УДК 342.52

МАРУЩАК Анатолій Іванович

МІЖНАРОДНО-ПРАВОВІ ПІДХОДИ ТА НАЦІОНАЛЬНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

Постановка проблеми. Правові механізми протидії дезінформації розбудовуються і в Україні, і в інших державах світу. Складність міжнародного та національного права щодо кампаній (операцій) із дезінформації зумовлена їхнім зв'язком як із кібероперераціями, так і з правовими вимогами щодо гарантування свободи слова.

На рівні міжнародно-правового регулювання положення щодо протидії дезінформації, як і загалом кібероперераціям, фактично не визначені. Останні можуть сприйматися як частина шпигунської діяльності, яка по суті не заборонена міжнародним правом.

На рівні національного законодавства держави використовують різні підходи щодо протидії дезінформації: від застосування положень чинних цивільних, адміністративних, а подекуди й кримінальних норм, що регулюють діяльність засобів масової інформації (далі – ЗМІ) та протидію дифамації, інформування громадян про небезпеку фейкових новин, до розроблення та прийняття цілеспрямованого законодавства з протидії поширенню неправдивих новин із штрафними санкціями імперативного видалення неправдивої інформації.

Створення в Україні Центру протидії дезінформації [1] і регламентування його діяльності в умовах загроз інформаційній безпеці держави потребує аналізу теоретико-правових основ протидії дезінформації з урахуванням фундаментальних принципів свободи думки і слова.

Аналіз останніх досліджень і публікацій свідчить про те, що питання інформаційної безпеки були предметом досліджень багатьох українських учених, а саме: В. Остроухова, В. Панченко, В. Петрова, В. Пилипчука, В. Польового, О. Розвадовського, Є. Скулиша, Т. Ткачука, О. Юрченка й ін.

Ще у 1934 році Л. Преус указував на «інтенсивні кампанії ворожої та підривної пропаганди проти територіальної цілісності та політичного порядку іноземних держав» [2]. Останніми роками проблеми протидії онлайн дезінформації досліджували К. Лангвардт [3], Б. Бреннен [4], Н. Янкович [5] та інші зарубіжні дослідники.

Однак у цілому питання міжнародно-правового та національно-правового регулювання протидії дезінформації було предметом наукових досліджень лише фрагментарно.

Метою статті є розкриття міжнародно-правових підходів і національно-правового регулювання протидії дезінформації.

Виклад основного матеріалу. Наукова думка та погляди юристів-практиків на проблему кібероперацій загалом і протидії дезінформації зокрема на сьогодні неодностайні. Наприклад, існують різні думки щодо російського втручання у вибори в США у 2016 році. Деякі зарубіжні автори визначають це як порушення міжнародного права [6]; інші не знаходять правових підстав для визнання таких дій порушенням [7]. Відповідь на питання кваліфікації дезінформаційних операцій як порушення норм міжнародного права має суттєве практичне значення. Адже визначення того, що дезінформаційні кампанії як різновид кібероперацій є порушенням міжнародного права, може стати передумовою для законного застосування державою сили на підставі норм міжнародного права. У цьому контексті зазначимо, що Гарі П. Корн припускає, що «незалежно від того, наскільки ймовірними та передбачуваними наслідками поширення Росією дезінформації про COVID-19 є смерть та хвороба, малоймовірно, що держави підуть так далеко, щоб засуджувати дії Росії як перевищення порогу застосування сили ...» [8].

Статут Організації Об'єднаних Націй передбачає, що «всі члени у своїх міжнародних відносинах утримуються від погрози силою або її застосування проти територіальної цілісності чи політичної незалежності будь-якої держави або будь-яким іншим чином, що не відповідає цілям Організації Об'єднаних Націй» [9].

На рівні ООН із 2004 року функціонує п'ять груп урядових експертів із вивчення питань, пов'язаних із кіберопераціями. У грудні 2018 року Генеральна Асамблея встановила два процеси для обговорення питання безпеки при використанні інформаційно-комунікаційних технологій (далі – ІКТ) у період 2019–2021 років [10]. Заключний основний звіт OEWG у березні 2021 року визначає «добровільні, необов'язкові норми відповідальної поведінки держав … Держави підкреслили, що такі норми … дозволяють міжнародній спільноті оцінювати діяльність держав. Відповідно до резолюції 70/237 Генеральної Асамблеї та визнаючи резолюцію Генеральної Асамблеї 73/27, державами рекомендовано уникати та утримуватися від використання ІКТ, що суперечить нормам відповідальної поведінки держав» [11]. Такий висновок, цілком очевидно, не переконає такі агресивно налаштовані держави, як Росія, припинити кібероперації, зокрема дезінформацію.

