

**АДМІНІСТРАТИВНЕ ПРАВО І АДМІНІСТРАТИВНИЙ ПРОЦЕС,  
ІНФОРМАЦІЙНЕ ПРАВО**

**ДЯКОВСЬКИЙ О. С.,**  
кандидат юридичних наук,  
старший викладач кафедри  
інформаційного, господарського  
та адміністративного права  
(*Національний технічний університет  
України «Київський політехнічний  
інститут імені Ігоря Сікорського»*)

УДК 347.998.85  
DOI <https://doi.org/10.32842/2078-3736/2024.4.28>

**ПРАВОВІ ТА ІНСТИТУЦІЙНІ МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ  
У РОЗВИНУТИХ КРАЇНАХ СВІТУ**

У статті розглянуто правові та інституційні механізми протидії дезінформації, також наголошено, що розвинуті країни активно розробляють і впроваджують різноманітні правові та інституційні механізми для протидії цьому явищу. Робота досліджує механізми, аналізуючи їх ефективність, переваги та недоліки, а також надає рекомендації щодо їхнього покращення. Основні положення статті зосереджуються на правових та організаційних (публічно-управлінських) механізмах протидії дезінформації, законодавстві про медіа. Розглядаються закони, які регулюють діяльність медіа-компаній та встановлюють стандарти для публікації інформації.

Окрема увага зосереджена на інституційних механізмах протидії дезінформації. Опрацьовано механізми координації між країнами та міжнародними організаціями для ефективної протидії дезінформаційним кампаніям. Наголошено на ефективності співпраці з приватним сектором. Вивчається взаємодія урядів з технологічними компаніями та соціальними мережами, такими як Facebook, у контексті виявлення та видалення дезінформаційного контенту. Оцінюється важливість програм, спрямованих на підвищення рівня медіаграмотності населення, що дозволяє громадянам краще розпізнавати фейкові новини. Розглядаються державні та недержавні інформаційні кампанії, які підвищують обізнаність громадськості про загрози дезінформації. Аналізується необхідність забезпечення прозорості дій урядів і приватних компаній у процесі протидії дезінформації, щоб уникнути зловживань владою. У висновках зазначено, що ефективна протидія дезінформації можлива лише за умови комплексного підходу, який поєднує правові, інституційні, освітні та етичні механізми. Наголошується, що при вирішенні судових спорів у даній сфері має місце оціночні судження котрі суд повинен враховувати та досліджувати їх наявність при прийнятті судового рішення, якщо даний факт має місце або сторона спору посиляється на дані обставини як на підставу своєї позиції. Надаються рекомендації щодо вдосконалення існуючих механізмів та наголошують на важливості міжнародного співробітництва у цій сфері.

**Ключові слова:** цифрові технології, дезінформація, законодавчі ініціативи, співробітництво, персональні дані, ідентифікація, дані про особу, протидія дезінформації, механізми координації, інституція, чутливі дані.



**Dyakovsky O. S. Legal and institutional mechanisms for countering disinformation in developed countries**

The article examines the legal and institutional mechanisms for countering disinformation, and also emphasizes that developed countries are actively developing and implementing various legal and institutional mechanisms to counter this phenomenon. The work examines the mechanisms, analyzing their effectiveness, advantages and disadvantages, and provides recommendations for their improvement. The main provisions of the article focus on legal and organizational (public-management) mechanisms for countering disinformation, media legislation. Laws that regulate the activities of media companies and establish standards for the publication of information are considered.

Special attention is paid to institutional mechanisms for countering disinformation. The mechanisms of coordination between countries and international organizations for effective counteraction to disinformation campaigns are elaborated. The effectiveness of cooperation with the private sector is emphasized. The interaction of governments with technology companies and social networks, such as Facebook, in the context of identifying and removing disinformation content is studied. The importance of programs aimed at increasing the level of media literacy of the population, which allows citizens to better recognize fake news, is assessed. The article also examines governmental and non-governmental information campaigns that raise public awareness of the threats of disinformation. The author analyzes the need to ensure transparency in the actions of governments and private companies in the process of countering disinformation in order to avoid abuse of power. The authors conclude that effective countering disinformation is possible only with a comprehensive approach that combines legal, institutional, educational, and ethical mechanisms.

It is emphasized that when resolving legal disputes in this area, there are evaluative judgments that the court must take into account and investigate their presence when making a court decision, if this fact exists or the party to the dispute refers to these circumstances as the basis of its position. Recommendations for improving existing mechanisms are provided and the importance of international cooperation in this area is emphasized.

