: a.chub.advokat@gmail.com

Віталій Олександрович ***КАРПІЧКОВ***
к.ю.н., доцент, Київський національний університет ім. Тараса Шевченка
ORCID: https://orcid.org/0000-0001-8529-1246
e-mail: n.zagrebelna@ukr.net

ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ У КІБЕРПРОСТОРІ: АНАЛІЗ ЗАРУБІЖНИХ ДОКТРИН

У статті досліджено теоретико-правові засади юридичної відповідальності у кіберпросторі на основі аналізу зарубіжних доктрин. Висвітлено специфічні риси Інтернету, що ускладнюють традиційне регулювання: транскордонність, децентралізація та відсутність фізичного контакту. Проаналізовано підходи Е. Катша, Д. Поста, С. Бреннер та С. Хевен до юрисдикції та національних принципів відповідальності. Особливу увагу приділено теорії Л. Лессіга про програмний код як регулятор поведінки. Обґрунтовано роль Будапештської конвенції у гармонізації міжнародних стандартів боротьби з кіберзлочинністю.

Ключові слова: *юридична відповідальність, кіберпростір, Інтернет, правопорушення, зарубіжна доктрина, цифрове середовище, діджиталізація, міжнародне співробітництво, інформаційні технології, цифрові права*

ВСТУП

У сучасних умовах цифровізація суспільства та стрімкий розвиток інформаційно-комунікаційних технологій створюють нові виклики для правової системи та механізмів юридичної відповідальності. Особливо актуальним стає питання протидії правопорушенням у мережі Інтернет, де традиційні моделі регулювання часто виявляються недостатніми через динамічність, децентралізовану структуру та транскордонний характер цифрового середовища.

МЕТА дослідження – сформувати комплексне наукове уявлення про правові механізми юридичної відповідальності у кіберпросторі на основі аналізу зарубіжних доктрин.

МЕТОДИ ДОСЛІДЖЕННЯ

Методи дослідження включають систематичний аналіз зарубіжних наукових джерел та нормативно-правових актів, що регулюють питання юридичної відповідальності в кіберпросторі. Застосовано порівняльний метод для вивчення різних правових систем і підходів до регулювання правопорушень в мережі Інтернет. Також застосовано міждисциплінарний підхід, що поєднує правові, соціальні та технічні аспекти для всебічного осмислення теми.

РЕЗУЛЬТАТИ

Зарубіжний досвід у сфері правового регулювання цифрового середовища є надзвичайно цінним для наукового аналізу проблематики, оскільки США, Велика Британія, Канада, Японія та країни Західної Європи стали центрами формування правових підходів у постіндустріальну інформаційну епоху ще на зламі 1980-1990-х рр. У цих юрисдикціях відбулася рання трансформація громадянського суспільства під впливом економічних, соціальних та політичних чинників, що зумовило розвиток концепцій регулювання цифрового простору та встановлення юридичної відповідальності за порушення у ньому. На думку E. Katsh, необхідність регулювання Інтернет-відносин полягає в тому, що правові питання стають актуальними у новому цифровому світі, де право починає рухатися у нових напрямах та втрачає свою традиційну форму, переходячи з паперу на екрани. В роботі «Law in digital world» E. Katsh вказує на те, що правові норми поширюються на рухливі та мобільні простори, де індивідуальні та колективні можливості комунікації ростуть, і де право вступає в контакт з новими визначеннями та очікуваннями, оптимально складним втіленням якого є мережа Інтернет [1, с. 84].

D. Post вважає, що мережа Інтернет апріорі не піддається централізованому регулюванню чи регламентації, тому правопорушення, що вчиняються у цьому цифровому середовищі, мають розглядатися казуально, зокрема із застосуванням принципу sui generis. З одного боку, така позиція має право на існування. Водночас, як ми вже зазначили та наводили в розрізі репрезентації результатів досліджень інших науковців, динаміка кількості правопорушень в мережі Інтернет зростає шаленими темпами, що зокрема спричинено ступенем сучасної діджиталізації. Тобто юстиція за кожним окремим випадком приречена на безнадійність в розумінні функціонування судової й правоохоронної систем, що суперечить положенням Європейської конвенції з прав людини [2] та принципу Judicis est jus dicere non dare.