Міжнародне право, застосовне до кібероперацій, значною мірою залежить від висновків незалежних експертів із міжнародного права, зафіксованих у Талліннському посібнику 2.0 [12].

У цьому документі робиться висновок, що «кібероперації, пов'язані з державами, які порушують суверенітет іншої держави, суперечать міжнародному праву» [12]. Відповідно до Талліннського посібника 2.0 міжнародне право, що застосовується до кібероперацій, масштаби та наслідки

певної кібероперації [12] можуть спровокувати поріг застосування сили в кібероперація.

Втручання у вибори, охорону здоров'я й інші сфери державного суверенітету за допомогою операцій з дезінформації можна тлумачити як такі, що суперечать міжнародному праву. Але, як зазначає Майкл Шмітт, міжнародне право в застосуванні до кібероперацій знаходиться «… в зародковому стані; багатьом питанням бракує ясності або вони є предметом важливих розбіжностей, що важливо брати до уваги, розкладаючи операції на їхні юридичні компоненти» [13].

Нарешті, можна припустити, що за аналогією з Додатковим протоколом до Конвенції про кіберзлочинність щодо криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи [14], найближчим часом може бути розроблено додатковий протокол до Конвенції про кіберзлочинність для боротьби з дезінформацією. Такий розвиток міжнародно-правового регулювання буде ймовірнішим, якщо тенденція криміналізації дезінформації (про яку йдеться нижче) поширіться на більшість країн світу.

Міжнародне право містить норму, що стосується свободи вираження поглядів, яка є життєво важливою для формування законодавчої бази із протидії дезінформації. Загальний коментар до статті 19 Міжнародного пакту про громадянські і політичні права передбачає: «Коли держава-учасниця посилається на законні підстави для обмеження свободи вираження поглядів, вона повинна продемонструвати конкретним і індивідуалізованим способом точний характер загрози, а також необхідність і пропорційність конкретних вжитих заходів, зокрема шляхом встановлення прямого та безпосереднього зв'язку між висловлюванням і загрозою» [15]. Можна зробити висновок, що для легітимізації діяльності з протидії дезінформації держава має продемонструвати: 1) точний характер загрози; 2) необхідність і пропорційність конкретної дії; 3) прямий і безпосередній зв'язок між певним висловлюванням і загрозою. Запропонована структура, що враховує принципи свободи думки і слова, має бути імплементована у вітчизняне законодавство з метою унормування державно-владної діяльності з протидії дезінформації.

Цифрова епоха характеризується наявністю різних підходів до регулювання нових видів інформаційних відносин. Як зазначив Орін Керр, «закон, створений для одного світу, може мати зовсім інший вплив, якщо його застосувати до фактів іншої епохи» [16]. У процесі розроблення законодавчої бази для протидії дезінформації корисним буде проведення аналізу законодавства та практики, які застосовуються при вирішенні цього питання в інших країнах.

Насамперед слід розглянути Кодекс практики щодо дезінформації у ЄС (далі – Кодекс). У Кодексі підписанти визнали «основне право на свободу вираження поглядів і відкритий інтернет, а також тонкий баланс, якого повинні дотримуватися при впровадженні будь-яких заходів щодо об-

меження поширення та впливу повідомлень (контенту)» [17]. Особлива увага в Кодексі приділяється «прецедентному праву Суду Європейського Союзу та Європейського Суду з прав людини щодо пропорційності заходів, спрямованих на обмеження доступу до шкідливого змісту та його розповсюдження» [17]. Кодекс практики підписали онлайн-платформи Facebook, Google, а також Twitter, Mozilla, Microsoft і TikTok, рекламодавці та суб'єкти рекламної індустрії [17]. Цікаво, що згаданих вище підписантів «уряди не повинні змушувати, а також вони не зобов'язані приймати добровільну політику видаляти чи забороняти доступ до законного вмісту чи повідомлень виключно на підставі того, що вони вважаються "неправдивими"» [17]. Цей принцип передбачає врахування при розробленні правової бази для протидії дезінформації таких двох умов:

1) відсутність в урядів повноважень примушувати модерувати контент;

2) модерація вмісту не може бути виконана лише на підставі того, що повідомлення вважаються «неправдивими».