**Key words:** *digital technologies, disinformation, legislative initiatives, cooperation, personal data, identification, personal data, countering disinformation, coordination mechanisms, institution, sensitive data.*

**Вступ.** Необмежений масив інформації щоденно отримає як окремі громадян так і суспільство в цілому. Збільшення обігу інформації включає в собі дані котрі є персональними та можуть впливати на ідентифікацію особи чи певної події. Значний розвиток соціальних мереж та медіа також зумовлює збільшення обсягу інформації, що її просто фізично неможливо перевірити окремій людині. Інформаційний простір, підсилений соціальними мережами, починає домінувати над простором фізичним, оскільки будь-яке інформаційне повідомлення вибудовано під ту чи іншу віртуальну позицію і тим самим поширює її, навіть не акцентуючи на цьому увагу.

Обґрунтованою є потреба у пошуку сучасних рішень, які стосуються розвитку правових та інституційних механізмів протидії дезінформації, в тому числі базуючись на кращих практиках іноземних держав. На зазначеному у своїх дослідженнях наголошують такі вчені як Бондар В. Т. [1], Звоздецька О. [2], Маляренко В. І. [4].

**Постановка завдання.** Метою статті є аналіз взаємодії між різними правовими та інституційними механізмами у протидії дезінформації у розвинутих країнах світу, зокрема, виявлення законодавчих ініціатив, регуляторних органів та громадських інституцій, що співпрацюють у забезпеченні інформаційної безпеки та сприяють підтримці демократичних цінностей.



**Результати дослідження.** Варто зазначити, що свобода слова, декларована ст. 34 Конституції України [3], за своїм змістом слугує вищою природною нормативністю, але в той же час являється предметом цілої низки маніпуляцій, які можуть приховувати дезінформаційні впливи. Вітчизняна судова практика в частині притягнення до відповідальності за поширення неправдивих відомостей, яскраво показує, що окрім повідомлень про факти та осіб, що є підставою для притягнення до відповідальності, ще одним чинником є оціночні судження котрі повинні досліджуватися судом при прийнятті судового рішення.

Разом з тим, в умовах воєнного стану, лише наявність дієвих (подекуди жорстких) обмежень, здатне поліпшити ситуацію, підвищити рівень правосвідомості окремих громадян суспільства. Як влучно зауважує Анка Фельдгузен, Посол ФРН в Україні: «Межі, з одного боку, між легітимним плюралізмом думок, включно із суперечливими, а з іншого – зі шкідливою дезінформацією, не завжди чіткі і зрозумілі, на жаль. Крім того, ми маємо визнати, що вони дуже залежать від нашого власного погляду на світ. І ми також маємо завжди пам'ятати, що будь-які правила, навіть якщо ми створюємо їх із найкращими намірами, можуть стати предметом зловживань або бути використаними проти нас самих. Україна звісно є в авангарді гібридних інформаційних кампаній та дезінформації, саме тому ця тема обговорюється тут багато років і викликає багато суперечок» [5].

Дезінформація існує в усіх інформаційних екосистемах світу, та може містити в своїй будові персональні дані в тому числі чутливі дані третіх осіб котрі не надавали згоду на їх розголошення. З цієї причини необхідний підхід, заснований на участі всього суспільства, який заохочував би представників уряду, громадянського суспільства та промисловості до спільної роботи з протидії дезінформації й посилення реакції суспільства. Механізм протидії дезінформації варто ідентифікувати як комплекс заходів, стратегій та інструментів, спрямованих на виявлення, запобігання та нейтралізацію дезінформації, а також на підвищення обізнаності і стійкості суспільства до неправдивої інформації (механізми включають технологічні, освітні, правові та організаційні аспекти).

Переважно в усіх розвинених юрисдикціях передбачено кримінальну або адміністративну відповідальність за поширення недостовірних відомостей, що спричиняють негативні наслідки для суспільства. Так, у 2019 році Парламентом Сінгапуру було прийнято Закон «Про захист від недостовірної інформації та маніпулювання в мережі Інтернет», який передбачає відповідальність за розповсюдження неправдивої інформації – істотно більш сувору, ніж передбачена національним законодавством. Характерно, що даний нормативно-правовий акт закріплює дезінформацію як спосіб поширення стосовно одного або більше суб'єктів на території Сінгапуру або за його межами інформації в мережі Інтернет особою, яка знала або повинна була знати, що відповідна інформація є неправдивою і що її поширення, імовірно, може: понести шкоду безпеці Сінгапуру або будь-якій його частині, здоров'ю населення, громадській безпеці та спокою, державній системі фінансів, громадським організаціям [13]. Таке, цілком обширне формулювання, досить змістовно розкриває об'єкти посягання, що захищаються законодавством. Зокрема для осіб, які поширюють неправдивий контент в мережі Інтернет, застосовується відповідальність у вигляді позбавлення волі на строк до 5 років або штраф, який не перевищує \$50 000. Якщо мова йде лише про юридичних осіб, то в цьому випадку максимальна межа штрафу сягає \$500 000.

