

Міністерство освіти і науки України
Національний університет “Києво-Могилянська академія”
факультет правничих наук
кафедра приватного права

Магістерська робота
освітній ступінь – магістр

на тему: ***“Вибори в епоху цифрових платформ: правові механізми
протидії маніпуляціям і дезінформації” / Elections in the age of digital
platforms: legal mechanisms to counter manipulation and disinformation***

Виконав:

Студент 2 року навчання магістерської
програми 081 “Право”

Бойко Денис Володимирович

dv.boiko@ukma.edu.ua

Керівник магістерської роботи:

Смирнова Тетяна Сергіївна

доцент кафедри приватного права

кандидат юридичних наук

Рецензент: _____

Магістерська робота захищена

з оцінкою: _____

Секретар ЕК _____

« ____ » _____ 2026 р.

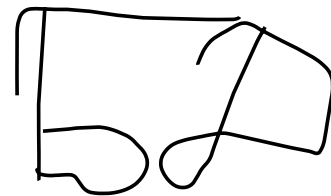
**Київ
2026**

Декларація академічної доброчесності

Я, Бойко Денис Володимирович, студент 2 року навчання магістерської програми за спеціальністю “Право” факультету правничих наук НаУКМА підтверджую наступне:

аписана мною магістерська робота на тему “Вибори в епоху цифрових платформ: правові механізми протидії маніпуляціям і дезінформації” / доброчесності та не містить порушень, передбачених п. 3.1. Положення про академічну доброчесність здобувачів освіти у НаУКМА, зі змістом якого я ознайомлений;

адана мною для перевірки електронна версія роботи є ідентичною її друкованій версії.



Бойко Д. В.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	5
ВСТУП.....	7
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ВИБОРЧОГО ПРОЦЕСУ В ЦИФРОВУ ЕПОХУ.....	11
1.1. Трансформація маніпуляцій у виборчому процесі в цифрову епоху.....	11
Роль цифрових платформ як суб'єктів впливу на виборчий процес та їхня відповідальність.....	17
Практика Європейського суду з прав людини у справах, пов'язаних з дезінформацією.....	20
РОЗДІЛ 2. РЕГУЛЯТОРНА МОДЕЛЬ ЄС ЩОДО ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ПІД ЧАС ВИБОРІВ.....	25
2.1. Еволюція регулювання дезінформації в ЄС: від Кодексу поведінки до Digital	
2.2. Роль європейських інституцій у протидії дезінформаційним кампаніям.....	36
РОЗДІЛ 3. ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРАВОВИХ МЕХАНІЗМІВ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯЦІЯМ В ОКРЕМИХ КРАЇНАХ.....	43
Правове регулювання Франції у сфері протидії дезінформації та інформаційним маніпуляціям.....	43
Правове регулювання Німеччини у сфері протидії дезінформації та інформаційним маніпуляціям.....	45
Правове регулювання Великої Британії у сфері протидії дезінформації та інформаційним маніпуляціям.....	48
Досвід Нідерландів у протидії дезінформації та інформаційним маніпуляціям	49
Досвід Литви та Латвії у протидії дезінформації та інформаційним маніпуляціям.....	52
Правове регулювання Іспанії у сфері протидії дезінформації та інформаційним маніпуляціям.....	53
Правове регулювання Сінгапуру у сфері протидії дезінформації та інформаційним маніпуляціям.....	54

РОЗДІЛ 4. ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ У ВИБОРЧОМУ ПРОЦЕСІ УКРАЇНИ: СТАН ТА НАПРЯМИ ВДОСКОНАЛЕННЯ.....	58
1. Стан українського законодавства: аналіз Виборчого кодексу та Закону України “Про медіа” щодо регулювання агітації в інтернеті, протидії дезінформації та інформаційним маніпуляціям.....	58
4.2. Інституційні механізми протидії дезінформації в Україні.....	62
Напрями вдосконалення правового регулювання протидії дезінформації у виборчому процесі.....	64
ВИСНОВКИ.....	71
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	74

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI Act - Artificial Intelligence Act - Регламент ЄС 2024/1689 про штучний інтелект)

AI Office - Європейський офіс з питань штучного інтелекту

Arcom - Autorité de régulation de la communication audiovisuelle et numérique -

Орган регулювання аудіовізуальної та цифрової комунікації, Франція

AVMSD - Audiovisual Media Services Directive - Директива про аудіовізуальні медіапослуги

CNMC - Comisión Nacional de los Mercados y la Competencia - Національна комісія з ринків і конкуренції, Іспанія

DMA - Digital Markets Act - Регламент ЄС 2022/1925 про цифрові ринки

DSA - Digital Services Act Регламент ЄС 2022/2065 про цифрові послуги

EDMO - European Digital Media Observatory - Європейська обсерваторія цифрових медіа

EEAS - European External Action Service - Європейська служба зовнішньополітичної діяльності

ERGA - European Regulators Group for Audiovisual Media Services - Європейська група регуляторів аудіовізуальних медіапослуг

ESTF - East StratCom Task Force - Оперативна робоча група зі стратегічних комунікацій “Схід”

EUISS - European Union Institute for Security Studies - Інститут досліджень безпеки ЄС

GDPR - General Data Protection Regulation - Загальний регламент захисту даних

IDEA - International Institute for Democracy and Electoral Assistance - Міжнародний інститут демократії та сприяння виборам

IFES - International Foundation for Electoral Systems - Міжнародна фундація виборчих систем

LLM - Large Language Model - велика мовна модель

NetzDG - Netzwerkdurchsetzungsgesetz - Закон про вдосконалення правозастосування в соціальних мережах, Німеччина

OFCOM - Office of Communications - Управління комунікацій, Велика Британія
OSA - Online Safety Act 2023 - Закон про онлайн-безпеку, Велика Британія
POFMA - Protection from Online Falsehoods and Manipulation Act 2019 - Закон про захист від онлайн-неправдивостей та маніпуляцій, Сінгапур
RAS - Rapid Alert System - Система швидкого сповіщення
RSF - Reporters Without Borders - Репортери без кордонів
StGB - Strafgesetzbuch - Кримінальний кодекс Німеччини
USAID - United States Agency for International Development - Агентство США з міжнародного розвитку
VLOP - Very Large Online Platform дуже велика онлайн-платформа за DSA

ГО - громадська організація
ЄС - Європейський Союз
ЄСПЛ - Європейський суд з прав людини
ЗМІ - засоби масової інформації
НУО - неурядова організація
ООН - Організація Об'єднаних Націй
РФ - Російська Федерація
США - Сполучені Штати Америки
ЦВК - Центральна виборча комісія
ШІ - штучний інтелект

ВСТУП

Актуальність теми. Зміна суспільно-політичних процесів внаслідок цифровізації суттєво змінила архітектуру сучасних виборчих кампаній. Виборчий процес, який традиційно вважався і вважається фундаментом демократичного устрою країн, сьогодні стикається з викликами розвитку технологій та швидкості розповсюдження інформації. Цифрові платформи, зокрема соціальні мережі, месенджери, пошукові системи, перетворилися з інструментів вільної комунікації на потужні важелі впливу, здатні не лише формувати громадську думку, а й системно впливати на волевиявлення громадян.

Проблема маніпуляцій та дезінформації в цифровому просторі набула критичного значення після низки виборчих циклів у провідних демократіях світу, де було зафіксовано використання мікротаргетингу на основі зібраної інформації, поширення фейкових новин за допомогою бот-мереж та застосування технологій штучного інтелекту, зокрема діпфейків. Прикладами використання цифрових технологій з метою втручання у виборчі процеси та впливу на громадську думку є зокрема вибори президента Сполучених Штатів Америки у 2016 році, референдум щодо виходу Британії зі складу Європейського союзу у 2016 році, вибори до Європейського парламенту у 2019 та 2024 роках, вибори президента Румунії у 2025 році тощо. Для України важливість наявності методів та інструментів протидії дезінформації та маніпуляціям складно переоцінити: в умовах відкритої збройної агресії з боку РФ, коли дезінформаційні операції спрямовані на підрив довіри до державних інституцій та на делегітимізацію виборчого процесу як такого, а також на можливий вплив РФ на виборчі процеси всередині країни.

Наочним прикладом втручання у виборчі процеси шляхом поширення дезінформації є вибори президента Румунії 24 листопада 2024 року. Проте Конституційний Суд Румунії своїм рішенням №32 від 6 грудня 2024 року скасував результати виборів, вказавши на необхідність розпочати виборчий процес спочатку. Суд аргументував це тим, що Уряд не вжив достатньо заходів задля протистояння ризикам пов'язаним з організованими кампаніями з поширення

дезінформації щодо виборчого процесу, а також можливого використання маніпуляції алгоритмами платформ спільного доступу до інформації, задля надання певним кандидатам несправедливих переваг, що суперечило принципам виборчого законодавства [1].

Незважаючи на запровадження дії воєнного стану в Україні, що унеможливило проведення виборів, питання проведення легітимних виборів з урахуванням викликів спричинених розвитком цифрових технологій та протидії маніпуляціям та дезінформації безперечно є актуальним для майбутніх суспільно-правових відносин в Україні. Це питання набуває особливої актуальності, враховуючи досвід виборчих процесів в інших країнах за останні 10 років.

Дослідження останніх років переконливо демонструють, що виборчі кампанії стали одним із ключових моментів для активізації дезінформаційних операцій. Як зазначають А. Касеро-Ріполлес, Л. Алонсо-Муньос та Д. Морет-Солер, хоча кількісно фальшивої інформації під час виборів може бути менше, ніж у звичайний період, вона має тенденцію до більш широкого поширення і, відповідно, більшого впливу на громадськість [2, с. 3]. Наслідки виборчої дезінформації переважно асоціюються з негативними ефектами для демократії: у попередніх кампаніях, зокрема виборах до Європейського парламенту 2019 року, дезінформація використовувалася для дестабілізації ЄС, а під час виборів у Кенії 2017 року для підриву довіри до політичної та виборчої системи та посилення поляризації [3, с. 31-49]. У цьому контексті дезінформація спрямована на делегітимізацію та зниження довіри до демократичних інституцій та процесів, а також на штучне та навмисне зміщення суспільного сприйняття, впливаючи на рішення виборців [2, с. 3].

Дослідження також показали, що контент, створений за допомогою ШІ, мав майже незначну присутність на виборах до Європарламенту 2024 року і становив лише 1,1% від загального обсягу дезінформації [2, с. 9]. При цьому 59,4% дезінформації становив повністю фальшивий контент, 23,4% - контент без належного контексту, 5,4% - частково фальшивий контент [2, с. 9]. Цей результат контрастує з досвідом окремих національних виборів, де використання створеної

dezінформації на основі штучного інтелекту було значно більш помітним. Попри це зважаючи на темпи розвитку ШІ технологій, цілком впевнено можна стверджувати про їх подальше застосування з метою вплинути на виборчі процеси та результати виборів.

Найбільш ваговою є проблема правового регулювання цифрових технологій, яке не завжди встигає за їх розвитком. Традиційні механізми виборчого права, розраховані на контроль над друкованими медіа, радіомовленням та телебаченням, виявляються малоефективними проти алгоритмічних маніпуляцій та транскордонного впливу технологічних гігантів. Крім цього виникає дилема пропорційного регулювання технологій, коли з одного боку технологія знаходиться на початковому етапі розвитку і надмірне регулювання може звести її нанівець, а з іншого боку у випадку динамічного росту технології правове регулювання не буде встигати за її розвитком і будь-які спроби “наздогнати” його будуть запізнілими через повільний процес регулювання. Це зумовлює необхідність перегляду концепції юридичної відповідальності за дезінформацію та інформаційними маніпуляціями, розробки нових стандартів прозорості політичної реклами та впровадження ефективних інструментів захисту громадськості від дезінформаційних атак. Попри це виникає питання балансу права людини на свободу вираження поглядів, передбаченого Європейською конвенцією прав людини, та публічним інтересом щодо захисту демократичного та відкритого виборчого процесу.

Мета дослідження полягає у комплексному теоретико-правовому аналізі викликів, які постають перед виборчим процесом у цифрову епоху, та розробці науково обґрунтованих рекомендацій щодо вдосконалення правових механізмів протидії маніпуляціям, дезінформації. Магістерська робота інтегрована у контекст досліджень щодо адаптації українського законодавства до стандартів ЄС, зокрема, Digital Services Act та AI Act, та реалізації стратегій інформаційної безпеки держави.

Для досягнення поставленої мети визначено такі завдання:

- дослідити еволюцію виборчих технологій у контексті розвитку цифрових платформ;
- визначити правову природу понять “дезінформація”, “маніпуляція” та “мікротаргетинг” у виборчому праві;
- проаналізувати міжнародний досвід, зокрема країн ЄС, Великої Британії та інших країн, щодо регулювання діяльності цифрових платформ під час виборчих процесів;
- оцінити ефективність чинного законодавства України у сфері захисту виборчого процесу від гібридних загроз;
- розробити пропозиції щодо впровадження алгоритмічної прозорості та механізмів швидкого реагування на дезінформаційні кампанії, спрямовані на викривлення громадської думки щодо окремих політичних питань.

Об’єктом дослідження є суспільні відносини, що виникають у процесі організації та проведення виборів в умовах функціонування глобальних цифрових платформ.

Предметом дослідження є правові норми, наукова література, судова практика та регуляторні механізми, спрямовані на запобігання маніпуляціям та дезінформації у цифровому середовищі під час виборчого процесу.

Методи дослідження. Для досягнення мети використано сукупність загальнонаукових та спеціальних методів:

- *діалектичний метод* - для вивчення розвитку інформаційних технологій у взаємозв’язку з демократичними процедурами;
- *порівняльно-правовий метод* - для аналізу моделей регулювання контенту в різних юрисдикціях;
- *системно-структурний метод* - для визначення ролі цифрових платформ як нових суб’єктів впливу на виборче право;
- *метод моделювання* - для розробки перспективних правових інструментів протидії маніпуляціям.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ВИБОРЧОГО ПРОЦЕСУ В ЦИФРОВУ ЕПОХУ

1.1. Трансформація маніпуляцій у виборчому процесі в цифрову епоху

Політична маніпуляція та дезінформація не є новими явищами для виборчого права та виборчого процесу, проте внаслідок цифрової трансформації вони зазнали значних якісних та кількісних змін. Традиційна модель політичної комунікації, що базувалася на вертикальній ієрархії “держава/партія - медіа - виборець”, була зміненена горизонтальною, децентралізованою екосистемою цифрових платформ. Цей перехід позначив еволюцію від класичної пропаганди до складних форм маніпуляції та дезінформації, що використовують алгоритмічні переваги соціальних мереж.

Пропаганда, яка панувала протягом 20 століття, була характерна своєю централізованістю, масовістю та відносно простотою ідентифікації джерела впливу. Вона апелювала до широких соціальних верств через телебачення, радіо та пресу, використовуючи переважно емоційне навіювання та цензуру. Юридичні механізми протидії такій пропаганді традиційно зосереджувалися на регулюванні діяльності ліцензованих медіа та встановленні відповідальності за пряму агітацію.