Також законодавство щодо протидії дезінформації у виборчій сфері в ЄС містить норму, відповідно до якої «виборці повинні мати можливість формувати свою думку незалежно, без насильства чи загрози насильства, примусу, спонукання чи маніпулятивного втручання будь-якого виду» [18].

У деяких державах уже запроваджено або триває процес розроблення законів про «фейкові новини» та інших ініціатив, таких як медіаграмотність. У Франції, наприклад, закон про боротьбу з поширенням дезінформації під час виборів був прийнятий у 2018 році. Законодавство надає владі повноваження видаляти фейковий контент, який розповсюджується через соціальні мережі, і блокувати сайти, які його публікують, а також забезпечувати більшу фінансову прозорість для спонсорованого контенту за три місяці до виборчого періоду. Закон містить три основні положення: 1) суддя має право діяти «пропорційно», але «будь-якими засобами», щоб зупинити поширення дезінформації перед виборами; 2) такі платформи, як Facebook, Twitter і YouTube, зобов'язані публікувати, хто і за яку ціну придбав спонсорований контент або рекламу кампанії; 3) закон надає Вищій аудіовізуальній раді – телерадіомовному регулятору – нові адміністративні права щодо нагляду за діяльністю платформ соціальних медіа [19].

У Сінгапурі закон 2019 року запровадив кримінальну відповідальність за поширення неправдивої інформації в інтернеті, що робить незаконним поширення в Сінгапурі «неправдивих заяв про факти», які ставлять під загрозу безпеку, «громадський спокій», громадську безпеку та відносини країни з іншими країнами; Закон карає людей, які публікують неправдиву інформацію, великими штрафами та навіть позбавленням волі: якщо «зловмисник» поширить неправдиву інформацію, загрожує штраф до 37 000 доларів США або п'ять років ув'язнення. Покарання збільшується

до 74 000 доларів і потенційного 10-річного тюремного терміну, якщо неправда була розповсюджена за допомогою «несправжнього облікового запису в інтернеті або бота»; таким платформам, як Facebook, загрожують штрафи в розмірі до 740 000 доларів за їхню роль у поширенні дезінформації [20].

Подібна ініціатива, спрямована на посилення кримінального покарання за кіберзлочини, зокрема й створення підроблених даних, розглядалася і в Грузії [21].

Загалом, як підсумував Пітер Рудік, існує чотири шляхи, якими країни вирішують проблему фейкових новин:

1) за відсутності законодавства, яке б чітко стосувалося об'єктивності новин, розміщених у соціальних мережах, країни застосовують відповідні положення чинних цивільних, кримінальних, адміністративних та інших законів, що регулюють засоби масової інформації, вибори та боротьбу з дифамацією (Велика Британія, Канада, Нікарагуа, Швеція та Японія);

2) прийняття нового та цілеспрямованішого законодавства, що накладає санкції на соціальні мережі, які поширюють неправдиві новини, зазвичай накладаючи штрафи та наказуючи видаляти інформацію, визнану неправдивою (Єгипет, Ізраїль, Китай, Малайзія, Німеччина, Росія та Франція; у Єгипті та Малайзії ці положення застосовуються екстериторіально);

3) залучення виборчих органів та цифрових платформ для забезпечення поінформованості електорату шляхом виявлення та блокування фейкових новин, надання ресурсів для перевірки фактів для широкої громадськості або шляхом масової публікації «справжніх» новин під час виборчого періоду та за його межами (Аргентина, Велика Британія, Китай та Малайзія);

4) інформування громадян про небезпеку фейкових новин (Кенія та Швеція) [22].

Прийняття законів про «фейкові новини» загрожує цензурою та може призвести до припинення критичних виступів, насамперед журналістів. Наприклад, у Росії, де незалежні ЗМІ фактично не функціонують, такий закон дає можливість уряду придушувати демократичні висловлювання. В автократичних країнах такі закони дозволяють прокурорам висувати звинувачення або штрафувати журналістів за публікацію інформації, яку влада визнала неправдивою або загрозливою [23]. Наприклад, Мохамед Монір, єгипетський журналіст, помер у лікарняному ізоляторі. Його заарештували за написання статті, яка критикує реакцію єгипетського уряду на пандемію, і звинуватили в поширенні неправдивих новин, зловживанні соціальними мережами та приєднанні до терористичної групи [24].