Водночас відповідальність за поширення завідомо недостовірної інформації існує і в правопорядках, які заведено вважати максимально гуманістичними. Так, у Норвегії передбачено кримінальну відповідальність щодо осіб, які займаються розповсюдженням неправдивих відомостей (ст. 187 Кримінального кодексу Норвегії). Як покарання за поширення дезінформації, в тому числі неправдивих прохань про допомогу, необгрунтоване застосування сигналу лиха або інших аналогічних дій, навмисно або у формі грубої необережності, що призвели до приїзду поліції, пожежників, служб швидкої допомоги або збройних сил, втручання рятувальників або призвели до залякування великої кількості людей, передбачено відповідальність у вигляді штрафу або позбавлення волі на строк до 6 місяців [11]. При цьому, аналогічне покарання передбачається також щодо будь-якої особи, яка надає



неправдиву інформацію, здатну викликати побоювання за чиєсь життя, здоров'я або порушення громадського спокою і порядку.

Досить динамічно розвивається як інституційне, так і нормативно-правове забезпечення щодо протидії дезінформації у Німеччині. Зокрема, боротьбу із поширенням неправомірної інформації розпочали із регулювання ключових засад у соціальних мережах. Із зазначеного питання, ще у 2015 році створено робочу групу, котра опікувалась розробкою профільного закону. Характерно, що таким діям передували цілком правові намагання німецької влади угодити із керівництвом таких світових гігантів як Facebook, Google і Twitter питання стосовно видалення шкідливого контенту. Як наслідок, закінчення переговорів не задовольнило представників ФРН, через що вже від 01.10.2017 було прийнято Закон «Про регулювання соціальних мереж» [10]. Із 2018 року в країні діє Кодекс практик протидії дезінформації в мережі Інтернет. Як окремий документ, наділений нормативно-правовою силою, він по більшій мірі акумулює перелік зобов'язань, котрі цифрові платформи та асоціації, які власне представляють інтереси рекламодавців та рекламну галузь, добровільно застосовують для боротьби з дезінформацією та пропагандою [4, с. 24].

Успішна модель побудови роботи серед органів виконавчої влади, які опікуються питаннями боротьби із дезінформацією прослідковується на прикладі органів публічної влади Польщі. Першочергово, згадаємо про Департамент соціальних комунікацій Міністерства внутрішніх справ і адміністрації Республіки Польща, до повноважень якого віднесено, зокрема, виявлення дезінформації у соціальних мережах. Окрім зазначеного, у цій ланці також задіяні:

- Канцелярія голови Ради Міністрів Польщі,
- Міністерство оборони Республіки Польща,
- Міністерство закордонних справ,
- Науково-дослідницький інститут «Наукова і академічна комп'ютерна мережа»

[1, с. 5].

Якщо існують підозри стосовно підривної діяльності розвідувальних іноземних служб, то в такому випадку до аналізу відповідних матеріалів та проведення розслідування залучаються фахівці Департаменту національної безпеки Канцелярії спільно з Агентством Внутрішньої Безпеки Республіки Польща. Цілком виправданим, на наш погляд, стало консолідоване рішення Великобританії та Польщі спільно створити підрозділ, котрий займатиметься виключно виявленням та протидією фейкам країни-окупанта нашої держави. В подальшому, він став амбасадором проведення консультацій протидії поширення неправдивих відомостей в медіа середовищі.

В цілому, модель державного управління в розрізі протидії дезінформації у Польщі, подібно вітчизняній практиці, розподілена за сферами компетенції: функціональний напрям безпеки дотримання соціальних комунікацій забезпечується всіма органами державної влади, окрім Агентства Внутрішньої Безпеки Республіки Польща, на яке покладено функцію стратегічних комунікацій. Систематично оновлюється і законодавство у даному напрямку. Так, 31.03.2023 року було прийнято спільну Постанову про боротьбу із дезінформацією сенатськими комісіями Культури і засобів інформації; Права людини, верховенства права і петицій; Закордонних справ та ЄС. Ключовим леймотивом крізь зміст даного документу проходить у наступному: обґрунтованою є потреба у розробці міжгалузевої стратегії протидії дезінформації, підвищення рівня освіченості населення в даному питанні, імплементації норм ЄС у сфері цифрових послуг. Щодо вдосконалення правового поля, депутатами Сейму внесено проєкт змін до § 1 ст. 130 Кримінального Кодексу Республіки Польща (1997 р.) у частині строку позбавлення волі на не менше 10 років або довічно (нині 5 років або довічно) за поширення дезінформації, діяльність на користь спеціальних служб іноземних держав [12].