Натомість сучасна дезінформація в епоху цифрових платформ, хоча і зберегла основні ознаки пропаганди 20 століття, зокрема в зверненні до емоцій і страхів людей, проте тепер полягає не лише в неправдивих новинах, або так званих fake news, а в системному процесі викривлення інформаційного простору. У правовому дискурсі Європейського союзу, зокрема у Європейському плані дій щодо демократії - European Democracy Action Plan від 3 грудня 2020 року [4], Європейська Комісія який класифікує викривлення інформації за кількома типами:

1. місінформація (misinformation) - помилковий або оманливий контент, який поширюється без шкідливого наміру, хоча наслідки все одно можуть бути шкідливими;
2. дезінформація (disinformation) - свідоме створення та поширення неправдивого контенту з метою маніпуляції та дестабілізації;

Ключовою відмінністю сучасної цифрової маніпуляції є її спрямованість або таргетованість: якщо класична пропаганда мала на меті охопити якомога більші верстви населення, то цифрові маніпуляції працюють більш точково. Завдяки інструментам мікротаргетингу, політичні суб'єкти можуть створювати тисячі варіацій одного й того самого повідомлення, видозмінених під психологічний профіль, страхи та вподобання конкретного виборця. Це створює ситуацію, коли публічний дискурс ділиться на так звані “інформаційні бульбашки” (англійською echo chambers), де виборець отримує тільки ту інформацію, яка підтверджує його упередження, що робить неможливою змагальність ідей як один з основних принципів демократичних виборів.

Важливим аспектом трансформації є зміна суб'єктного складу маніпуляцій. Окрім офіційних штабів кандидатів, на сцену вийшли так звані “проксі-суб'єкти”: бот-ферми, соціально-мережеві тролі та алгоритмічні системи. Це породжує проблему у визначенні джерела впливу, а саме юридичної складності у встановленні зв'язку між маніпулятивним контентом та конкретним суб'єктом виборчого процесу.

Ще однією значною проблемою є поява технологій штучно створених медіа, так званих діпфейків (deep fakes). Якщо раніше пропаганда маніпулювала контекстом чи інтерпретацією фактів або створювала неправдиві інформаційні відомості, то сучасні системи великих мовних моделей (LLM) або так званих систем штучного інтелекту дозволяють фальсифікувати саму реальність, створюючи аудіо- та відеозаписи виступів осіб, яких ніколи не існувало. Це підриває довіру до візуальних доказів і створює феномен інформаційної недовіри, коли виборець перестає вірити будь-яким джерелам інформації, що є критичною загрозою для довіри до виборів.

Таким чином, трансформація виборчих маніпуляцій полягає у переході від відкритого переконання до прихованого алгоритмічного управління поведінкою виборця. Правова наука сьогодні змушена шукати баланс між захистом свободи слова та необхідністю регулювання когнітивної безпеки громадян, оскільки

класичні заборони на наклеп чи порушення правил агітації більше не охоплюють всього спектру гібридних загроз у цифровому просторі.

Як зазначає К. Філіпчук, загрозу демократії та виборам створює дезінформація, яка має далекосяжні наслідки для прав людини та демократичних норм у всьому світі. Вона загрожує свободі думки, праву на приватність та праву на демократичну участь, а також ставить під загрозу низку економічних, соціальних та культурних прав. Дослідниця підкреслює, що дезінформація зменшує ширші показники якості демократії, підриваючи довіру громадян до демократичних інституцій. Дезінформація під час виборів підриває довіру до інститутів демократії, розпалюючи хибні негативні переконання щодо чесності виборів, або ж підтримує диктаторів, створюючи хибно позитивні уявлення про них [5, с. 288-290].

Для розуміння масштабу проблеми слід звернутися до конкретних прикладів впливу цифрових технологій на виборчі процеси. За результатами референдуму про вихід Великої Британії з ЄС у 2016 році розрив у голосуванні склав лише 3% (51% - за, 48% - проти) [6]. Дослідники вважають, що така поляризація думок стала наслідком активного поширення таргетованої реклами у Facebook як з боку кампаній на підтримку однієї з позицій, так і британських політичних діячів. Схожа ситуація відбувалась під час президентських виборів у США 2016 року, коли кандидати активно використовували соціальні мережі, аналітику великих даних та мобільні застосунки для охоплення потенційних виборців.

Результатом обох політичних кампаній стало накопичення приватних даних мільйонів користувачів Facebook без їх згоди. Приватна англійська компанія Cambridge Analytica зібрала понад 50 мільйонів профілів користувачів Facebook та їхніх персональних даних, створивши систему, яка профілювала окремих виборців для націлювання на них персоналізованої політичної реклами

Системи профайлінгу розроблені таким чином, аби на основі зібраних даних про користувача робити висновки про його особисті уподобання. В

подальшому такі профілі та прогнози використовуються для персоналізації політичних повідомлень, наприклад висвітлення у рекомендованих повідомленнях реклами у соціальних мережах. Фундаментальним документом, що вирішує питання обробки персональних даних при профайлінгу, є Загальний регламент захисту даних (GDPR), який визначає профайлінг як будь-яку форму автоматизованої обробки персональних даних для оцінки особистих аспектів фізичної особи, зокрема для аналізу або прогнозування інтересів, поведінки та розташування. Обробка чутливих даних особи дозволяється виключно за її згодою, за винятком передбачених законом випадків. Також важливо, що профайлінг може створювати чутливі дані на основі логічних висновків із звичайних персональних даних, які у сукупності з іншими даними стають спеціальними та можуть виявити політичні переконання, сексуальну орієнтацію та інші захищені характеристики [8, с. 21].

Мікротаргетинг полягає у використанні персональних даних, стратегічно спрямованому на адресування індивідуальних персоналізованих повідомлень виборцям, яких можна переконати чи мобілізувати. Техніка мікротаргетингу зазвичай включає три кроки: збір особистих даних; використання цих даних для визначення груп людей, сприйнятливих до певного повідомлення; надсилання індивідуалізованих онлайн-повідомлень [8, с. 19]. Тоді ж публічний дискурс фрагментується на вищезгадані “інформаційні бульбашки”, де виборець отримує тільки ту інформацію, яка підтверджує його упередження.

Побудова більш прицільної та ефективної кампанії, що ґрунтується на масивах персональних даних, очевидно створює загрози для базових засад свободи волевиявлення. Під час використання традиційних медіа політичну рекламу бачить вся виборча аудиторія, а її поширення обмежене виборчим періодом. Онлайн-реклама, на відміну від телевізійної, спрямована на вузькі категорії виборців, не має кордонів чи часових обмежень [8, с. 4]. Це означає, що прихована передвиборча реклама може відбуватись значно раніше до початку виборчого процесу.

Координована неавтентична поведінка передбачає створення мереж облікових записів або сторінок, які працюють для введення в оману публіки. Ботами називають елементи програмного забезпечення, призначені для автоматизації повторюваних завдань. У соціальних мережах боти часто видають себе за справжніх користувачів з метою обдурити як людей, так і алгоритми [8, с. алгоритмів та автоматизованих програмних продуктів, навмисно спрямованих на управління та поширення оманливої інформації у соціальних мережах, а також на імітацію користувачів задля маніпулювання громадською думкою на різних платформах [9].

Кодекс поведінки щодо дезінформації визначає конкретні маніпулятивні поведінки та практики: створення та використання фейкових акаунтів, захоплення акаунтів та бот-керувану ампліфікацію; імпресонацію; зловмисні діпфейки; купівлю фейкової залученості; непрозорі оплачені повідомлення або просування від інфлюенсерів; координовану неавтентичну поведінку; поведінку користувачів, спрямовану на штучне підсилення охоплення або передбачуваної публічної підтримки дезінформації [10].

Також новою загрозою для публічної довіри є використання згенерованих відео, так званих діпфейків. Прикладом загрозливого використання діпфейків стали кібератаки з Російської Федерації на початку повномасштабної війни проти України, коли було опубліковано діпфейк Президента Зеленського, який нібито закликав громадян скласти зброю [11]. У Франції перед виборами до Європарламенту 2024 року з'явилося фейкове відео з кандидаткою [11a].

У контексті зловживання алгоритмами онлайн-платформ особливу загрозу становить їх здатність маніпулювати публічною думкою. Підсвідомі та персоналізовані рівні алгоритмічного переконання можуть чинити значний вплив на когнітивну автономію фізичних осіб та їх право формувати думку та приймати незалежні рішення, що зазначено у Декларації Комітету міністрів Ради Європи про маніпулятивні можливості алгоритмічних процесів від 13 лютого 2019 року

Як зазначають М. Маук та М. Громпінг, більшість людей у масовому суспільстві дізнається про політику через опосередковану інформацію, тому вона цілком може вплинути на те, як люди формують переконання щодо чесності виборів. Зокрема, дезінформація може погіршити сукупну точність інформації, доступної людям для оновлення своїх переконань [13, с. 965-998].

Окремим напрямком цифрових загроз є маніпулятивні опитування у виборчому процесі. У виборчих кампаніях часто можна помітити маніпуляції при проведенні опитувань громадської думки, які вимірюють та порівнюють політичну конкуренцію. Зловмисні гравці можуть маніпулювати статистичними даними для досягнення власних цілей. Як зазначається в аналітичному звіті ГО “Лабораторія цифрової безпеки”, соціологічні опитування мають здебільшого негативний вплив у пострадянських країнах, де маніпуляція думкою часто виражена через приховування замовників опитувань. Яскраві приклади маніпуляції було виявлено при проведенні місцевих виборів в Україні у 2020 році: при висвітленні результатів соціопитування медіа не вказували замовників дослідження, даних про час проведення, територію охоплення, розмір вибірки та статистичну похибку [8, с. 24].

Рекомендація №R(99)15 Комітету міністрів Ради Європи державам-членам про заходи щодо висвітлення виборчих кампаній у ЗМІ передбачає, що нормативно-правові рамки повинні забезпечувати надання громадськості достатньої інформації для формування судження про цінність опитувань, зокрема: назву організації-замовника опитування, використану методологію, вибірку та похибку, дату проведення [14]. Рекомендація CM/Rec(2022)12 фактично дублює ці вимоги, додатково передбачаючи можливість заборони проведення опитувань під час виборчого процесу [15].

Важливим аспектом трансформації виборчих маніпуляцій у цифрову епоху є вимір впливу ІІІ на вибори. Як зазначається в аналітичному документі IFES, ІІІ відіграє значну роль у тому, як виборці бачать і сприймають виборчий процес. Технології ІІІ можуть бути використані для створення та поширення неправдивої інформації або пропаганди, що може вплинути на думку виборців

або підривати довіру до державних інституцій. Аналізуючи великі масиви даних, алгоритми ШІ можуть виявляти вразливі групи населення та адаптувати дезінформаційні кампанії, щоб відмовляти їх від участі у виборах або взаємодії з державними службами [16, с. 8].

Генеративний ШІ може бути використаний для маніпулювання контентом, що пов'язаний з інформацією щодо виборів, потенційно впливаючи на електоральну поведінку. Різні форми ШІ систем швидко долають технологічні обмеження, і здатність до переконання з часом може посилюватися: деякі моделі ШІ можуть зробити можливими маніпуляції у формі фейкових новин, підроблених відео або постів у соціальних мережах, покликаних обдурити користувачів. Наприклад, під час виборчої кампанії до Європейського парламенту у 2024 році чат-боти Google, Microsoft та OpenAI надавали неправдиву інформацію про дати виборів і процедури голосування, що було зафіксовано Democracy Reporting International [17].

Виборче право має розвиватися та пристосовуватися до змін та можливостей, пов'язаних із новими цифровими реаліями. Як зауважує М. Ярд, хоча технології можуть допомогти досягти як ефективності, так і прозорості виборів, вони зазвичай впроваджуються так, що сприяють першій над другою, ризикуючи передати владу “від багатьох” до “рук небагатьох” [18].

Е. Ф. Джадж та А. М. Корхані вказують, що надмірне регулювання політичних висловлювань може поставити під загрозу політичну участь поінформованого виборця [19]. Як наслідок виникає необхідність комплексної стратегії, яка б захищала виборчі права та виборчі процедури від надмірного цифрового впливу зацікавлених сторін [5, с. 290].

1.2. Роль цифрових платформ як суб'єктів впливу на виборчий процес та їхня відповідальність

Процес цифровізації призвів до серйозних змін у структурі медіаспоживання населення. Як зазначає А. І. Гаркот, користувачі все частіше обирають не онлайн-версії традиційних медіаресурсів, а контент, який створюється індивідуальними користувачами або їх невеликими командами на

платформах спільного доступу до інформації. Такі користувачі здобувають значну аудиторію, яка співмірна з аудиторією традиційних медіа або навіть перевершує її, при цьому на них не поширюються законодавчі обмеження, характерні для медіа [20, с. 324].

Результати щорічного дослідження USAID/Internews демонструють, що соціальні мережі стали домінуючим джерелом новин, яке використовують 84% респондентів. Водночас 42% респондентів вказали, що для отримання новинного контенту використовують лише цей різновид медіа. Аудиторія традиційних сайтів новин скорочується: з 42% у 2022 році до 30% у 2024-му. Кількість глядачів телебачення як джерела новин зменшилася до 30% [21]. Ці дані свідчать про фундаментальну зміну інформаційного ландшафту, в якому цифрові платформи перетворилися з інструментів комунікації на потужні важелі впливу на виборчий процес.

Аналіз платформ поширення фальшивого контенту під час виборів до Європарламенту 2024 року показує, що X (раніше Twitter) (32,4%) та Facebook (21,9%) були двома основними каналами поширення дезінформації [2, с. 12]. Помітним є також TikTok (9,7%), платформа, яка визнається в літературі за свою здатність вірусно поширювати фальшивий контент [2, с. 12]. Значний відсоток дезінформації також поширювався через традиційні медіа (13,3%), що стосувалося переважно заяв політиків, які були повністю або частково неправдивими. Проте у таких випадках поширення фейків покладалося на самих політичних акторів, а не на журналістів [2, с. 12].

При цьому WhatsApp та Telegram відіграли незначну роль у поширенні фальшивого контенту під час виборів до Європарламенту 2024 [2, с. 12]. Все ж варто зауважити, що зашифровані месенджери суттєво ускладнюють моніторинг та виявлення дезінформації, на що вказують інші дослідження.

Аналіз виборів 2019 року в Іспанії підтверджує значну роль Facebook як платформи для поширення політичної дезінформації. Дослідження Л. Кано-Орон, Д. Кальво, Г. Лопес Гарсії та Т. Бавієри 14 684 рекламних оголошень на Facebook, опублікованих п'ятьма основними національними політичними

партіями Іспанії під час двох загальних виборів 2019 року, показало, що, хоча дезінформаційні повідомлення у рекламі були нечастими, вони були присутні переважно у контенті партій Ciudadanos та VOX [22, с. 1]. Примітно, що основною темою рекламних оголошень була єдність Іспанії, пов'язана з питанням незалежності Каталонії, що засвідчує вплив національного контексту на зміст виборчої дезінформації [22, с. 1].

Дослідження також виявило, що рекламні стратегії політичних партій на Facebook були подібними до стратегій традиційної реклами. Так звані “традиційні” партії довше утримувалися від відмови від класичних форм ведення кампанії порівняно з новими партіями, що демонструє, що суб'єкти, які впроваджують дезінформаційні стратегії, не обмежуються лише крайнім правим сегментом ідеологічного спектра [22, с. 1]. Сфера між дезінформацією, пропагандою та рекламою є розмитою: інформація, що публікується урядами, державними установами та партіями, відображає їхній порядок денний у спосіб, що відрізняється від об'єктивної та доказової інформації [22, с. 4].