Праця цього дослідника, крім іншого, містить достатньо повний та всебічний опис специфічних рис:

1. Інтернет є загальнодоступним і необмежений географічними кордонами. Це дає користувачам можливість змінювати юрисдикційну компетенцію і переходити під більш вигідні правила або контроль. Інтернет дає змогу відносно легко переходити від однієї юрисдикційної компетенції однієї держави до іншої або уникати втручання регулятора, що призводить до створення «вільного ринку» нормативних режимів.

2. Деякі види діяльності в Інтернет можуть бути неконтрольованими і закодованими, що ускладнює відслідковування та перехоплення комунікацій з боку держави.

3. Наукова література не має загальноприйнятого поняття, пов'язаного з регулюванням інформації та Інтернет.

4. Невідомо, як вплив Інтернет-права вплине на свободу розповсюдження інформації і чи може воно стати інструментом для введення цензури.

5. Нині не створено механізми впровадження і реалізації національного права у віртуальному просторі, й ефективність цих механізмів є невідомою. Спірним є питання, які установи можуть встановлювати правила в Інтернет та забезпечувати їхній захист.

6. Неясно, як Інтернет-право має застосовуватися, оскільки важко визначити точний момент здійснення акту або певної події в цьому середовищі. Крім того, можливості покарання правопорушників в Інтернет обмежено необхідністю ідентифікації правопорушника і вимогами до матеріального здійснення правопорушення [3].

Підтримала цей погляд й американська дослідниця Suzan V. Brenner. Вона підкреслює, що найбільш проблемною характеристикою Інтернет з погляду юрисдикційної політики є те, що він стирає межу між внутрішньодержавною і міжнародною передачею інформації [4, с. 349]. Також Suzan V. Brenner диверсифікує такі ознаки правопорушень в мережі Інтернет:

– вони не вимагають фізичного контакту між жертвою та злочинцем у момент вчинення злочину;

– часто є автоматизованим за своєю природою вчинення. Це означає, що суб'єкт злочину за допомогою комп'ютерних технологій може протягом короткого періоду часу вчинити багато правопорушень, що значно збільшує їх кількість;

– суб'єкт правопорушення в мережі Інтернет необмежений фізичними обставинами, які є в реальному світі.

Неординарний підхід запропонувала C. Heven. Вчена переконана й наводить аргументи на користь того, що логічно регулювати Інтернет подібно до інших глобальних просторів, які використовуються на користь всіх країн і не піддаються військовій мілітаризації. Вона запропонувала встановити відповідальність у кіберпросторі відповідно до національного принципу кримінальної юрисдикції, діючий на території інших загальнодоступних територій. Це означає, що особа, яка вчинила злочин у кіберпросторі, підлягатиме відповідальності перед країною свого громадянства. Вона також вказує на необхідність узгодження загальних правил користування Інтернет на міжнародному рівні та впровадження принципу обов'язкового співробітництва між країнами у розслідуванні злочинів, вчинених в кіберпросторі [5, с. 64]. Зауважимо, що у разі реалізації схожої концепції світ зіткнувся зі схожою проблемою, котра часто виражається у міжнародному публічному праві: держави регулярно під виглядом благих намірів просто лобіюють власні інтереси, що у підсумку не сприяє адекватному розв'язанню проблеми. Як результат, у разі правового регулювання мережі Інтернет та встановлення якихось одних планетарних стандартів і засад регламентації правопорушень в мережі Інтернет, юридичної відповідальності за них був би високий рівень монополізації та нав'язування позиції сили більш технологічно розвинутими державами.

A. Stein, розглядаючи проблематику юрисдикційності в контексті правопорушень в мережі Інтернет, дійшов висновку, що унормування юридичної відповідальності можливе лише на рівні кожної окремої держави з урахуванням специфіки правової системи, формалізованих джерел права та практики правозастосування. Водночас автором не заперечується позиція стосовно створення наднаціональних (проте не глобальних) інструментів захисту і відповідно інструментів примусу відносно правопорушників за посягання в мережі Інтернет [6, с. 424].