Найбільшу релевантність щодо політики з протидії дезінформації має при цьому саме закон про цифрові послуги, оскільки саме у ньому відображено нові зобов'язання з протидії незаконному контенту, заборони на певні види цільової реклами, доступу дослідників до



ключових даних та створення структур наглядю. Водночас закон про цифрові ринки відображає більшою мірою положення щодо конкуренції в цифровому просторі. Побудова нових зобов'язань за принципом спільного управління стала способом стримування платформ у їхній спроможності не тільки впливати на цифровий простір, а й надмірно експлуатувати дані користувачів у комерційних цілях.

Варто зазначити, що нові закони ухвалено не лише в Польщі, але в цілому ЄС загалом, на тлі загального масштабування політики співдружності у цифровій сфері загалом і в царині фейкового контенту зокрема. Зростання кількості згадок «дезінформації» в різних стратегічних документах [4-7] вказувало на додаткову сек'юритизацію загрози, що дало змогу перейти від консультативного та добровільного реагування до законодавчої й наглядової ролі інститутів ЄС. При цьому, процес включення дезінформації в регулятивне поле відбувся через економічну площину, оскільки всі попередні дії були складовою частиною діяльності з розвитку єдиного цифрового ринку.

Окремо слід згадати унікальну особливість протидії фейкам в Аргентині. У цій країні немає окремого закону, спрямованого на боротьбу з дезінформацією, однак це єдина держава у світі, де є спеціальні «спостерігачі» за недостовірною інформацією. Вони з'явилися 2020 року, коли Федеральне управління із захисту аудіовізуальних комунікацій створило новий департамент «Nodio» назвавши його «Обсерваторія зі спостереження за дезінформацією та символічною владою в цифрових медіа та платформах». Метою цієї організації було названо «захист громадян від неправдивих, зловмисних і оманливих новин». Рішення про її створення критикували різні активісти, журналісти та громадські діячі, включно з місцевими депутатами, за можливий вплив цензури на засоби масової інформації доти, доки не було офіційно роз'яснено, що «Обсерваторія» не переймає на себе каральну функцію, а виконує суто аналітичну.

Фактично, в Аргентині створили першу відому у світі самостійну державну офіційну організацію, що займається перевіркою достовірності заявленої інформації («фактчек») і роботою над медіаграмотністю населення, яка не виконує каральних функцій. Раніше подібні організації були тільки цивільними або виключно фінансово спонсорованими державами.

На основі вищевказаному можна узагальнити, що ключовою проблемою в боротьбі з дезінформацією є неможливість провести чітку межу між фактами і вигадкою та встановити явний намір заподіяти шкоду. Ненавмисні помилки або певні форми вираження думки чи переконань, а також сатиру і пародію нелегко охопити в рамках бінарного аналізу фактів або вигадки. Більше того, дезінформація призначена для заподіяння шкоди, часом поширюється в Інтернеті третіми сторонами, які не мають подібного наміру (що класифікується як ненавмисне поширення неправдивої інформації). З метою забезпечення свободи слова, плюралістичного характеру дискусій і підвищення соціальної стресостійкості, Україна має вжити низку дієвих заходів, серед яких виділяємо:

- розвиток механізмів співробітництва з країнами ЄС, яким вдається успішно нівелювати дезінформаційні кампанії;
- зміцнення взаємодії з міжнародними партнерами, в т.ч. шляхом проведення нарад, семінарів, воркшопів в першу чергу для працівників органів публічної влади та представників засобів масової інформації;
- розширення підтримки громадянського суспільства, незалежних медіа та журналістів, а також посилення моніторингу порушень свободи засобів масової інформації;
- взаємодія з онлайн-платформами з метою захисту споживачів, включно з підвищенням прозорості їхньої роботи, нарощування співпраці з «фактчекерами», протидія рекламі, яка вводить в оману;
- підвищення інформаційної грамотності населення, включно з критичним мисленням і цифровими навичками, через проекти з розвитку медіаграмотності та підтримку організацій громадянського суспільства.