Т. Бавієра, Х. Санчес-Хункерас та П. Россо підкреслюють, що рекламна платформа Facebook надає політичним партіям виборчий інструмент, що дозволяє охоплювати надзвичайно деталізовану аудиторію [23, с. 1]. Непрозора модель поширення реклами у Facebook робить його привілейованим каналом для розповсюдження фейкових новин та дезінформації [23, с. 3]. Реклама на Facebook довела свою ефективність, коли намір полягає у посіянні розколу серед електорату [23, с. 3]. Дослідження Фаулера та співавторів надало докази того, що претенденти та кандидати нижчого рівня більше використовують Facebook, ніж телевізійну рекламу, через нижчу вартість реклами у соціальних мережах. У результаті виборці знайомились з інформацією про більшу кількість кандидатів на Facebook, ніж на телебаченні, що є позитивним явищем для демократії [23, с. 4]. Водночас при вивченні контенту того ж кандидата на обох каналах, виявилось, що реклама на Facebook менш схильна до атак на суперника, менше обговорює проблеми та більше посилює партійність: ці три відмінності вказують на

використання реклами в соціальних мережах для мобілізації існуючих прихильників, а не для переконання маргінальних виборців [23, с. 4].

Одним із перших кроків для встановлення регламентації правового статусу користувачів платформ спільного доступу до відео та інформації в Європейському Союзі стала Директива Європейського Парламенту та Ради ЄС 2018/1808/EU від 14 листопада 2018 року, якою вносилися зміни у Директиву аудіовізуальних медіапослуг”. Для цього було введено термін “відео створені користувачами” (user-generated video) [24]. У Директиві зазначається, що хоча платформи спільного доступу до відео і не мають редакційного контролю над відео, що публікуються їх користувачами, вони повинні здійснювати модерацію такого контенту на предмет наявності інформації, що порушує законодавство

Таким чином, правовий статус цифрових платформ як суб’єктів впливу на виборчий процес є одним із найбільш актуальних питань сучасного виборчого права. Необхідність встановлення для них відповідальності зумовлена їх здатністю системно впливати на волевиявлення громадян через алгоритмічне управління контентом, мікротаргетинг та створення умов для поширення дезінформації. Для України, яка перебуває в умовах гібридної агресії, це питання набуває екзистенційного значення.

1.3. Практика Європейського суду з прав людини у справах, пов’язаних з дезінформацією

Аналіз практики Європейського суду з прав людини у контексті цифрових загроз потребує дослідження нових підходів, що формуються у відповідь на виклики цифрової епохи. Вибори є основною складовою демократії, за допомогою якого окремі особи та політичні партії отримують владу. Міжнародно-правова система сформувала усталені правові принципи виборчого процесу, що визначають його прийнятність, законність та легітимацію результатів. Вільні та чесні вибори є основою демократичного процесу, а виборчі

зловживання підривають легітимність виборчого процесу, загальну прийнятність результатів виборів та кидають виклик процесу демократизації [5, с. 288].

Принципово важливою для формування нових стандартів стала практика Європейського суду з прав людини. Рішення у справі “Бредшоу та інші проти Сполученого Королівства” від 22 липня 2025 року створило важливий прецедент для захисту демократії від зовнішнього втручання. Суть скарги полягала в тому, що уряд Великої Британії, маючи надійні звіти розвідки про спроби Росії втрутитися у демократичні процеси (включаючи референдум щодо Brexit 2016 року та парламентські вибори 2019 року), не провів належного розслідування

ЄСПЛ у цій справі вперше чітко встановив, що право на вільні вибори (стаття 3 Першого протоколу до Конвенції) покладає на державу позитивний обов’язок не просто утримуватися від втручання у вибори, а й активно захищати виборчий процес від зовнішніх загроз, таких як іноземна дезінформація та кібератаки. Суд визнав, що кампанії дезінформації й іноземне втручання здатні істотно впливати на демократію [25, п. 147, 158]. Водночас ЄСПЛ надав державам широкі межі розсуду у виборі конкретних інструментів захисту, зазначивши, що вони повинні бути збалансовані з правом на свободу вираження поглядів [25, п. 159-162].

Суддя ЄСПЛ Андраш Якаб в окремій думці запропонував конкретні регуляторні рішення, зокрема зобов’язати соціальні мережі забезпечувати ідентифікацію користувачів, за замовчуванням показувати у стрічці лише контент від обраних джерел, запровадити затримку перед публікацією, розглянути заборону мікротаргетованої політичної реклами; зобов’язати розробників ШІ-чат-ботів вживати заходів проти поширення дезінформації. Він також наголосив, що на державу має бути покладено чітке зобов’язання розслідувати подібні випадки, інакше право на вільні вибори стає ілюзорним [26].

У справі “Тімпул Інфо-Магазин та Ангел проти Молдови” ЄСПЛ розглядав конфлікт між свободою преси та правом на захист репутації [27]. Молдовська газета опублікувала статтю, яка критикувала уряд за непрозорі закупівлі

автомобілів, згадуючи чутки про можливий хабар [27, п. 7-8]. Інвестиційний фонд D.H., згаданий у статті, подав позов про дифамацію, який було частково задоволено національними судами [27, п. 9, 14, 19]. Суд наголосив на провідній ролі преси в демократичному суспільстві [27, п. 31] та зазначив, що стаття була спрямована на критику уряду з питання справжнього суспільного інтересу [27, п. 32]. Суд встановив, що національні органи вирвали цитату про хабар з контексту захисту, якщо вони не є повністю безпідставними [27, п. 36]. Відсутність детальної інформації про транзакцію як від уряду, так і від інвестиційного фонду виправдовувала повідомлення журналістом навіть неперевіраних чуток [27, п. 32, 36]. ЄСПЛ також зауважив, що стаття була написана в контексті майбутніх виборів і містила політичне висловлювання, щодо якого “межі допустимої критики є ширшими” [27, п. 38]. Відповідно, Суд визнав порушення статті 10 Конвенції [27, п. 40-41].

У справі “Меджліс Ісламської Спільноти Брчко та інші проти Боснії і Герцеговини” ЄСПЛ встановив, що громадські та інші неурядові організації, привертаючи увагу до питань суспільного інтересу, виконує роль “громадського охоронця” подібну до преси [28, п. 86]. Однак, як і журналісти, НУО мають діяти добросовісно з метою надання точної та достовірної інформації [28, п. 87]. Найважливішим фактором у справі була достовірність інформації [28, п. 107]: заявники були зобов’язані перевіряти фактичні твердження, які є дифамаційними щодо приватних осіб [28, п. 109]. Національні органи встановили невідповідність між тим, що заявникам повідомили, і тим, що вони повідомили в листі [28, п. 112]. ЄСПЛ дійшов висновку, що порушення статті 10 не було [28, п. 122], встановлюючи важливий баланс між свободою вираження поглядів та захистом репутації.

У справі “Салов проти України” ЄСПЛ розглядав питання кримінального переслідування за поширення інформації під час виборчої кампанії. Сергія Салова, адвоката і представника кандидата в Президенти України Олександра Мороза, було засуджено за перешкоджання виборчим правам громадян шляхом

поширення неправдивої інформації про смерть діючого Президента Леоніда Кучми через підроблений випуск газети “Голос України” [29, п. 13, 28]. Суд наголосив, що стаття 10 Конвенції не забороняє обговорення або поширення отриманої інформації, навіть якщо виникають сумніви щодо її вірогідності [29, п. 113]. ЄСПЛ також врахував обмежений вплив інформації, оскільки заявник мав лише вісім екземплярів підробленої газети [29, п. 114]. Щодо пропорційності втручання, Суд зазначив, що покарання (5 років умовного позбавлення волі, штраф і анулювання адвокатської ліцензії) було надто суворим [29, п. 115]. ЄСПЛ визнав порушення статті 10 Конвенції [29, п. 116], встановивши принцип: обговорення та поширення інформації, навіть неправдивої, не може бути підставою для непропорційно суворого покарання в контексті виборчих кампаній.

Аналіз практики ЄСПЛ дозволяє виокремити ключові правові позиції: при визначенні меж допустимого втручання у свободу вираження поглядів ЄСПЛ враховує контекст справи, природу інформації та потенційну шкоду від поширення; суд розрізняє фактичні твердження та оціночні судження; медіа та неурядових організацій, виконуючи роль “громадського охоронця”, мають дотримуватися професійних стандартів; обмеження свободи вираження поглядів має бути пропорційним легітимній меті; ЄСПЛ враховує суворість санкцій, визнаючи непропорційність кримінального покарання за поширення інформації в контексті виборчих кампаній.

Висновки до Розділу 1. Сучасна дезінформація відрізняється від пропаганди ХХ століття своєю таргетованістю, фрагментацією публічного дискурсу на так звані “інформаційні бульбашки” та використанням проксі-суб’єктів - бот-ферм, тролів та алгоритмічних систем, що ускладнює встановлення зв’язку між маніпулятивним контентом та конкретним суб’єктом виборчого процесу. Поширеним явищем також є мікротаргетинг на основі використання персональних даних, використання генеративного штучного інтелекту, а також маніпулятивні соціологічні опитування. Поширення цих практик було підтверджене у низці виборчих кампаній, зокрема у президентських

виборах США 2016 року, референдумі щодо виходу Великої Британії з ЄС та виборах до Європейського Парламенту 2019 та 2024 років.

Також можна дійти висновку, що цифрові платформи трансформувалися з технічних посередників на повноцінних суб'єктів впливу на виборчий процес. Дослідження підтверджують, що соціальні мережі стали домінуючим джерелом новин для 84% респондентів, тоді як аудиторія традиційних медіа поступово скорочується. Аналіз поширення дезінформації під час виборів до Європарламенту 2024 року засвідчив провідну роль таких соціальних мереж як до поширення оманливого контенту.

У практиці Європейського суду з прав людини сформувалися важливі правові позиції щодо захисту виборчого процесу від цифрових загроз. Знаковим є недавнє рішення у справі “Бредшоу та інші проти Сполученого Королівства”, у якому ЄСПЛ вперше встановив, що право на вільні вибори покладає на державу позитивний обов’язок не лише утримуватися від втручання у вибори, а й активно захищати виборчий процес від зовнішніх загроз, зокрема іноземної дезінформації та кібератак. Аналіз справ “Тімпул Інфо-Магазин та Ангел проти Молдови”, “Меджліс Ісламської Спільноти Брчко проти Боснії і Герцеговини” та “Салов проти України” засвідчує, що ЄСПЛ розрізняє фактичні твердження та оціночні судження, враховує контекст справи та вимагає пропорційності санкцій, водночас не виключаючи обмежень свободи вираження поглядів за наявності легітимної мети. Таким чином, формування правових механізмів протидії маніпуляціям у виборчому процесі потребує балансу між захистом свободи слова та необхідністю забезпечення когнітивної безпеки виборця як невід’ємної передумови вільного волевиявлення.

Підсумовуючи аналіз теоретико-правових засад захисту виборчого процесу в цифрову епоху, можна стверджувати, що трансформація маніпуляцій у виборчому процесі, зміна правового статусу цифрових платформ та розвиток міжнародних стандартів вільних виборів формують нову правову реальність, в якій захист демократичного волевиявлення потребує комплексного та

технологічно розвиненого підходу. Для України, яка протистоїть збройній агресії РФ , формування правових механізмів протидії цифровим загрозам на виборах є не просто питанням удосконалення законодавства, а питанням збереження та зміцнення демократичних засад державності.

РОЗДІЛ 2. РЕГУЛЯТОРНА МОДЕЛЬ ЄС ЩОДО ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ПІД ЧАС ВИБОРІВ

2.1. Еволюція регулювання дезінформації в ЄС: від Кодексу поведінки до Digital Services Act та спеціалізованих регламентів

У контексті еволюції регулювання дезінформації в ЄС важливим є розуміння контексту, що обумовив регуляторні дії. Як зазначають Д. А. Фузієк, А. Е. Стуг'яну та Т.-В. Ефтімі-Еглтон, перед виборами до Європейського парламенту 2019 року ЄС зіткнувся з двома головними проблемами: алгоритмами, що надають додаткову видимість контенту, який генерує залученість та численні коментарі, тим самим посилюючи провокативні або дискусійні думки, та моделлю бізнесу, заснованою на увазі, яка сприяє поляризації та фрагментації онлайн-інформаційного простору [30, с. 4-5]. Надмірна представленість такого контенту на платформах соціальних мереж створює не лише враження, що ці ідеї поділяються більшою частиною суспільства, а й сприяє мейнстрімізації радикальних думок, включаючи теорії змови та пропаганду [30, с. 5].

Ще однією загрозою, з якою зіткнувся ЄС, було зменшення явки виборців. Ця тактика, яка покладається на поширення неправдивої онлайн-інформації щодо процедур голосування, раніше була застосована на президентських виборах у США 2016 року, де шкідливі онлайн-групи вдало відвернули американських виборців від участі у демократичному процесі [30, с. 5]. Крім того, як показали вибори до Європарламенту 2014 року, ЄС загальна явка виборців склала лише 42,6% виборців ЄС, які взяли участь у голосуванні, що вказувало на вразливість ЄС до зловмисних атак, здатних посилити вже існуючі негативні тенденції [30, с.

Дослідження європейської регуляторної моделі протидії дезінформації під час виборів потребує насамперед окреслення концептуального підходу Європейського Союзу до самого феномену дезінформації. У європейській правовій доктрині було відсутнє уніфіковане нормативне визначення цього поняття, однак існувала низка офіційних інтерпретацій, що використовуються в

актах м'якого права (англійською *soft law*) та актах інституцій Європейського Союзу, які формують поняттєву основу для подальшого законодавчого регулювання.

Початковим етапом системної відповіді ЄС на загрози, пов'язані з дезінформацією, став План дій проти дезінформації - *Action Plan against* дано визначення дезінформації як верифіковано неправдивої або оманливої інформації, що створюється, подається та поширюється з метою отримання економічної вигоди або навмисного введення в оману громадськості, і яка може завдати суспільної шкоди [31, с. 2]. При цьому документ чітко визначає, що суспільна шкода включає загрози демократичним процесам, а також суспільним благам, таким як здоров'я громадян ЄС, навколишнє середовище чи безпека. Важливо, що до дезінформації не відносяться ненавмисні помилки, сатира і пародія, або чітко визначені партійні новини та коментарі [31, с. 2].

У документі також наголошується, що заходи, передбачені в Плані дій, спрямовані лише на контент дезінформації, який є легальним відповідно до законодавства ЄС або національного законодавства. Вони реалізуються без шкоди для законів ЄС або будь-якої з держав-членів, які можуть бути застосовані, включаючи правила щодо нелегального контенту [31, с. 2]. Це розмежування між легальним дезінформаційним контентом та нелегальним контентом є принципово важливим для розуміння європейського підходу: ЄС не прагне криміналізувати дезінформацію як таку, а натомість створює механізми зменшення її впливу, зберігаючи при цьому свободу вираження поглядів.

Як зазначається у Вступі Плану дій, дезінформація становить значну загрозу для європейських демократій та суспільств, і Союз повинен вирішувати цю проблему, дотримуючись європейських цінностей та свобод. Документ підкреслює, що дезінформація підриває довіру громадян до демократії та демократичних інституцій, сприяє поляризації громадської думки та втручається у демократичні процеси прийняття рішень [31, с. 11-12]. Ці положення є особливо релевантними в контексті виборчих процесів, оскільки саме під час

виборів наслідки дезінформації можуть мати найбільш деструктивний вплив на демократичний устрій.

Саме цей документ заклав основу для саморегулювання онлайн-платформ через створення першого Кодексу практики щодо дезінформації - Code of Practice on Disinformation, який було підписано у вересні 2018 року. План дій визначив чотири стовпи координованої відповіді ЄС на загрозу дезінформації: покращення можливостей інституцій Союзу щодо виявлення, аналізу та викриття дезінформації; зміцнення координованих та спільних відповідей; мобілізація приватного сектору; а також підвищення обізнаності та зміцнення суспільної стійкості [32, с. 5]. Особливу увагу було приділено контексту виборів до Європейського Парламенту 2019 року, що свідчить про безпосередній зв'язок антидезінформаційної політики ЄС із захистом виборчих процесів.