У Китаї найсуворіші закони у світі, оскільки уряд криміналізує створення чи поширення чуток, які «підривають економічний і соціальний порядок». Закон 2017 року зобов'язує платформи соціальних медіа лише цитувати та посилатися на статті новин із зареєстрованих ЗМІ. Наприкінці серпня 2018 року влада Китаю запустила додаток, який дає можливість людям повідомляти про потенційно

неправдиву інформацію, він також використовує штучний інтелект для автоматичного виявлення чуток [19].

Недемократичні підходи до протидії дезінформації, як у Росії та інших автократичних урядах, обмежують свободу слова та демократію. Ці альтернативи не можуть бути використані в Україні.

З погляду сучасних подій в Україні прийняття та застосування закону проти дезінформації може бути виправдане як надзвичайний захід проти міжнародно визнаної російської воєнної агресії в поєднанні з гібридною війною. Проте цей закон має відповідати міжнародному праву та визнаним принципам свободи думки і слова.

Висновки. Підсумовуючи викладене, зазначимо, що в системі ООН із 2004 року функціонувало декілька груп урядових експертів із вивчення питань, пов'язаних із кібероперація-ми. Однак напрацьовані рекомендації утримуватися від використання інформаційно-комунікаційних технологій, що суперечить нормам відповідальної поведінки держав, не є перешкодою для здійснення кібероперацій, зокрема дезінформаційних кампаній. Натомість Талліннський посібник 2.0 обґрунтовує можливість застосування сили у відповідь на кібероперації на підставі норм міжнародного права. Тому робимо висновок, що втручання у вибори, охорону здоров'я та інші сфери державного суверенітету за допомогою операцій із дезінформації можна тлумачити як такі, що суперечать міжнародному праву.

У міжнародно-правових документах передбачено, що для легітимізації діяльності з протидії дезінформації держава має продемонструвати: точний характер загрози; необхідність і пропорційність конкретної дії; прямий і безпосередній зв'язок між певним висловлюванням і загрозою.

За результатами аналізу Кодексу практики щодо дезінформації у ЄС рекомендується враховувати при розробленні правової бази для протидії дезінформації: відсутність в урядів повноважень примушувати платформи соціальних медіа модерувати контент; неможливість модерації змісту лише на підставі того, що повідомлення вважаються «неправдивими».

Аналіз тенденцій щодо запровадження в деяких країнах законів про «фейкові новини» засвідчує, що прийняття та застосування закону проти дезінформації в Україні може бути виправдане як надзвичайний захід проти міжнародно визнаної російської воєнної агресії, проте він (закон) має відповідати міжнародному праву, зокрема принципам свободи думки і слова.

Перспективами подальших наукових пошуків є вивчення питання взаємодії Центру протидії дезінформації з інститутами громадянського суспільства задля забезпечення інформаційної безпеки особи, суспільства і держави та розроблення рекомендацій щодо її організації.

Список використаних джерел

1. Положення про Центр протидії дезінформації, затверджене Указом Президента України від 07.05.2021 № 187/ 2021. *Офіційний вісник Президента України.* 2021. № 15. Ст. 774.

2. Preuss L. International Responsibility for Hostile Propaganda against Foreign States. *American Journal of International Law*. 1934. 28(4). P. 649–668. DOI:10.2307/ 2190753.

3. Kyle Langvardt. Regulating Online Content Moderation. *Georgetown Law Journal*. 2018. Vol. 106. Issue 5.

4. Bonnie Brennen. Making Sense of Lies, Deceptive Propaganda, and Fake News. *Journal of Media Ethics* 32. 2017. No. 3.

5. Jankowicz N. The Only Way to Defend Against Russia's Information War. *The New York Times*. Sept. 25, 2017. URL: https://mobile.nytimes.com/2017/09/25/ opinion/the-only-way-to-defend-against-russias-informationwar.html (дата звернення: 10.11.2021).

6. Steven J. Barela. Zero Shades of Grey: Russian-Ops Violate International Law. *Just Security*. Mar. 29, 2018. URL: https:// www.justsecurity.org/54340/shades-grey-russian-ops-violate-international-law (дата звернення: 11.11.2021).