Різнобічний підхід до боротьби з дезінформацією обумовлений її поширеністю у багатьох сферах суспільної діяльності. Відповідно, за рахунок грамотного підходу до



вибудовування публічно-управлінських структур, до сфери відповідальності яких буде належати усунення даного суспільно-негативного феномену, а також в силу консолідації зусиль всіх суб'єктів, прямо чи опосередковано задіяних в усуненні дезінформаційних впливів, можливо щонайбільше мінімізувати ризики розповсюдження даних, котрі негативно впливають на суспільство.

**Висновки.** Отже, за результатами проведеного дослідження можемо узагальнити, що в прогресивних країнах світу сформувалися дві практики управління, пов'язані з дезінформацією. Інституційні рамки, спрямовані на багатостороннє регулювання, створені ще до закону про цифрові послуги, але узагальнені в ньому, зберегли свою актуальність. Їхнім основним предметом регулювання залишився посередник інформаційного впливу у вигляді цифрових платформ. Зберегли свою значимість і дії, націлені на об'єкт інформаційного впливу. Однак зміна геополітичної ситуації змусила, зокрема, країни ЄС повернутися до риторики періоду початкового формування політики, пов'язаної з активним стратегічним наративом.

Крім такого публічно-управлінського підходу до боротьби суспільства з дезінформацією, важливим елементом для ефективної протидії є співпраця між державними органами та органами місцевого самоврядування, а також у рамках ЄС і з його державами-партнерами. Крім того, уряди країн ЄС постійно обмінюються інформацією з операторами соціальних мереж з метою зміцнення прозорих правил поведінки у соціальних мережах і забезпечення їх послідовного дотримання всіма сторонами. Україна поступово переймає досвід провідних держав, але в умовах повномасштабної війни ситуація вимагає більш жорстких та рішучих змін. Перспективи подальших наукових пошуків вбачаємо у аналізі та адміністративно-правовій оцінці реалізованих в період повномасштабного вторгнення росії на територію України заходів із протидії дезінформації.

#### Список використаних джерел:

1. Бондар В. Т. Механізми державного управління республіки Польща з протидії дезінформації. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. Вип. 10. 2023. <https://doi.org/10.54929/2786-5746-2023-10-02-01>
2. Звоздецька О. Медіафорум: аналітика, прогнози, інформаційний менеджмент: зб. наук. праць. Чернівці: Чернівецький нац. ун-т, Том 10. 2022. С. 107–122.
3. Конституція України. *Відомості Верховної Ради України* (ВВР). 1996. № 30. с. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
4. Маляренко В. І. Крайні практики зарубіжного досвіду боротьби з фейками та дезінформацією. Інформація і право. Вип. № 3(38). 2021. С. 21–27.
5. Протидія дезінформації: європейські підходи та стандарти: новини та заходи. 2021. URL: <https://www.coe.int/uk/web/kyiv/-/responding-to-disinformation-european-practices-and-standards>
6. European Commission. Joint Communication The EU's Cybersecurity Strategy for the Digital Decade Join/2020/18 Final. 2020. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018>
7. European Commission. Digital Education Action Plan 2021–2027 Resetting education and training for the digital age COM/2020/624 final. 2020. URL: <https://education.ec.europa.eu/focus-topics/digitaleducation/action-plan>
8. European Commission. Communication On the EU Security Union Strategy COM/2020/605 Final. 2020. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605>
9. European Commission. Communication Shaping Europe's Digital Future COM/2020/67 Final. 2020. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067>
10. *Netzwerkdurchsetzungsgesetz*. URL : [https:// de.wikipedia.org/wiki/Netzwerkdurchsetzungsgesetz](https://de.wikipedia.org/wiki/Netzwerkdurchsetzungsgesetz)



11. Penal Code of the Kingdom of Norway (LOV-2005-05-20-28) / Lovdata. URL: [https://lovdata.no/dokument/NLE/lov/2005-05-20-28/KAPITTEL\\_2#KAPITTEL\\_2](https://lovdata.no/dokument/NLE/lov/2005-05-20-28/KAPITTEL_2#KAPITTEL_2)
12. Posłowie odpowiedzą na działania wrogich służb wywiadowczych? [Members of Parliament to respond to hostile intelligence services?]. InfoSecurity, 24. (2023, 7 Lipca). URL: <https://infosecurity24.pl/legislacja/poslowie-odpowiedza-na-dzialania-wrogich-sluzb-ywiadowczych>
13. Protection from Online Falsehoods and Manipulation Act. Singapore Statutes Online. 02.10.2019. URL: <https://sso.agc.gov.sg/Act/POFMA2019>