Особливу увагу в Плані дій приділено ролі соціальних медіа як засобу поширення дезінформації. Як зазначається в документі, технології відеоманіпуляції (deep fakes) та фальсифікації офіційних документів, використання ботів для поширення дискусійного контенту, тролінг-атаки на профілі у соціальних мережах та крадіжка інформації стали стандартними інструментами дезінформаційних кампаній [32]. Хоча традиційні методи, такі як телебачення, газети, веб-сайти та ланцюгові електронні листи, продовжують відігравати важливу роль у багатьох регіонах, варто звернути увагу на інструменти та методи, що використовуються і змінюються швидко, і відповідь на ці загрози повинна еволюціонувати так само стрімко.

План дій також акцентує увагу на проблемі дезінформації з боку третіх країн, яка часто є частиною гібридної війни, що включає кібератаки та спроби зламу профілів. Документ підкреслює, що іноземні державні актори все частіше застосовують стратегії дезінформації для впливу на суспільні дебати, створення розколів та втручання у процеси демократичного прийняття рішень [32]. Ці стратегії спрямовані не лише на держави-члени, але й на країни-партнери у Східному Партнерстві, Південному сусідстві, на Близькому Сході та в Африці.

Такий транскордонний характер загрози обумовлює необхідність координованої відповіді на рівні всього Союзу.

Значним кроком у трансформації регуляторного підходу став Європейський план дій щодо демократії - European Democracy Action Plan, COM(2020) 790 final) від 3 грудня 2020 року, де Європейська Комісія запропонувала систематизований підхід до класифікації та протидії різним формам інформаційних загроз. Цей документ суттєво розширив концептуальний апарат, чітко розмежувавши різні явища, які зазвичай відносять до категорії “дезінформація”, наголошуючи, що таке розмежування є важливим для розробки відповідних політичних заходів.

Зокрема, План дій щодо демократії розрізняє:

- дезінформацію (disinformation) - помилковий або оманливий контент, що поширюється з наміром обману або забезпечення економічної чи політичної вигоди і який може завдати суспільної шкоди;
- неправдиву інформацію (misinformation) - помилковий або оманливий контент, який поширюється без шкідливого наміру, хоча наслідки все одно можуть бути шкідливими;
- операції з інформаційного впливу (information influence operations) - скоординовані зусилля внутрішніх або іноземних акторів впливати на цільову аудиторію, використовуючи різноманітні оманливі засоби;
- іноземне втручання в інформаційний простір (foreign interference in the forming and expression of political will of individuals from another country or its agents [4, с. 18].

У розділі 2.1 Плану дій щодо демократії Комісія наголосила, що для захисту цілісності виборів необхідно вийти за межі добровільного виконання правил платформами. План дій щодо демократії проголосив курс на перетворення Кодексу практики з чисто саморегулюючого інструменту на спільнорегулюючий (co-regulatory) механізм, що інтегрується в ширшу правову рамку Акта про цифрові послуги - Digital Services Act. Зокрема, Комісія

оголосила про намір підготувати законодавчу пропозицію щодо прозорості спонсорованого політичного контенту та посилити Кодекс практики на основі настанов, які будуть розроблені Комісією. Цей підхід ознаменував принциповий зсув від парадигми саморегулювання до спільнорегулювання у сфері протидії дезінформації під час виборів.

Кодекс поведінки щодо дезінформації фактично дублює розуміння феномену дезінформації, представлене в Плані дій щодо демократії. У преамбулі Кодекс розширює концептуальне розуміння дезінформації, включаючи до цього поняття такий же спектр явищ, як у Плані дій щодо демократії: місінформацію, дезінформацію, операції інформаційного впливу та іноземне втручання в інформаційний простір [32, с. 11]. Така розширена інтерпретація відображає еволюцію розуміння проблеми дезінформації за період з 2018 по 2025 рік.

Особливу практичну цінність для захисту виборчого процесу має те, що Кодекс визначає конкретні маніпулятивні поведінки та практики, які підпадають під поняття дезінформації, в тому числі створення та використання фейкових акаунтів, захоплення акаунтів та бот-керована ампліфікація, імперсонація (видавання себе за іншу особу), зловмисні діпфейки, купівля фейкової залученості, непрозорі оплачені повідомлення або просування від інфлюенсерів, створення і використання акаунтів, що беруть участь у координованій неавтентичній поведінці, поведінка користувачів, спрямована на штучне підсилення охоплення або передбачуваної публічної підтримки дезінформації тощо [32, с. 20]. Кожна з цих практик може бути використана під час виборчих кампаній для маніпулювання громадською думкою та викривлення волевиявлення громадян.

Кодекс поведінки щодо дезінформації демонструє еволюцію підходів ЄС до протидії дезінформації від добровільних саморегулюючих стандартів 2018 року до формалізованого механізму в рамках Закону про цифрові послуги. Як зазначається у Кодексі, у січні 2025 року його було перетворено на Кодекс поведінки відповідно до Закону про цифрові послуги - DSA [33, с. 1]. Це суттєво підвищує правовий статус та обов'язковість виконання стандартів протидії

дезінформації. Важливим внеском Кодексу є також визначення структурованої системи суб'єктів, які його підписали.

Принципове значення для розуміння сучасного стану регулювання має Висновок Європейської Комісії від 13 лютого 2025 року щодо оцінки Кодексу практики протидії дезінформації відповідно до статті 45 DSA. У цьому документі Єврокомісія здійснила офіційну оцінку Кодексу в контексті Закону про цифрові послуги, визначаючи його правовий статус та роль в європейській системі протидії дезінформації. Європейська Комісія зазначає, що з моменту свого створення Кодекс практики протидії дезінформації призначався для того, щоб стати частиною нормативно-правової бази, встановленої DSA [33, с. 1]. Наразі понад 40 зацікавлених сторін підписали Кодекс, включаючи сім онлайн-платформ і пошукових систем, які були визначені Комісією як провайдери дуже великих онлайн-платформ або дуже великих онлайн-пошукових систем.

Згідно з оцінкою Комісії, хоча кодекси залишаються добровільними, підписанти можуть дотримуватися зобов'язань, взятих у таких кодексах, як засіб виконання свого обов'язку запроваджувати розумні, пропорційні та ефективні заходи щодо пом'якшення ризиків відповідно до статті 35 DSA [33, с. 2]. Таким чином, для дуже великих онлайн-платформ Very Large Online Platforms дотримання Кодексу стає інструментом пом'якшення системних ризиків, а його невиконання може тягнути суворі санкції.

Особливу цінність для теоретико-правового розуміння проблеми дезінформації у контексті виборів представляє пояснення Комісією, як Кодекс співвідноситься з основними правами. У документі підкреслюється, що поширення дезінформації в інтернеті є особливим суспільним ризиком, який може перешкоджати громадянам Союзу та іншим особам здійснювати свої основні права [33, с. 6]. Серед ключових зобов'язань Кодексу, які мають безпосереднє значення для захисту виборчого процесу, варто виділити: перевірку розміщення реклами (Розділ II), політичну рекламу (Розділ III), цілісність послуг (Розділ IV), розширення можливостей користувачів (Розділ V), розширення

можливостей дослідницької спільноти (Розділ VI) та розширення можливостей спільноти фактчекерів (Розділ VII).

Важливо відзначити, що Європейська Комісія після детального аналізу дійшла висновку, що Кодекс практики протидії дезінформації відповідає умовам для кодексів поведінки, визначеним у статті 45(1) та (3) Регламенту ЄС 2022/2065 регуляторної системи протидії дезінформації. Такий висновок підтверджує процес еволюції європейського правового підходу до розуміння та регулювання дезінформації - від добровільних ініціатив до формалізованих механізмів у рамках обов'язкового законодавства ЄС.

Сьогоднішня регуляторна модель ЄС базується на взаємодії кількох фундаментальних нормативних актів, кожен з яких вносить свій внесок у комплексну систему захисту виборчого процесу від дезінформаційних загроз. Директива ЄС 2018/1808 Audiovisual Media Services Directive (AVMSD), яка внесла зміни до Директиви 2010/13/EU (AVMSD), у пункті 4 преамбули визнає зміну ринкових реалій та необхідність поширення стандартів безпеки на платформи спільного доступу до відео. Стаття 28b цієї Директиви зобов'язує держави-члени забезпечити, щоб платформи спільного доступу до відео вживали належних заходів для захисту користувачів від контенту, що містить підбурювання до ненависті та насильства. У контексті виборів це положення має особливе значення, оскільки відеоплатформи стали одним з основних каналів поширення політичної дезінформації та маніпулятивного контенту [24].

Крім того, стаття 30b Директиви 2010/13/EU у редакції Директиви 2018/1808 засновує Європейську групу регуляторів аудіовізуальних медіа-послуг ERGA, до складу якої входять представники національних регуляторних органів у сфері аудіовізуальних медіа-послуг [24]. ERGA забезпечує технічну експертизу Європейській Комісії для послідовного впровадження Директиви в усіх державах-членах, сприяє обміну досвідом та найкращими практиками, а також надає висновки на запит Комісії щодо технічних та фактичних аспектів питань, що стосуються юрисдикції, порушень та правил загального суспільного інтересу

]. Ця функція є критично важливою для оперативного реагування на транскордонні випадки поширення дезінформації під час виборчих кампаній.

Центральним елементом нової регуляторної архітектури ЄС є Регламент ЄС 2022/2065 - Акт про цифрові послуги - Digital Services Act - DSA, запровадив для дуже великих платформ з 25 серпня 2023 р., а для всіх платформ з 17 лютого 2024 р. DSA запроваджує обов'язки належної обачності для провайдерів цифрових послуг, зокрема для дуже великих онлайн-платформ та дуже великих онлайн-пошукових систем. Стаття 34 DSA зобов'язує ці платформи проводити оцінку системних ризиків, у тому числі будь-яких фактичних або передбачуваних негативних наслідків для здійснення основних прав, зокрема права на свободу вираження поглядів та права на інформацію, а також для громадянського дискурсу, виборчих процесів та громадської безпеки. Стаття 35 DSA вимагає від платформ впровадження розумних, пропорційних та ефективних заходів з пом'якшення виявлених ризиків, а стаття 37 передбачає проведення незалежних аудитів для перевірки виконання цих зобов'язань [34].

Принципово важливим є те, що DSA не обмежується лише боротьбою з нелегальним контентом, а охоплює також системні ризики, пов'язані з поширенням легальної, але шкідливої інформації, зокрема дезінформації під час виборів. Як зазначається у статті 104 DSA, Кодекс практики протидії дезінформації згадується як існуючий саморегулюючий інструмент, який може бути інтегрований у рамки Регламенту. Це підтверджується й у Висновку Комісії 2025 року, де зазначається, що DSA забезпечує надійну правову основу, накладаючи на провайдерів дуже великих онлайн-платформ та пошукових систем зобов'язання ретельно виявляти, аналізувати, оцінювати та пом'якшувати системні ризики, такі як будь-які фактичні або передбачувані негативні наслідки для громадянського дискурсу, виборчих процесів та безпеки [33, с. 3]. Санкції за порушення DSA можуть сягати до 6% від глобального річного обороту платформи, що створює реальний фінансовий стимул для дотримання вимог щодо протидії дезінформації.

Варто також зазначити, що DSA передбачає створення Європейської ради з питань цифрових послуг - European Board for Digital Services, яка складається з координаторів цифрових послуг, призначених кожною державою-членом. Ця рада забезпечує послідовне застосування Регламенту на всій території Союзу, координує спільні розслідування та консультує Комісію щодо питань системних ризиків, у тому числі ризиків для виборчих процесів. Створення цього наглядового органу свідчить про намір ЄС забезпечити не лише нормативне, а й інституційне підґрунтя для ефективної протидії дезінформації на рівні всього Союзу.

Попри вказані позитивні характеристики DSA, щодо обмежень наявного регулювання, О. Романишин зазначає, що DSA не містить чіткого правового визначення дезінформації, що може призвести до фрагментації серед держав-членів ЄС щодо його застосування [35, с. 5]. Крім того, DSA переважно покладає обов'язок боротьби з дезінформацією на дуже великі онлайн-платформи (VLOPs), тоді як інші цифрові сервіси, які також поширюють дезінформацію, не підпадають під ті самі зобов'язання [35, с. 6]. Під час президентських виборів 2022 року у Франції менші платформи, такі як Telegram та Discord, використовувалися для поширення дезінформації та мови ненависті без того ж рівня нагляду [35, с. 6]. Європейський Парламент також висловив занепокоєння щодо відсутності регулювання для платформ, таких як Reddit та Telegram, де дезінформація поширюється значною мірою без моніторингу [35, с. 6].

Окреме важливе місце в системі протидії маніпуляціям під час виборів посідає Регламент ЄС 2024/900 від 13 березня 2024 року про прозорість та таргетинг політичної реклами. Як зазначено у пункті 4 преамбули цього Регламенту, необхідність забезпечення прозорості є легітимною суспільною метою, що відповідає цінностям, які поділяються Союзом та його державами-членами. Регламент підкреслює, що політична реклама може бути інструментом дезінформації, особливо коли вона не розкриває свою політичну природу, надходить від спонсорів за межами Союзу або використовує методи таргетування

відкритих та чесних політичних дебатів, а також для протидії маніпулюванню інформацією та втручанню.

Регламент 2024/900 суттєво розширює інституційний інструментарій, запроваджуючи обов'язок держав-членів призначити компетентні органи для нагляду за прозорістю політичної реклами. Стаття 15 Регламенту передбачає створення Європейського репозиторію для онлайн-політичної реклами, який адмініструється Комісією, що дозволяє здійснювати централізований аудит рекламних кампаній. Більше того, згідно з пунктом 6 преамбули Регламенту, в контексті політичної реклами часто використовуються методи таргетування та доставки рекламних повідомлень на основі обробки персональних даних, включаючи дані, що розкривають політичні переконання. Такі методи можуть становити особливі загрози для законних суспільних інтересів, зокрема для чесності, рівних можливостей та прозорості виборчого процесу [36, пункт 6 преамбули].

Значення Регламенту 2024/900 для захисту виборчого процесу важко переоцінити. Як зазначається у пункті 7 преамбули, політична реклама наразі регулюється неоднорідно в державах-членах, причому національне законодавство зазвичай зосереджується на традиційних медіа-формах. Існують специфічні обмеження щодо транскордонного надання послуг політичної реклами, які впливають на проведення транскордонних та загальноєвропейських політичних кампаній. Водночас прогалини та лакуни в національному законодавстві деяких держав-членів призводять до того, що політична реклама іноді поширюється без урахування відповідних національних правил, ризикуючи підірвати регулювання прозорості політичної реклами [36, пункт 7 преамбули]. Регламент покликаний гармонізувати ці правила на рівні всього ЄС, забезпечуючи єдині стандарти прозорості незалежно від того, через яку юрисдикцію поширюється рекламне повідомлення.

Ще одним важливим елементом регуляторної моделі ЄС є Регламент ЄС 2024/1689 від 13 червня 2024 року або як його ще називають Акт про штучний інтелект - AI Act. Згідно з пунктом 60 преамбули Акта, системи ШІ, що

використовуються для впливу на результати виборів або поведінку виборців під час здійснення ними свого права голосу, повинні бути віднесені до систем ШІ з високим ступенем ризику. Це означає, що розробники та оператори таких систем зобов'язані дотримуватися суворих вимог щодо прозорості, документації, людського нагляду та управління ризиками [37]. Стаття 50 Акта про ШІ встановлює зобов'язання щодо прозорості для контенту, згенерованого штучним інтелектом: користувачі повинні бути чітко поінформовані про те, що вони взаємодіють із ШІ або споживають синтетичний контент, зокрема так звані діпфейки [37]. Це положення є критично важливим для забезпечення права виборця на отримання достовірної інформації під час виборчих кампаній.