7. Michael N. Schmitt. «Virtual» Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law, 19 Chi. J. Int'l L. 30. 2018.

8. Gary P. Corn. Coronavirus Disinformation and the Need for States to Shore Up International Law, Lawfare. Apr. 2, 2020. URL: https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law (дата звернення: 08.11.2021).

9. United Nations. *Charter of the United Nations*. Octob. 24, 1945. 1 UNTS XVI, available at. URL: https://www.refworld.org/ docid/3ae6b3930.html (дата звернення: 12.10.2021).

10. Developments in the field of information and telecommunications in the context of international security. URL: https:// www.un.org/disarmament/ict-security. Group of Governmental Experts. URL: https://www.un.org/disarmament/group-of-governmental-experts/www.refworld.org/ docid/3ae6b3930.html (дата звернення: 12.10.2021).

11. Open-ended working group on developments in the field of information and telecommunications in the context of international security. A/AC.290/2021/CRP.2 Conference room paper. Mar. 10, 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата звернення: 08.10.2021).

12. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2nd edition. Cambridge University Press, 2017.

13. Michael N. Schmitt. Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum, 8 *HARV. NAT'L SEC. L. J.* 239. 2017.

14. Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. URL: https://www.coe.int/en/web/ conventions/full-list/-/conventions/treaty/ 189 (дата звернення: 12.10.2021).

15. UN Human Rights Committee (HRC). *General comment no. 34, Article 19, Freedoms of opinion and expression.* Sept. 12, 2011, CCPR/C/GC/34. URL: https:// www.refworld.org/docid/4ed34b562.html (дата звернення: 11.10.2021).

16. Orin S. Kerr. Foreword: Accounting for Technological Change, 36 HARV. J.L. & PUB. POL'Y 403, 403 (2013).

17. Code of Practice on Disinformation. Signed in Brussels, Sept. 2018. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454 (дата звернення: 12.10.2021).

18. Council of Europe. *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14.* Novem. 4, 1950, ETS 5. URL: https://www.refworld.org/docid/3ae6b3b04.html (дата звернення: 12.10.2021).

19. Daniel Funke, Daniela Flamini. A guide to anti-misinformation actions around the world. URL: https://www.poynter.org/ifcn/anti-misinformation-actions/#us (дата звернення: 12.10.2021).

20. Protection from Online Falsehoods and Manipulation Act 2019 of Singapore. URL: https://sso.agc.gov.sg/Act/POFMA2019?ValidDate=20210102&ProvIds=P13- (дата звернення: 11.10.2021).

21. Parliament hears bill on stricter punishment for cyber crimes. URL: https://agenda.ge/en/news/2021/732 (дата звернення: 12.10.2021).

22. Peter Roudik. Initiatives to Counter Fake News: Comparative Summary. Apr. 2019. URL: https://www.loc.gov/law/help/fake-news/compsum.php (дата звернення: 12.10.2021) April 2019.

23. Rush to pass 'fake news' laws during Covid-19 intensifying global media freedom challenges. URL: https://ipi.media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/ (дата звернення: 12.10.2021).

24. Censorious governments are abusing «fake news» laws. URL: https://www.economist.com/international/2021/02/11/censorious-governments-are-abusing-fake-news-laws (дата звернення: 12.10.2021).

Аннотация. В статье проанализированы международно-правовые подходы и национально-правовое регулирование противодействия дезинформации, основные законодательные акты, регламентирующие решение вопроса такого противодействия в зарубежных странах. Определены условия легитимизации в государстве деятельности по противодействию дезинформации.

Обосновано, что законодательство по противодействию дезинформации в Украине должно соответствовать международному праву, в частности принципам свободы мысли и слова.

Ключевые слова: дезинформация, кибероперации, международное право, национальное право, свобода слова.

Abstract. The article analyzes international-legal approaches and national-legal regulation of counteraction to misinformation as well as key legislative acts regulating the solution of corresponding issues in foreign countries. The authors determined conditions aimed at the legitimization of activities related to countering misinformation.

The article substantiates the fact that the legislation on combating misinformation in Ukraine must comply with the international law, in particular the principles of freedom of thought and speech.

Key words: misinformation, cyber operations, international law, national law, freedom of speech.