У сучасному науковому осмисленні правопорушень у мережі Інтернет значно зростає увага до комплексного міждисциплінарного підходу, що поєднує правові, технічні та соціальні аспекти. Так, дослідники підкреслюють, що цифрове середовище характеризується високою динамічністю, децентралізованою структурою та тісним зв'язком з технічними протоколами, що створює нові виклики для класичних правових парадигм. З огляду на це, коментатори Інтернет-права зауважують, що традиційні юридичні моделі часто виявляються недостатніми для ефективного регулювання поведінки в цифровому просторі, оскільки технологічні реалізації можуть мати регуляторний ефект, який не завжди охоплюється формальними нормами права.

Однією з фундаментальних робіт у цій галузі є монографія Lawrence Lessig «Code and Other Laws of Cyberspace» та її оновлене видання «*Code: Version 2.0*» (2006), де автор розглядає спосіб, у який програмний код і технічні стандарти формують поведінку у цифровому середовищі подібно до юридичних норм. Lessig підкреслює, що поряд із законодавством архітектура інформаційних систем є вагомим регулятором, що впливає на те, що саме є можливим або забороненим у мережі.

Крім того, сучасні дослідження Інтернет-права зосереджено на проблемах юрисдикції та міжнародного співробітництва у випадках правопорушень, що мають транснаціональний характер. У багатьох країнах суди та науковці стикаються з питаннями, як визначати компетентну правову систему у спорах, що виникають у глобальній мережі, та які критерії мають застосовуватися для встановлення юрисдикційної належності. Дискусії охоплюють як територіальні принципи застосування права, так і підходи, які враховують місце виникнення юридично значимих наслідків правопорушення або значний зв'язок з певною правовою системою.

На рівні міжнародного співробітництва з протидії кіберзлочинності значну увагу привертає Будапештська конвенція Ради Європи про кіберзлочинність, яка встановлює рамкові стандарти криміналізації певних діянь у кіберпросторі та механізми міжнародної правової допомоги та координації. Ця конвенція є прикладом того, як міжнародний правовий режим може сприяти узгодженню різних національних підходів до питань юридичної відповідальності за правопорушення в мережі.

В межах сучасного наукового дискурсу питання протидії правопорушенням у мережі Інтернет та встановлення юридичної відповідальності за дії в цифровому середовищі широко досліджуються як у рамках національного, так і міжнародного права. Це пояснюється тим, що трансформація громадянського суспільства під впливом глобальної цифровізації спричинила появу нових видів правопорушень, які виходять за межі традиційних правових категорій. З огляду на це закордонна наукова думка концентрує увагу на комплексному аналізі правових, технологічних і соціальних аспектів функціонування правопорядку у цифровому середовищі.

Одним з ключових елементів міжнародної системи правового регулювання у сфері кіберзлочинності є Будапештська конвенція Ради Європи про кіберзлочин-

ність (2001), що встановлює загальні стандарти криміналізації окремих діянь у кіберпросторі, а також механізми міжнародного співробітництва у розслідуванні та притягненні до відповідальності за такі правопорушення. Цей документ широко цитується у науковій літературі як базовий міжнародний правовий інструмент, що сприяє узгодженню різних національних правових систем у сфері боротьби з кіберзлочинністю.

Теоретичні дослідження у сфері Інтернет-права також звертають увагу на проблеми юрисдикції та застосування права у глобальному цифровому середовищі. Так, у класичному аналізі юридичних наслідків функціонування Інтернет автори наголошують, що традиційні підходи до встановлення юрисдикції (територіальні принципи, місце реєстрації сервера чи проживання сторін) не завжди адекватні для цифрового простору, де правовідносини часто мають транскордонний характер і не обмежуються фізичними кордонами. Це питання активно досліджується у працях з порівняльного та міжнародного права. Загалом зарубіжні дослідження у цій сфері підкреслюють необхідність міжнародної координації правових норм, спрямованих на захист прав і свобод у цифровому середовищі, а також формування ефективних механізмів відповідальності за правопорушення в Інтернет. У цьому контексті науковці звертають увагу на важливість інтеграції національного законодавства з міжнародними стандартами, зокрема у питаннях взаємної правової допомоги та обміну доказами між державами.