Акт про штучний інтелект побудований на підставі оцінювання рівня ризиків і визначає чотири рівні: неприйнятні ризики, високі ризики, обмежені ризики та мінімальні ризики. До неприйнятних ризиків належать системи ШІ, що становлять відверту загрозу безпеці та правам людини, наприклад системи, які маніпулюють поведінкою людей або класифікують їх на основі соціального скорингу. У сфері виборів можна передбачити, що системи ШІ, які класифікують осіб на підставі їхньої поведінки під час голосування або навмисно поширюють маніпулятивну інформацію серед вразливих груп населення, підпадають під цю категорію [16, с.17].

Щодо систем ШІ з високим ступенем ризику, в остаточному тексті Акту зазначено, що виняток становлять лише інструменти, що використовуються для організації, оптимізації та структурування політичних кампаній з погляду адміністрування та матеріально-технічного забезпечення. Для систем високого ризику передбачено обов'язкові системи управління ризиками, суворі зобов'язання щодо управління даними та правила людського нагляду за моделлю. Штрафи за недотримання заборони практик ШІ складають до 35 000 000 євро або до 7% загального річного обороту [16, с. 18].

Важливим є також те, що Акт про штучний інтелект поширює свою юрисдикцію на постачальників систем ШІ за межами ЄС, зокрема в Україні, якщо результати згенеровані системою, призначені для використання в межах

ЄС. Очікується, що Україна як країна'-кандидат на вступ до ЄС найближчими роками інкорпорує Акт про штучний інтелект у своє національне законодавство в межах процесу вступу до ЄС [16, с. 10].

Класифікація систем ШІ, що впливають на виборчий процес, як систем високого ризику тягне за собою низку конкретних обов'язків для їхніх розробників та операторів. Зокрема, такі системи мають відповідати вимогам щодо якості даних, технічної документації, ведення журналів подій, людського нагляду та кібербезпеки. Розробники зобов'язані проводити оцінку відповідності перед виведенням системи на ринок, а оператори - забезпечувати належне використання системи відповідно до інструкцій виробника. У контексті виборів це означає, що будь-яка система ШІ, що використовується для таргетування виборців, генерації політичного контенту або аналізу електоральних настроїв, підпадає під жорстке регулювання, що суттєво обмежує можливості маніпулювання через алгоритмічні засоби.

Взаємозв'язок між Актом про ШІ та іншими елементами регуляторної моделі ЄС є особливо значущим. Як зазначається у Висновку Комісії 2025 року, Кодекс практики протидії дезінформації було оновлено з урахуванням набуття чинності Актом про ШІ та Регламентом про політичну рекламу [33, с. 2]. Це свідчить про прагнення ЄС до створення інтегрованої правової рамки, де різні нормативні акти доповнюють один одного, забезпечуючи комплексний захист від маніпуляцій на всіх рівнях - від генерації контенту штучним інтелектом до його поширення через цифрові платформи та таргетування конкретних категорій виборців.

Таким чином, сучасна регуляторна модель ЄС перейшла від точкових ініціатив саморегулювання до комплексної системи актів, де прозорість реклами, відповідальність платформ, стандарти протидії дезінформації та безпека алгоритмів утворюють єдиний правовий щит для захисту виборчих процесів. Ця еволюція від м'якого права до жорсткого нормативного регулювання відображає усвідомлення на рівні ЄС того факту, що добровільні зобов'язання платформ самі

по собі є недостатніми для ефективної протидії дезінформації, особливо в контексті критично важливих для демократії виборчих процесів.

2.2. Роль європейських інституцій у протидії дезінформаційним кампаніям

Ефективність правових механізмів ЄС щодо протидії дезінформації під час виборів забезпечується багаторівневою інституційною архітектурою, яка поєднує політичний нагляд, технічну експертизу та оперативне реагування. Формування цієї інституційної інфраструктури відбувалося поступово, починаючи з 2015 року, і сьогодні становить розгалужену екосистему взаємопов'язаних органів та структур, кожна з яких виконує специфічну функцію у захисті демократичного дискурсу від маніпулятивних втручань.

Фундамент інституційної співпраці був закладений у Плані дій проти дезінформації 2018 року, який запровадив Систему швидкого сповіщення Rapid Розділі 3.2 Плану дій, RAS виконує функції платформи для обміну даними про дезінформаційні кампанії в реальному часі, що дозволяє координувати відповіді на гібридні загрози під час виборчих циклів [31]. Система передбачає, що кожна держава-член повинна визначити контактний пункт, який ідеально розташований у підрозділах стратегічних комунікацій, для забезпечення координації з усіма відповідними національними органами, а також з Комісією та Європейською службою зовнішньополітичної діяльності. У випадках, коли дезінформація стосується виборів або функціонування демократичних інституцій у державах-членах, національні контактні пункти мають тісно співпрацювати з національними виборчими мережами [31, с. 8].

Першою спеціалізованою структурою ЄС, створеною для протидії дезінформації, стала Оперативна робоча група зі стратегічних комунікацій East StratCom Task Force, далі - ESTF, заснована у березні 2015 року в рамках Європейської служби зовнішньополітичної діяльності (EEAS). Створення ESTF відбулося після рішення Європейської Ради про необхідність боротьби з російськими дезінформаційними кампаніями. Цей підрозділ допомагає ЄС у

країнах Східної Європи та адмініструє веб-сайт “EUvsDisinfo.eu”, де публікуються виявлені випадки дезінформації [38]. Як зазначається у Плані дій проти дезінформації, East StratCom Task Force проаналізувала та висвітлила понад 4500 прикладів дезінформації з боку Російської Федерації, виявляючи численні дезінформаційні наративи та підвищуючи обізнаність щодо інструментів, методів та намірів дезінформаційних кампаній [31].

Разом з тим діяльність ESTF не позбавлена критики, що свідчить про складність балансування між протидією дезінформації та забезпеченням свободи слова. Зокрема, у впливовому виданні EU Observer у 2018 році нідерландський політик Ар'єн Н'єбор висловив позицію про необхідність закриття веб-сайту “EUvsDisinfo.eu”, аргументуючи це принципом невтручання держави у вільні медіа [39]. Автор навів випадок безпідставного звинувачення трьох голландських медіа-ресурсів у поширенні дезінформації, що завершився судовим позовом проти Європейського Союзу. Він стверджував, що боротьба з дезінформацією має здійснюватися не державними органами, а іншими вільними медіа, експертами та неурядовими організаціями, та поставив під сумнів твердження про суттєвий вплив російської дезінформації на європейські демократії, підкреслюючи відсутність конкретних доказів впливу іноземного втручання на результати виборів чи референдумів [39]. Ця дискусія засвідчує важливість додержання балансу між ефективною протидією дезінформації та збереженням демократичних свобод, що є одним із ключових викликів для інституційної архітектури ЄС.

Значним кроком у зміцненні аналітичної спроможності ЄС стало створення у червні 2020 року Європейської обсерваторії цифрових медіа European Digital керівництвом Європейського університетського інституту у Флоренції (Італія) та включає інформаційну лабораторію Орхуського університету та Афінський технологічний центр. Обсерваторія об'єднує фахівців у сфері виявлення та аналізу дезінформації, зберігаючи незалежність та неупередженість у виконанні

своїх завдань під керівництвом Виконавчої ради та незалежної Дорадчої ради

Діяльність EDMO зосереджена на кількох стратегічних напрямках, що мають безпосереднє значення для захисту виборчого процесу. Організація забезпечує функціонування безпечної онлайн-платформи для академічного аналізу дезінформаційних кампаній та надання публічної інформації для підвищення обізнаності щодо дезінформації. EDMO проводить навчальні заходи з різних тем, пов'язаних із дезінформацією, для відповідних зацікавлених сторін, включаючи фактчекерів, дослідників, журналістів та політиків. Також організація підтримує та сприяє координації незалежної діяльності з перевірки фактів у Європі у тісному зв'язку з національними хабами EDMO [40].

EDMO займається підтримкою та координацією академічних дослідницьких заходів з питань дезінформації в Європі, зокрема створенням репозиторію відповідної рецензованої наукової літератури. На основі досліджень та аналізу організація надає рекомендації європейським інституціям та урядам щодо дотримання платформами соціальних медіа Кодексу практики протидії дезінформації. EDMO також забезпечує підтримку державним органам у моніторингу заходів, вжитих онлайн-платформами для обмеження поширення та впливу дезінформації, та проактивно пропонує відповідним органам науково обґрунтовані рішення [40]. Важливим напрямком роботи EDMO є створення рамкової основи для забезпечення безпечного доступу до даних онлайн-платформ для дослідницьких цілей та виявлення і пом'якшення загроз здоровому онлайн-інформаційному середовищу.

Центральну роль у моніторингу аудіовізуального контенту відіграє Група європейських регуляторів аудіовізуальних медіа-послуг ERGA, створена згідно з статтею 30b(1) [24] Директивою про аудіовізуальні медіа-послуги N 2010/13/EU для забезпечення узгодженого впровадження нормативно-правової бази ЄС у сфері аудіовізуальних медіа [24]. До складу ERGA входять представники національних регуляторних органів або органів у сфері аудіовізуальних медіа-послуг, які мають основну відповідальність за нагляд за цими послугами [24,

стаття 30b(2)]. В контексті виборів ERGA здійснює моніторинг виконання платформами своїх зобов'язань щодо маркування політичного контенту. Важливість цієї інституції підкреслюється і в European Democracy Action Plan, де Комісія визначила ERGA як одного з ключових партнерів у реалізації стандартів медіаграмотності, передбачених статтею 33а Директиви N 2010/13/EU [4].

Особливо важливою є роль ERGA у координації між країнами-членами, оскільки вона забезпечує співпрацю та надає своїм членам інформацію, необхідну для застосування Директиви [24, стаття 30b(3)(c)]. У контексті протидії дезінформації ERGA надає висновки на запит Комісії щодо технічних та фактичних аспектів питань відповідно до статей Директиви, що стосуються юрисдикції, порушень та правил загального суспільного інтересу [6, стаття 30b(3)(d)]. Ця функція є критично важливою для оперативного реагування на транскордонні випадки поширення дезінформації під час виборчих кампаній, коли маніпулятивний контент може одночасно поширюватися у декількох юрисдикціях.

Регламент ЄС 2024/900 про прозорість політичної реклами суттєво розширив інституційний інструментарій ЄС у сфері захисту виборів. Стаття 15 Регламенту передбачає створення Європейського репозиторію для онлайн-політичної реклами, який адмініструється Європейською Комісією [36, п. 64]. Цей механізм дозволяє здійснювати централізований аудит рекламних кампаній та покликаний забезпечити наглядові органи можливість ідентифікувати замовників реклами, що є критично важливим для виявлення прихованого фінансування з-за кордону та іноземного втручання у виборчі процеси.

Новим інституційним гравцем у цій архітектурі став Європейський офіс з питань штучного інтелекту AI Office, створений у межах Регламенту 2024/1689 контролювати моделі штучного інтелекту загального призначення [37]. У виборчий період AI Office співпрацює з Європейською радою з питань цифрових послуг European Board for Digital Services для оцінки того, як алгоритми рекомендацій на великих платформах можуть сприяти поширенню

dezінформації. Цей підхід підкріплюється Висновком Комісії 2025 року, який наголошує на важливості незалежного аудиту, згідно зі статтею 37 DSA, для перевірки виконання платформами своїх антиdezінформаційних зобов'язань [33].

Важливим елементом інституційної архітектури є також Постійна цільова група Permanent Task-force, передбачена Висновком Єврокомісії. Ця багатосторонній форум, що очолюється Комісією, включає підписантів Кодексу та представників EDMO, EEAS та ERGA. Цільова група отримала конкретні завдання, зокрема щодо створення системи швидкого реагування в період виборів та кризових ситуацій, а також щодо регулярного обговорення питання необхідності оновлення зобов'язань та заходів Кодексу з урахуванням технологічних, суспільних, ринкових та законодавчих змін [33, с. 4].

Слід також зазначити роль Європейської мережі співробітництва у сфері виборів European Cooperation Network on Elections, створеної у 2019 році напередодні виборів до Європейського Парламенту. Ця мережа забезпечує конкретний та практичний обмін інформацією з широкого кола тем, пов'язаних із забезпеченням вільних та чесних виборів, включаючи протидію dezінформації, кібербезпеку виборчої інфраструктури та онлайн-моніторинг [36, п. 100]. Мережа працює у тісній координації з Системою швидкого сповіщення та Групою співробітництва з мережної та інформаційної безпеки, що забезпечує комплексний підхід до захисту виборчих процесів від гібридних загроз.

Отже, інституційна модель ЄС трансформувалася в цілісну екосистему, де політична координація через RAS поєднується з аналітичними спроможностями EDMO, регуляторним наглядом ERGA, моніторингом політичної реклами на основі Регламенту 2024/900 та технологічним моніторингом з боку AI Office. Така багаторівнева структура забезпечує не лише виявлення dezінформації, а й юридичне примушування цифрових платформ до дотримання стандартів демократичного дискурсу. Водночас ця модель не позбавлена недоліків: критики вказують на ризики надмірного втручання держави в інформаційний простір, потенційну загрозу свободі слова та складність балансування між ефективною протидією маніпуляціям та збереженням демократичних свобод. Проте

загальний вектор розвитку інституційної архітектури ЄС свідчить про перехід до концепції активного захисту інформаційного суверенітету виборця як невід'ємної складової демократичного процесу.

Висновки до Розділу 2. Проведений аналіз регуляторної моделі ЄС щодо протидії дезінформації під час виборів дозволяє дійти до певних висновків. По-перше, еволюція правового регулювання протидії дезінформації в Європейському Союзі відображає послідовний перехід від концепції м'якого права та добровільних зобов'язань до комплексної системи жорсткого нормативного регулювання. Цей перехід відбувався поетапно: від Плану дій проти дезінформації 2018 року через Європейський план дій щодо демократії 2020 року до прийняття Акта про цифрові послуги (DSA), Регламенту про прозорість політичної реклами та Акта про штучний інтелект.

По-друге, концептуальне розуміння феномену дезінформації в європейському правовому просторі суттєво еволюціонувало. Від початкового визначення дезінформації як верифіковано неправдивої інформації ЄС перейшов до класифікації, що охоплює місінформацію, дезінформацію, операції з інформаційного впливу та іноземне втручання в інформаційний простір. Таке розмежування є важливим для розробки відповідних правових відповідей на різні типи загроз для виборчого процесу.

По-третє, сучасна інституційна система ЄС у сфері протидії дезінформації під час виборів є багаторівневою та заснованою на взаємодії множинних інституцій. Система швидкого сповіщення (RAS), Оперативна робоча група зі стратегічних комунікацій (ESTF), Європейська обсерваторія цифрових медіа та Європейський офіс з питань штучного інтелекту (AI Office) створюють систему моніторингу та реагування на дезінформаційні загрози. В той же час варто зауважити, що ефективність цієї системи залежить від належної координації між усіма її елементами, а також від готовності держав-членів ЄС імплементувати і дотримуватись відповідних стандартів на національному рівні. Досвід ЄС у побудові комплексної системи є надзвичайно цінним для країн, що

прагнуть вдосконалити власні механізми захисту виборчих процесів, зокрема для України.

РОЗДІЛ 3. ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРАВОВИХ МЕХАНІЗМІВ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯЦІЯМ В ОКРЕМИХ КРАЇНАХ

3.1. Правове регулювання Франції у сфері протидії дезінформації та інформаційним маніпуляціям

Основою французького законодавства у сфері регулювання інформаційного простору став Закон про свободу преси 1881 року від 29 липня 1881 року *Loi du 29 juillet 1881 sur la liberté de la presse*, стаття 27 якого встановлює кримінальну відповідальність за публікацію, поширення або відтворення неправдивих повідомлень, фабрикацій або документів, помилково приписаних третім особам, якщо такі дії, вчинені недобросовісно, порушили громадський спокій або були здатні його порушити. Санкція за це правопорушення сягає 45 000 євро штрафу [41].

Щодо дезінформації в контексті виборів, то в Кодексі виборчому Франції *Code électoral* у статті L. 97 встановлено спеціальну відповідальність за поширення неправдивих новин, недобросовісних чуток або наклепницьких заяв, що мають на меті відвернути виборців від голосування або зловмисно вплинути на голоси одного чи кількох виборців, а стаття L. 52-1 окремо забороняє використання у виборчих цілях, у трьох місяцях, що передують першому числу місяця проведення виборів, будь-якої комерційної реклами через пресу або будь-який засіб аудіовізуальної комунікації [42].

Виборчий кодекс Франції також містить регулювання прозорості виборчої агітації, зокрема стаття 163-1 передбачає перелік інформації, яку повинні надавати онлайн-платформи протягом трьох місяців перед виборами: інформацію про особу, яка оплачує розміщення контенту; інформацію про використання персональних даних; суму винагороди за просування інформаційного контенту. Вся інформація зібрана у єдиному реєстрі у відкритому доступі. За порушення правил прозорості передбачено ув'язнення до одного року або штраф 75 тисяч євро [42].

У відповідь на сучасні виклики щодо дезінформації та інформаційних маніпуляцій, Франція у 2018 році ухвалила Закон про маніпулювання інформацією (Loi n° 2018-1202). Його особливістю є фокус на онлайн-платформах та швидкому реагуванні під час виборчих періодів, зокрема відповідно до ч. 1 ст. 11 Закону, оператори онлайн-платформ повинні вживати заходів для боротьби з поширенням неправдивої інформації, яка може порушити громадський порядок або підірвати цілісність будь-яких виборів. Закон передбачає процедуру прискореного судового розгляду “référé” справ про неправдиву інформацію протягом 48 годин після подання позову, який має бути зареєстрований не пізніше трьох місяців з моменту публікації. Французькі суди мають дискреційні повноваження щодо обмеження поширення неправдивих новин протягом виборчого періоду, якщо вони широкомасштабно розповсюджуються та можуть негативно вплинути на результат виборів [43].

Другим важливим компонентом французької моделі є покладення на великі онлайн платформи обов'язку співпраці. Згідно зі статтями 11 та 13 закону 2018 року, оператори онлайн-платформ, які перевищують поріг у 5 мільйонів унікальних відвідувачів на місяць середньорічно, зобов'язані запровадити доступний для користувачів механізм повідомлення про неправдиву інформацію; призначити юридичного представника на території Франції; забезпечувати прозорість алгоритмів модерації контенту, оприлюднювати інформацію про спонсорський характер політичної реклами та щорічно подавати декларацію регулятору [43].

Значну роль у регулюванні інформаційного простору відіграє Autorité de аудіовізуальних медіа та захисту прав в інтернеті. Діяльність Arcom включає функції від протидії незаконному контенту та захисту неповнолітніх до моніторингу дотримання норм щодо виборчих кампаній [44].

Французький підхід піддавався критиці, переважно за надто розпливчате визначення неправдивої інформації та потенційну небезпеку приватної цензури з боку платформ, які матимуть стимул надмірно блокувати контент задля

уникнення санкцій, а французьку владу звинувачували у створенні так званої “поліції думок” (“thought police”), що може накладати обмеження на будь-який контент, який їй не подобається. [45].

3.2. Правове регулювання Німеччини у сфері протидії дезінформації та інформаційним маніпуляціям

Німеччина запровадила Закон про вдосконалення правозастосування в соціальних мережах *Netzwerkdurchsetzungsgesetz - NetzDG*, який створив механізми боротьби з протиправним вмістом, включаючи фейкові новини. Закон надавав повноваження видаляти з соціальних мереж різні види неправдивої або незаконної інформації. Прийняття закону стало реакцією на повільне реагування

Важливою категорією закону є поняття “протиправного контенту” (*rechtswidrige Inhalte*), яке § 1 абз. 3 *NetzDG* визначає не самостійно, а через перелік конкретних статей Кримінального кодексу Німеччини (*Strafgesetzbuch*, 130, 131, 140, 166, 184b, 185–187, 189, 201a, 241 та 269 *StGB*), що охоплюють зокрема: розповсюдження пропагандистських матеріалів неконституційних організацій (§ 86), використання символів неконституційних організацій (§ 86a), підготовку тяжких злочинів проти держави (§ 89a), публічні заклики до вчинення злочинів (§ 111), порушення громадського спокою шляхом погрози злочинами (§ 126), створення кримінальних та терористичних організацій (§§ 129-129b), розпалювання ненависті (*Volksverhetzung*, § 130), образу (§ 185), наклеп (§§ 186, 187), запламування пам’яті померлих (§ 189), погрози (§ 241) та підробку даних, що мають доказове значення (§ 269) [46].

NetzDG не створює нового матеріального правопорушення “дезінформації” чи “неправдивих новин”, а лише запроваджує процедуру оперативного видалення контенту, який уже й до прийняття закону був протиправним відповідно до загальних кримінальних норм.

Водночас слід зазначити, що серед перелічених складів немає окремої норми про “фейкові новини” як такі - частина потенційно дезінформаційного

контенту охоплюється статтями 186, 187 StGB (наклеп, поширення завідомо неправдивих відомостей, що ганьблять конкретну особу) лише за умови, що такі повідомлення спрямовані проти конкретної ідентифікованої особи. Чисто електоральна дезінформація неперсоніфікованого характеру, наприклад, неправдиві відомості про процедуру голосування, підрив довіри до інституцій, у переліку протиправних складів NetzDG прямо не фігурує.

Процедурний механізм закону, закріплений у §§ 2–3 NetzDG, передбачає три основні складові. По-перше, обов'язок звітування у статті 2, відповідно до якого провайдери соціальних мереж, які отримують протягом календарного року більше 100 скарг на протиправний контент, зобов'язані готувати німецькомовний звіт про роботу зі скаргами та публікувати його у Bundesanzeiger та на власному сайті піврічно, не пізніше ніж через місяць після завершення півріччя. Звіт має містити вичерпну інформацію щодо загальних зусиль провайдера, алгоритмів автоматичного розпізнавання, механізмів подання скарг, кількості одержаних скарг з уточненням за джерелом і підставою, персонального складу та кваліфікації працівників, які розглядають скарги, кількості скарг, що призвели до видалення контенту, з уточненнями за термінами реагування (24 години, 48 годин, тиждень, пізніше) та інших аспектів [46].

По-друге, обов'язок розробки ефективної процедури розгляду скарг відповідно до статті 3. Провайдер повинен забезпечити, щоб явно протиправний контент видалявся або до нього блокувався доступ протягом 24 годин після надходження скарги та будь-який інший протиправний контент видалявся, як правило протягом семи днів. Семиденний строк може бути перевищений, якщо рішення залежить від встановлення фактичних обставин або якщо провайдер передає рішення визнаному органу регульованого саморегулювання [46].

По-третє, відповідальність за порушення за статтею 4. Адміністративна відповідальність може наставати у вигляді штрафу до 5 мільйонів євро для самого провайдера, а у випадках, передбачених загальними нормами щодо відповідальності юридичних осіб, цей штраф може досягати ще вищих сум. Окремо передбачено штраф до 500 000 євро за певні менш тяжкі

правопорушення, такі як неналежне ведення звітності та невиконання вимог щодо процедур. Адміністративним органом, що здійснює контроль за виконанням закону, є Федеральне відомство юстиції (Bundesamt für Justiz) - саме воно уповноважене застосовувати штрафи. Адміністративна відповідальність може наставати, навіть якщо правопорушення не вчинене на території Німеччини

Однак документ викликав значну критику через можливість його використання як прецеденту для встановлення цензури у соціальних мережах авторитарними режимами. Human Rights Watch назвала закон недосконалим, стверджуючи, що він може призвести до невиправданої, надмірно широкої цензури та створить небезпечний прецедент [47]. “Репортери без кордонів” навіть зазначили, що німецький закон вплинув на впровадження Росією власного закону про мову ненависті [48]. Оксфордський інтернет-інститут застерігав, що закон може суттєво обмежити свободу вираження поглядів [49].

У червні 2017 року Девід Кей, Спеціальний доповідач ООН з питань захисту свободи думки та вираження поглядів, направив офіційного листа уряду Німеччини. Його основні зауваження включали: законопроект передбачав видалення інформації на підставі розмитих понять, що несумісно зі статтею 19 Міжнародного пакту про громадянські та політичні права; високі штрафи (до 50 мільйонів євро у Проекті Закону) були непропорційними; вимога видаляти контент протягом 24 годин створювала ризик “запобіжної цензури”; відповідальність за видалення контенту покладалася на приватні компанії без належного судового контролю; вимоги зберігати дані підривали право на анонімне вираження думок [50].

Поправками 2021–2022 років NetzDG було істотно вдосконалено: запроваджено інститут зустрічного подання (Gegenvorstellung) в § 3b, що надає як авторам контенту, так і скаржникам право оскаржити рішення про модерацію через спеціальну процедуру всередині платформи; розширено обов’язок повідомлення Федерального бюро кримінальної поліції (Bundeskriminalamt) про окремі категорії контенту, який містить ознаки тяжких злочинів; створено

спеціальний механізм адміністративного арбітражу для вирішення спорів між користувачами та платформами [46].

3.3. Правове регулювання Великої Британії у сфері протидії дезінформації та інформаційним маніпуляціям

Закон Сполученого Королівства про онлайн-безпеку 2023 року Online systemу регулювання діяльності постачальників онлайн-послуг, спрямовану на захист користувачів від шкідливого контенту [51]. Архітектура закону істотно відрізняється від континентальних європейських моделей. Британський закон передбачає підхід, орієнтований на “обов’язки турботи” (duties of care) та системне управління ризиками, що загалом нагадує конструкцію Регламенту ЄС 2022/2065 про цифрові послуги DSA, але водночас містить специфічні елементи, важливі для захисту виборчого процесу від маніпуляцій.

Сфера дії OSA охоплює дві основні категорії: “регульовані послуги

к
о
р
и
с
т

у Закон передбачає створення спеціального дорадчого комітету з питань дезінформації та місінформації в рамках OFCOM. Основними функціями комітету є надання консультацій щодо методів протидії дезінформації, реалізації нововажень вимагати інформацію та виконання функцій популяризації медіаграмотності. Закон передбачає диференційований підхід: цільовими об’єктами є випадки, коли дезінформація є протиправною за змістом, завдає шкоди дітям та/або є профінансованою іншою державою, підпадаючи під Злочин іноземного втручання [51].

р Важливим доповненням став National Security Act 2023, який запровадив злочини іноземного втручання у вибори, встановив визначення іноземної влади,

с
т

посилив покарання за шпигунство та саботаж, пов'язані з іноземною владою, та запровадив Систему реєстрації іноземного впливу (Foreign Influence Registration). Міхалевська К., Романюк П.]. На політичному рівні у 2022 році створено Робочу групу із захисту демократії (Defending Democracy Taskforce), яка координує зміцнення виборчої інфраструктури та протидію іноземним інформаційним операціям [26].

3.4. Досвід Нідерландів у протидії дезінформації та інформаційним маніпуляціям

Королівство Нідерланди обрало модель, що ґрунтується переважно на саморегулюванні та м'якому праві, на відміну від жорстких законодавчих підходів інших держав-членів ЄС. Цей підхід базується на низці чинників: відсутність значних інцидентів дезінформаційного характеру у виборчій історії країни, традиційно високий рівень довіри до виборчого процесу та висока явка виборців на національних виборах.

Центральним документом цієї моделі є Нідерландський Кодекс поведінки щодо прозорості онлайн-політичної реклами (Dutch Code of Conduct Transparency Online Political Advertisements), розроблений Міжнародним інститутом демократії та сприяння виборам (International IDEA) у консультаціях з політичними партіями, представленими в Палаті представників Нідерландів, та онлайн-платформами на запит Міністерства внутрішніх справ та зв'язків з Королівством [52].

Правова природа Кодексу полягає в добровільних правилах поведінки. Документ прямо передбачає, що участь є добровільною та не може замінити чинне або майбутнє законодавство. Водночас, як зазначається в самому документі, це не виключає того, що Кодекс виконує важливу сигнальну функцію та апелює до індивідуальної відповідальності політичних партій та онлайн-платформ за сумлінне виконання їхніх спільних та окремих обов'язків [52]. Така конструкція є типовою для нідерландської правової традиції, що віддає перевагу довірі та діалогу, а не формальним санкціям.

Кодекс охоплює дві категорії суб'єктів: онлайн-платформи та політичні партії, зареєстровані для виборів. Сферою регулювання є переважно платна онлайн-політична реклама, проте Кодекс частково охоплює і неоплачуваний, так званий “органічний”, контент, оскільки його роль для чесних та демократичних онлайн-кампаній не менша, а відсутність прозорості щодо того, хто розміщує і поширює органічний контент, також є релевантною [52].

Зобов'язання, які беруть на себе обидві категорії підписантів, поділяються на три групи. Перша - спільні зобов'язання відповідно до статті 3.1 Кодексу: відповідальне використання онлайн-політичної реклами для збереження цілісності виборів, сприяння та дотримання прозорості онлайн-політичної реклами та уникнення поширення оманливого контенту, мови ворожнечі та повідомлень, що підбурюють до насильства [52].

Друга група - зобов'язання політичних партій відповідно до пункту 3.2:

- суворе дотримання рекламних політик платформ та надання правдивої інформації для процедур реєстрації та верифікації;
- підтримання етичних меж щодо поєднання різних наборів даних та їх завантаження на платформи з метою мікротаргетингу;
- утримання від психологічного профілювання для цілей таргетингу;
- утримання від використання посередників для розміщення політичної реклами без атрибуції до партії;
- відмова від прямої купівлі політичної реклами іноземними суб'єктами на підтримку партії та утримання від отримання іноземного фінансування для оплати онлайн-політичної реклами (за винятком отриманого від членів партії, що проживають за кордоном);
- утримання від неетичної онлайн-поведінки, такої як поширення контенту з метою відмови виборців від голосування, дезінформації про процес голосування, використання фальшивих акаунтів або автоматичних ботів для маніпулювання думкою виборців, тролінгу, безпідставних звинувачень або кібербулінгу; утримання від навмисного розміщення, поширення або просування оманливого контенту; утримання від використання

спотворених аудіовізуальних повідомлень, включаючи дипфейки; утримання від поширення контенту, що підбурює до насильства або є мовою ворожнечі [52].