ВИСНОВКИ

Отже, іноземна доктрина в розрізі проблематики правопорушень в мережі Інтернет має більш глибоке коріння та тривалу історію становлення. Висловлені закордонними авторами позиції переважно не резонують з вітчизняними дослідженнями. Багато в чому цей факт спричинений спільною рецепцією ідей та концепцій для їхнього подальшого розроблення. Водночас в закордонних джерелах є більш розлогий плюралізм стосовно самого базису регулювання мережі Інтернет та юридичної відповідальності за правопорушення в цій мережі відповідно.

References

1. Katsh M.E. Law in a Digital World. Oxford, 1995. pp. 81-94. URL: https://surl.li/ektqmr

2. Convention for the Protection of Human Rights and Fundamental Freedoms (with protocols) (European Convention on Human Rights): International Convention of Nov. 4, 1950: as of Aug. 1, 2021. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text [in Ukrainian].

3. Post D.G. Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace. *Journal of Online Law.* 1995. URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/iljuta29&div=81&id=&page

4. Brenner S.V. Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? *Rutgers Computer & Technology Law Journal.* 2004. Vol. 30. Iss. 1. pp. 342–357. URL: https://surl.lu/umanzy

5. Heaven C.P. A Proposal for Removing Road Blocks from the Information Superhighway By Using an Integrated International Approach to Internet Jurisdiction. *Minnesota Journal of Global Trade.* 2001. Vol. 10. pp. 373–384. URL: https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1120&context=mjil

6. Stein A.R. Symposium: Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision. *Northwestern University Law Review.* 2004. Vol. 98. pp. 411–454. URL: http://dx.doi.org/10.21511/bbs.16(1).2021.07

Anton CHUB
Doctor of Legal Sciences, Head of the Department, National Academy of Management
ORCID: https://orcid.org/0000-0002-6900-4865
e-mail: a.chub.advokat@gmail.com

Vitalii KARPICHKOV
PhD in Legal Sciences, Associate Professor, Taras Shevchenko National University of Kyiv
ORCID: https://orcid.org/0000-0001-8529-1246
e-mail: n.zagrebelna@ukr.net

LEGAL LIABILITY IN CYBERSPACE: ANALYSIS OF FOREIGN DOCTRINES

Introduction. *In current conditions characterized by the rapid digitalization of society and the development of information and communication technologies, new challenges arising before the legal system are analyzed, in particular regarding the mechanisms of legal liability for offenses committed in the Internet space. The relevance of this topic is determined by the growing complexity of traditional models of legal regulation, which often do not correspond to the dynamic and decentralized nature of the digital environment, providing new opportunities for criminal activity.*

The purpose of the paper *is to form a comprehensive scientific understanding of the legal mechanisms of legal liability in cyberspace based on the analysis of foreign doctrines.*

Results. *In the study, the views of such authors as E. Katsch, D. Post, S. Brenner, A. Stein and S. Haven were studied, who express unique considerations regarding legal liability for offenses committed in the Internet space. It was found that the Internet, limited only by conditional borders, allows offenders to avoid jurisdictional norms, making their identification difficult. The constant growth of the number of automated actions on the Internet confirms the need to adapt legal norms to the conditions of the new digital environment. The specifics of offenses in cyberspace, which often occur without physical contact between subjects, are studied. It is noted that such offenses are mostly automated, which significantly increases the level of threat to society and requires new regulatory approaches. The need to integrate national legislation with international standards is also analyzed, in particular in the context of the Budapest Convention, which promotes the establishment of common norms and mechanisms of liability for cybercrimes.*

Conclusions. *The studied positions of foreign authors reveal significant differences with domestic research, which emphasizes the need for a further integrative approach to legal mechanisms of liability. The importance of pluralism of foreign concepts and their adaptation to the domestic context is emphasized.*

Keywords: *legal responsibility, cyberspace, Internet, offenses, foreign doctrine, digital environment, digitalization, international cooperation, information technology, digital rights*