Третя група - зобов'язання онлайн-платформ (пункт 3.3 Кодексу), що мають найбільш розгалужений характер. Вони включають:

- розробку та впровадження відповідних механізмів прозорості;
- надання деталей про рекламодавців та рекламу в публічно доступних бібліотеках з можливістю легкого завантаження та порівняння даних;
- обов'язкову реєстрацію та верифікацію політичних рекламодавців; адекватне та чітке звітування щодо “оплачено за” (paid for by) та діапазону витрат;
- заборону транскордонної політичної реклами з-поза меж Європейського Союзу; встановлення прозорості щодо онлайн-політичної реклами, включно з обсягами витрат та охопленням;
- впровадження зручного для користувачів механізму реагування на запити; розробку та впровадження політик платформ щодо безпеки та приватності користувачів і виборчої цілісності;
- видалення політичної реклами або будь-якого контенту, що підбурює до насильства чи є мовою ворожнечі, у найкоротший можливий період після виявлення; протидію будь-якій неточній інформації про виборчий процес (інформації про виборців, процес голосування та виборчі дільниці);
- поширення досвіду з попередніх виборів в інших країнах; проведення післявиборчого огляду нідерландської виборчої кампанії та дотримання Кодексу [52].

Нідерландський Кодекс став першим подібним у ЄС. Напередодні виборів 2021 року 11 із 13 парламентських партій та платформ (Facebook, Google, Snapchat, TikTok) взяли зобов'язання щодо прозорості, включно із заборонаю поширення політичної реклами з-поза меж ЄС та реєстрацією політичних акторів-рекламодавців [8, с. 18].

Основною слабкою стороною нідерландського підходу є обмежена сила добровільного дотримання за відсутності реальних санкцій, оскільки Кодекс прямо визнає, що його дотримання не може забезпечуватися примусово.

Крім того, в умовах транскордонного впливу цифрових платформ та електоральних маніпуляцій національне саморегулювання має обмежений ефект. Але з впровадженням Акту про цифрові послуги DSA та Регламенту про прозорість і таргетування політичної реклами на рівні ЄС нідерландський підхід отримує інституційне підкріплення, що усуває частину його недоліків.

3.5. Досвід Литви та Латвії у протидії дезінформації та інформаційним маніпуляціям

Литва як країна Балтійського регіону має особливе значення в контексті європейських практик протидії дезінформації. Специфіка литовського досвіду полягає у випереджальному характері реагування на проблему дезінформації. Балтійські країни, включно з Латвією, ще до подій 2014 року в Україні усвідомлювали загрози, пов'язані з дезінформаційними кампаніями, хоча їхні застереження рідко знаходили розуміння серед інших членів ЄС [53, с. 1542]. Латвія та Литва належали до категорії країн, які ініціювали та активно підтримували розвиток спільних контрзаходів на рівні ЄС.

У січні 2015 року Литва разом з Естонією, Данією та Великою Британією представила документ під назвою “EU Strategic Communication Responding to дезінформації Росії [54].

Балтійський підхід до протидії дезінформації ґрунтується на розумінні цього явища як реальної загрози безпеці. Країна активно використовувала свій досвід та експертизу для переконання інших держав ЄС у необхідності колективних дій. Особливістю литовського підходу можна вважати поєднання заходів національного рівня з активним просуванням ініціатив на загальноєвропейському рівні.

На національному рівні Литва реалізувала низку заходів щодо обмеження впливу російських медіа. Литовська влада вдавалася до закриття російських медіа-платформ, таких як Sputnik [55].

Спільно з іншими балтійськими країнами Латвія долучилася до створення Оперативної робочої групи зі стратегічних комунікацій East StratCom Task Force, надавши своїх експертів. Ця ініціатива мала на меті протидію дезінформації, спрямованій проти ЄС, особливо тій, що походила з Росії. Латвія була серед країн, які фінансували роботу групи через направлення національних експертів. Важливим аспектом литовського досвіду є розуміння обмежень, які накладаються європейським законодавством щодо свободи слова та преси. Як і інші балтійські держави, Литва усвідомила необхідність спільного європейського підходу до протидії дезінформації, оскільки національні інструменти виявлялися недостатніми через міжнародну природу загрози [53, с. 1543].

Литовський та латвійський підхід демонструє важливість тісної співпраці між різними інституціями ЄС. Представники Латвії координували свої дії з партнерами в Раді ЄС, Європейському парламенті та ESTF для досягнення спільної мети - посилення протидії дезінформації в країнах Балтії та ЄС загалом , с. 1547-1548].

3.6. Правове регулювання Іспанії у сфері протидії дезінформації та інформаційним маніпуляціям

Королівство Іспанія є цікавим прикладом непрямого підходу до регулювання дезінформації через загальне аудіовізуальне законодавство. Закон 13/2022 від 7 липня 2022 року про загальну аудіовізуальну комунікацію Ley виконання Директиви 2010/13/ЄС в редакції Директиви ЄС 2018/1808, не містить спеціальних норм про електоральну дезінформацію, проте включає декілька положень, релевантних для протидії інформаційним маніпуляціям [56]. Стаття 99 Закону прямо передбачає захист користувачів щодо дезінформації (Protección de los usuarios respecto de la desinformación) як один з обов'язкових принципів діяльності постачальників послуги обміну відео через платформу [56]. Стаття 10

Закону покладає на компетентний аудіовізуальний орган Comisión Nacional de los postales providers of services exchange video obligations to take measures for the development of media literacy in all sectors of society, which have the goal of development of competencies, which allow citizens to use media with effectiveness and security, obtain access and critically analyze information, distinguish facts from opinions, recognize false news and disinformation processes [56].

Законом також було введено термін “користувачі, що мають особливе значення”. Це особи, що публікують відео на платформах спільного доступу з метою поширення контенту, мають редакційний контроль над таким контентом та для яких ця діяльність становить основну або значну частину доходу. Королівським декретом 444/2024 від 30 квітня 2024 року встановлено конкретні критерії: отримання доходу не менше 300 000 євро за попередній рік, наявність не менше 1 000 000 підписників або 2 000 000 на декількох платформах, публікація не менше 24 відео за рік [57].

Стаття 124 Закону 13/2022 окремо регулює аудіовізуальні комерційні комунікації, пов'язані з низкою чутливих сфер, серед яких прямо названі політична участь і виборча пропаганда (Participación política y propaganda]. Окремою підставою для виключення зі сфери дії норм про комерційну комунікацію визначено діяльність, що впливає з Органічного закону 5/1985 від 19 червня про загальний виборчий режим, тобто власне виборча агітація має регулюватися спеціальним виборчим законодавством, а не загальним аудіовізуальним законом [56]. Іспанська модель тим самим демонструє розмежування між загальною медіарегуляцією, до сфери якої входить протидія дезінформації як соціальному явищу, та виборчим правом, що залишається автономною галуззю.

3.7. Правове регулювання Сінгапуру у сфері протидії дезінформації та інформаційним маніпуляціям

Закон про захист від онлайн-неправдивостей та маніпуляцій 2019 року - Парламентом Сінгапуру 8 травня 2019 року і він набрав чинності 2 жовтня 2019 року [57]. Закон спрямований на запобігання електронному поширенню в Сінгапурі неправдивих заяв про факти, протидію використанню онлайн-акаунтів для такої комунікації та інформаційних маніпуляцій, а також на посилення прозорості онлайн-політичної реклами [58].

Стаття 7 POFMA встановлює широку юрисдикційну рамку: особа не повинна вчиняти жодних дій ні в Сінгапурі, ні поза ним з метою комунікації в Сінгапурі заяви, знаючи або маючи підстави вважати, що це є неправдою, і що така комунікація може: бути шкідливою для безпеки Сінгапуру; впливати на публічне здоров'я, безпеку, спокій або фінанси; шкодити дружнім відносинам з іншими країнами; вплинути на результат виборів Президента, загальних або проміжних виборів депутатів Парламенту, або референдуму; підбурювати до ворожнечі між різними групами осіб; зменшувати громадську довіру до виконання обов'язків урядом, органом держави або статутним органом [58]. Санкція за порушення статті 7 для індивіда становить штраф до 50 000 сінгапурських доларів або позбавлення волі до 5 років, або обидва види санкцій; для юридичних осіб - штраф до 1 мільйона сінгапурських доларів [58].

Ключовим інструментом POFMA є “Вказівка про виправлення” (Correction Direction), що зобов'язує особу, яка поширила неправдиве твердження, розмістити коригувальне повідомлення, яке прямо вказує, що раніше опубліковану інформацію ідентифіковано як неправдиву; при цьому Вказівка не вимагає видалення оригінальної неправдивої публікації - вона співіснує з виправленням [57]. У більш серйозних випадках застосовується “Вказівка про припинення комунікації” (Stop Communication Direction) - наказ про припинення доступу до неправдивого контенту [57]. Технологічні компанії можуть отримати наказ про блокування акаунтів, що поширюють неправдиві відомості. Уповноваженим органом, що видає такі вказівки, є будь-який міністр уряду Сінгапуру, що становить характерну особливість моделі та водночас її головну

вразливість, оскільки рішення приймається виконавчою владою, а не судом [57]. Опозиційні політики, правозахисні організації, журналісти й науковці неодноразово критикували Закон за надмірне зосередження повноважень у руках виконавчої влади [59].

Висновки до Розділу 3. Порівняльно-правовий аналіз механізмів протидії дезінформації та маніпуляціям у виборчому процесі окремих країн дозволяє виокремити низку концептуально відмінних моделей правового регулювання та зробити такі висновки.

Французька модель характеризується поєднанням механізмів кримінальної та виборчої відповідальності за поширення неправдивої інформації, закладених ще Законом про свободу преси 1881 року та статтями L. 97 і L. 52-1 Виборчого кодексу Франції, з сучасним Законом про маніпулювання інформацією 2018 року (Loi n° 2018-1202). Особливістю французького підходу є фокус на онлайн-платформах та швидкому реагуванні: запровадження прискореної судової процедури *référé* з розглядом справи протягом 48 годин, обов'язків платформ із порогом понад 5 мільйонів унікальних відвідувачів щодо механізмів повідомлення про неправдиву інформацію, прозорості алгоритмів модерації та призначення юридичного представника у Франції.

Німецька модель, втілена у Законі про вдосконалення правозастосування в соціальних мережах NetzDG, який не створює нового правопорушення дезінформації, а запроваджує лише процедуру оперативного видалення контенту, протиправного відповідно до загальних кримінальних норм. Закон встановлює перелік складів злочинів за *Strafgesetzbuch*, що становлять “протиправний контент”, обов'язки звітування для платформ із понад 100 скаргами на рік, видалення явно протиправного контенту протягом 24 годин та адміністративну відповідальність до 5 мільйонів євро. Поправками 2021-2022 років модель було вдосконалено через інститут зустрічного подання та механізм адміністративного арбітражу.

Водночас варто зауважити, що і законодавство Німеччини, і Франції піддавались суттєвій критиці з боку правозахисників через ризики цензури,

розпливчасті визначення неправдивої інформації та ризику надмірного видалення контенту.

Британська модель, закріплена у Законі про онлайн-безпеку 2023 року ризиками, що нагадує правову конструкцію DSA, в цьому випадку робиться акцент на захисті виборчого процесу саме від іноземного втручання.

Нідерландська модель, на відміну від попередніх, заснована переважно на саморегулюванні та м'якому праві. Кодекс охоплює дві категорії суб'єктів, онлайн-платформи та політичні партії, та передбачає три групи зобов'язань: спільні зобов'язання щодо відповідального використання політичної реклами, зобов'язання політичних партій щодо утримання від мікротаргетингу на основі психологічного профілювання та використання дипфейків та найбільш розгалужені зобов'язання онлайн-платформ. Однак основною слабкою стороною є обмежена сила добровільного дотримання за відсутності реальних санкцій.

Литовська модель вказує на підхід, заснований на сприйнятті дезінформації як загрози національній безпеці. Її особливістю є поєднання заходів національного рівня, зокрема обмеження діяльності російських медіаплатформ на кшталт Sputnik, з активним просуванням колективних ініціатив на рівні ЄС, насамперед через спільну з Естонією, Данією та Великою Британією пропозицію “EU Strategic Communication Responding to Propaganda” 2015 року та участь у East StratCom Task Force. Литовський досвід засвідчує, що для країн, які стикаються з постійним зовнішнім інформаційним тиском, такі як Україна, національні інструменти є недостатніми, що зумовлює необхідність вбудовування їх у спільну європейську архітектуру протидії дезінформації.

Іспанська модель є прикладом непрямого підходу до регулювання дезінформації через загальне аудіовізуальне законодавство. Закон 13/2022 про загальну аудіовізуальну комунікацію не містить спеціальних норм про електоральну дезінформацію, проте передбачає у статті 99 захист користувачів від дезінформації як обов'язковий принцип діяльності постачальників послуг обміну відео, а у статті 10 - обов'язок розвитку медіаграмотності. Окрему увагу

варто приділити свідомому розмежуванню між загальною медіарегуляцією та виборчим правом, яке залишається автономною галуззю.

Сінгапурська модель протидії, втілена у Законі про захист від онлайн-неправдивостей та маніпуляцій 2019 року, є найбільш жорсткою серед розглянутих та передбачає широку юрисдикційну рамку, спеціалізовані інструменти у вигляді Вказівки про виправлення (Correction Direction) і Вказівки про припинення комунікації (Stop Communication Direction), а також значні санкції у вигляді штрафу до 1 мільйона сінгапурських доларів для юридичних осіб. Водночас ключовою вразливістю моделі є зосередження повноважень з винесення таких вказівок у руках виконавчої влади, а не суду.

РОЗДІЛ 4. ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ У ВИБОРЧОМУ ПРОЦЕСІ УКРАЇНИ: СТАН ТА НАПРЯМИ ВДОСКОНАЛЕННЯ

4.1. Стан українського законодавства: аналіз Виборчого кодексу та Закону України “Про медіа” щодо регулювання агітації в інтернеті, протидії дезінформації та інформаційним маніпуляціям

Правові механізми протидії дезінформації у виборчому процесі України формуються на перетині декількох законодавчих актів, кожен з яких регулює окремі аспекти виборчої комунікації та інформаційного простору. Ключовими серед них є Виборчий кодекс України від 19 грудня 2019 року № 396-ІХ та Закон України “Про медіа” від 13 грудня 2022 року № 2849-ІХ. Разом з тим, як свідчить аналіз цих документів, чинне законодавство залишається орієнтованим переважно на регулювання традиційних медіа, і значною мірою не враховує специфіки цифрового інформаційного простору та пов’язаних з ним загроз для виборчого процесу.

Виборчий кодекс України закріплює принцип рівного виборчого права, який у контексті інформаційного простору конкретизується через вимогу рівного та неупередженого ставлення засобів масової інформації та інформаційних агентств до кандидатів і партій - суб’єктів виборчого процесу відповідно до ч. 5 ст. 12 [60]. Крім того, стаття 12 зобов’язує ЗМІ здійснювати інформування про перебіг виборчого процесу "на засадах збалансованості, достовірності, повноти і точності, об’єктивності поширюваної інформації". Ці положення є базовими стандартами для регулювання виборчих комунікацій, однак не передбачають конкретних механізмів для боротьби з маніпулятивним контентом у соціальних мережах та на цифрових платформах.

Особливого значення у контексті протидії дезінформації набуває стаття 49 Виборчого кодексу, яка регулює участь засобів масової інформації та інформаційних агентств в інформаційному забезпеченні виборів. Відповідно до частини 2 цієї статті, ЗМІ зобов’язані поширювати повідомлення про перебіг виборчого процесу, базуючись на засадах достовірності, повноти і точності,

об'єктивності та неупередженого подання, не допускаючи перекручування інформації. При цьому вимога отримувати інформацію “з двох і більше джерел, віддаючи перевагу першоджерелам” є важливим стандартом журналістської верифікації. Нагляд за дотриманням цих вимог здійснює Національна рада України з питань телебачення і радіомовлення щодо аудіовізуальних ЗМІ.

Суттєвий правовий механізм закріплений у статті 50 Виборчого кодексу, присвяченій особливостям поширення результатів опитування громадської думки. Частина 1 зобов'язує організації, що проводять опитування, зазначати час проведення, охоплення, розмір та спосіб формування вибірки, метод опитування, точне формулювання запитань, статистичну похибку та замовників. Ці вимоги відповідають стандартам Рекомендації CM/Rec(2022)12 Комітету міністрів Ради Європи та спрямовані проти маніпулятивних опитувань, які, як зазначають А. Людва та М. Дворовий, мають здебільшого негативний вплив у пострадянських країнах, де маніпуляція думкою часто виражена через приховування замовників досліджень [8, с. 28].

Важливою для розуміння обсягу правового регулювання передвиборної агітації є стаття 51 Виборчого кодексу, що визначає форми та засоби такої агітації. Серед передбачених форм пункт 4 частини 1 вказує на оприлюднення в друкованих та аудіовізуальних (електронних) засобах масової інформації політичної реклами, виступів, інтерв'ю, нарисів, відеофільмів, аудіо- та відеокліпів, інших публікацій та повідомлень. Разом з тим Кодекс не передбачає спеціального регулювання для цифрових платформ, зокрема соціальних мереж та месенджерів, які сьогодні стали одними з домінуючих середовищ для поширення передвиборної агітації та дезінформації. Частина 5 статті 51 встановлює заборону на приховану передвиборну агітацію та розміщення незамаркованих агітаційних матеріалів, однак механізм контролю за виконанням цих вимог у цифровому просторі залишається без чіткого врегулювання [60].

Стаття 57 Виборчого кодексу встановлює обмеження щодо ведення передвиборної агітації, серед яких частина 5 прямо забороняє поширення завідомо неправдивих відомостей про кандидата, партію або організацію партії -

суб'єктів виборчого процесу. При цьому встановлено обов'язок засобу масової інформації надати право на спростування не пізніш як через три дні після оприлюднення. Ця норма є важливим, однак вузьким антидезінформаційним механізмом, оскільки поширюється лише на відомості про конкретних кандидатів, не охоплюючи системних дезінформаційних наративів щодо виборчого процесу загалом, а також не регулює поширення неправдивих відомостей поза виборчим фондом.

Закон України “Про медіа” від 13 грудня 2022 року є більш сучасним нормативним актом, що адаптує українське законодавство до стандартів Директиви ЄС 2018/1808/EU. Він вводить поняття “онлайн-медіа” (ст. 1 п. 36), “платформа спільного доступу до відео” (ст. 1 п. 38) та “платформа спільного доступу до інформації” (ст. 1 п. 39), тим самим розширюючи регуляторне охоплення на цифровий інформаційний простір [61]. Це є суттєвим кроком вперед порівняно з попереднім законодавством, що регулювало лише традиційні ЗМІ.

Водночас частина 4 статті 2 Закону “Про медіа” визначає важливе розмежування: “Особливості діяльності суб'єктів у сфері медіа щодо агітації та інформування у період проведення виборів і референдумів регулюються законодавством про вибори та референдуми, крім здійснення Національною радою повноважень щодо нагляду та контролю у період проведення виборів та референдумів у порядку, визначеному цим Законом” [61]. Це означає, що Закон “Про медіа” відповідає Виборчого кодексу щодо агітаційної діяльності медіа у виборчий період, водночас зберігаючи контрольні повноваження Національної ради.

Важливою нормою Закону “Про медіа” є стаття 4, яка проголошує принципи свободи діяльності у сфері медіа та встановлює, що будь-які обмеження зазначених свобод можуть бути встановлені лише на підставі закону, якщо це є необхідним у демократичному суспільстві, і є пропорційним щодо поставленої мети. При цьому частина 2 статті 4 прямо посилається на практику Європейського суду з прав людини як джерело права при впровадженні обмежень

у сфері медіа [60]. Це є важливим конституційним орієнтиром для розробки антидезінформаційного законодавства з урахуванням стандартів свободи вираження поглядів.

Стаття 5 Закону “Про медіа” визначає основні завдання державної політики у сфері медіа, серед яких особливо значимими є забезпечення достовірності та збалансованості подання інформації, гарантування вільного і відкритого обговорення суспільно важливих проблем, захист користувачів інформації, а також забезпечення ефективного нагляду за дотриманням вимог і обмежень у сфері медіа з метою захисту національного медіапростору від актуальних загроз інформаційній безпеці відповідно до п. 15 ч. 1 ст. 5 [61]. Останнє положення є прямим визнанням загроз інформаційній безпеці на рівні законодавства, що створює правову основу для розбудови відповідних механізмів.

Важливим регуляторним елементом є розширення юрисдикції Закону “Про медіа” на провайдерів платформ спільного доступу до відео, які не зареєстровані у державах - членах ЄС за ч. 12 ст. 2 [61]. При цьому частина 13 статті 2 поширює дію Закону на іноземні аудіовізуальні, друковані та онлайн-медіасервіси, якщо вони “спрямовані на територію та аудиторію України” [61]. Ці норми є відповіддю на проблему іноземного втручання через цифрові платформи, яка є особливо актуальною для України в умовах повномасштабного інформаційного протистояння з Російською Федерацією.

Закон України “Про медіа” передбачає, що користувачі платформ спільного доступу не є суб’єктами онлайн-медіа, крім випадків добровільної реєстрації. Як наслідок, особа може поширювати інформацію на значну аудиторію, не підпадаючи під встановлені для медіа обов’язки та обмеження. В умовах війни такі канали можуть використовуватися для розповсюдження дезінформації, прихованої російської пропаганди чи вигідних для агресора наративів. Визнання користувачів з великим впливом суб’єктами онлайн-медіа було б найоптимальнішим варіантом правового врегулювання, оскільки це адекватно відображало б ключову роль цих суб’єктів у медіаспоживанні українців [20, с.

Загалом, аналіз чинного законодавства вказує на низку системних недоліків у правовому регулюванні протидії дезінформації у виборчому процесі. По-перше, ані Виборчий кодекс, ані Закон “Про медіа” не містять визначення дезінформації як окремого правового поняття у виборчому контексті, що унеможлиблює чітке встановлення юридичних наслідків її поширення. По-друге, правове регулювання передвиборної агітації в інтернеті носить фрагментарний характер, оскільки законодавство не передбачає механізмів маркування та верифікації інтернет-агітації, вимог щодо прозорості онлайн-реклами на зразок тих, що запровадив Регламент ЄС 2024/900. По-третє, ані Виборчий кодекс, ані Закон “Про медіа” не регулюють використання алгоритмів і технологій мікротаргетингу у виборчих кампаніях, хоча саме вони становлять ключовий інструмент маніпулятивного впливу на виборців [8, с. 15-17]. По-четверте, відсутня правова основа для встановлення відповідальності цифрових платформ, соціальних мереж та месенджерів, за поширення дезінформаційного контенту під час виборів.

Підсумовуючи викладене, чинне законодавство України у сфері політичної реклами та агітації є застарілим і не враховує роль онлайн-інструментів. Виборчий кодекс України регулює лише загальні питання, пов’язані з розміщенням політичної реклами. Вона має бути відокремлена від інших матеріалів і позначена, а опитування громадської думки мають публікуватися із зазначенням часу проведення, території охоплення, розміру вибірки, методу опитування та замовників. Однак онлайн-медіа та онлайн-платформи фактично не підпадають під дію вимог Кодексу, що створює широкий простір для маніпуляцій та зловживань. Роль цифрових технологій у майбутньому лише зростатиме, тому вже сьогодні слід впроваджувати відповідні законодавчі зміни.

4.2. Інституційні механізми протидії дезінформації в Україні

Інституційна архітектура протидії дезінформації у виборчому процесі України включає кілька ключових суб’єктів, повноваження яких у відповідній сфері визначені чинним законодавством. Однак, на відміну від моделей ЄС, ця

система характеризується розпорошеністю повноважень та відсутністю єдиного центру, що обмежує її ефективність.

Центральна виборча комісія (ЦВК) є основним органом, що відповідає за адміністрування виборчого процесу. Відповідно до Виборчого кодексу, ЦВК здійснює контроль за дотриманням законодавства про вибори, зокрема в частині передвиборної агітації. У контексті інформаційних загроз стаття 49 Кодексу покладає на ЦВК обов'язок отримувати від Національної ради та органів виконавчої влади інформацію про виявлені порушення правил інформаційного забезпечення виборів. Разом з тим у системі повноважень ЦВК відсутні інструменти для безпосереднього моніторингу та реагування на дезінформацію в мережі Інтернет.

Національна рада України з питань телебачення і радіомовлення є спеціалізованим медіарегулятором, повноваження якого у виборчий період визначені як Виборчим кодексом, так і Законом “Про медіа”. Відповідно до ч. 4 статті 49 Виборчого кодексу, Національна рада здійснює нагляд за дотриманням вимог в частині участі електронних (аудіовізуальних) засобів масової інформації в інформаційному забезпеченні виборів та при проведенні передвиборної агітації. При цьому в разі виявлення порушень Рада інформує відповідні виборчі комісії та вживає заходів, передбачених законодавством. Закон України “Про медіа” розширив повноваження Ради до сфери онлайн-медіа та платформ спільного доступу до відео, що є кроком у напрямку охоплення цифрового виміру дезінформації.

Певну роль у формуванні інституційної відповіді на цифрові виклики у виборчому процесі відіграє Міністерство цифрової трансформації України, яке відповідає за розробку державної політики у сфері цифровізації, зокрема питань штучного інтелекту. Як зазначається в аналітичному документі IFES, присвяченому адаптації законодавства ЄС у сфері штучного інтелекту до виборчих процесів, Міністерство цифрової трансформації, ЦВК та громадянське суспільство мають розробляти стратегії протидії та, за потреби, використання ШІ

для забезпечення вільних, чесних і безпечних виборів в Україні в повоєнний період [16, с. 7].

Суспільне значення для виявлення дезінформаційних кампаній в Україні відіграє громадянське суспільство, як і в багатьох інших країнах. Як зазначають А. Людв та М. Дворовий у звіті ГО “Лабораторія цифрової безпеки”, яскраві приклади маніпуляції з результатами соціологічних опитувань без зазначення замовників були виявлені під час місцевих виборів в Україні 2020 року [8, с. 28].

Незважаючи на наявність зазначених інституцій, система протидії дезінформації у виборчому процесі України має суттєві недоліки. По-перше, відсутній єдиний координаційний механізм для оперативного обміну даними між інституціями та державами-членами. По-друге, жодна з існуючих інституцій не має повноважень та технічного потенціалу для проведення системного моніторингу дезінформації в соціальних мережах та на цифрових платформах у реальному часі. Однак можна зауважити, що в Україні існують громадські організації на зразок Європейської обсерваторії цифрових медіа, які об’єднують дослідників та фактчекерів для комплексного аналізу дезінформаційних загроз, зокрема і у виборчому процесі.

Порівняння інституційних можливостей України з аналогічними структурами в ЄС, зокрема East StratCom Task Force, EDMO та ERGA, дозволяє дійти висновку, що Україна потребує формування розгалуженої міжінституційної платформи протидії дезінформації, яка б поєднувала повноваження державних органів у примусовому припиненні дезінформації та притягненні до відповідальності, аналітичний потенціал академічних установ та практику фактчекінгу громадянського суспільства.

4.3. Напрями вдосконалення правового регулювання протидії дезінформації у виборчому процесі

Вдосконалення правового регулювання протидії дезінформації у виборчому процесі України є нагальним і складним завданням, яке вимагає системного підходу та врахування як міжнародних стандартів і досвіду ЄС, так і специфічних умов повоєнного відновлення. Як зауважує К. Філіпчук, потрібна

комплексна стратегія, яка б захищала виборчі права та виборчі процедури від впливу цифрового суспільства з її проявами кібератак та дезінформації [5, с. 291].

Першим і ключовим напрямом є нормативне визначення дезінформації у виборчому праві. Чинний Виборчий кодекс оперує лише поняттям “завідомо неправдивих відомостей” відповідно до ст. 57 ч. 5, що є вузьким і не охоплює системних форм маніпуляції інформаційним простором. Необхідно запровадити у Виборчий кодекс визначення дезінформації, аналогічне тому, що сформульоване у Плані дій ЄС проти дезінформації: верифіковано неправдива або оманлива інформація, що створюється та поширюється з метою навмисного введення в оману громадськості, яка може завдати суспільної шкоди, включаючи загрози демократичним процесам. При цьому важливо зберегти чітке розмежування між дезінформацією з умисними намірами та помилковою інформацією з відсутністю таких намірів, що унеможливить надмірне обмеження свободи вираження поглядів.

Другим напрямом є регулювання передвиборної агітації та політичної реклами в інтернет, зокрема в соціальних мережах. Виборчий кодекс не містить спеціальних норм щодо онлайн-агітації, залишаючи це питання майже нерегульованим. З урахуванням досвіду Регламенту ЄС 2024/900 про прозорість та таргетинг політичної реклами, доцільним видається запровадження таких правових вимог, як обов’язкове маркування онлайн-агітації із зазначенням замовника, заборона на фінансування онлайн-агітації від суб’єктів, що перебувають поза межами України, або замасковане фінансування та вимога щодо обліку та звітності онлайн-рекламних витрат у рамках виборчого фонду.

Третій напрям полягає у встановленні правових обмежень щодо мікротаргетингу у виборчих кампаніях. Мікротаргетинг, заснований на обробці персональних даних виборців, становить одну з ключових загроз принципу рівного доступу до інформації та є одним із механізмів маніпуляції виборчою поведінкою, яка призводила до скандалів на кшталт Cambridge Analytica [8, с. 10-12]. Україна, яка є країною-кандидатом на вступ до ЄС, має привести відповідне регулювання у відповідність до положень GDPR щодо обробки персональних

даних у політичних цілях. Зокрема, доцільним є: встановлення чіткої заборони на мікротаргетинг, заснований на чутливих категоріях персональних даних (зокрема даних про політичні переконання); запровадження вимоги розкриття параметрів таргетування у виборчій рекламі; встановлення відповідальності цифрових платформ за використання даних виборців для цілей виборчого мікротаргетингу без їхньої явної згоди.

Четвертим напрямом є розробка регуляторних норм щодо систем штучного інтелекту у виборчому процесі. Акт ЄС про штучний інтелект відносить системи ШІ, що використовуються для впливу на результати виборів або поведінку виборців, до систем з високим ступенем ризику, що тягне за собою суворі вимоги щодо прозорості та людського нагляду [16, с. 12-14]. Оскільки Україна як країна-кандидат на вступ до ЄС найближчими роками має внести Акт про штучний інтелект у своє національне законодавство, підготовка правової основи для цього процесу є першочерговим завданням. Зокрема, вже зараз доцільним є закріплення у Виборчому кодексі вимоги маркування контенту, згенерованого штучним інтелектом, зокрема діпфейків, та встановлення відповідальності за його розповсюдження у виборчий період з метою маніпулювання виборцями.

П'ятим напрямом є встановлення відповідальності цифрових платформ за контент, що становить дезінформаційну загрозу виборчому процесу. Ані Виборчий кодекс, ані Закон “Про медіа” не встановлюють зобов’язань для операторів соціальних мереж у виборчий період. З урахуванням підходу DSA, відповідно до якого великі онлайн-платформи зобов’язані проводити оцінку системних ризиків та вживати заходів для їх пом’якшення, доцільним є запровадження аналогічних вимог в українському законодавстві: зобов’язати великі цифрові платформи проводити оцінку ризиків дезінформації у виборчий період та звітувати про вжиті заходи перед регуляторними органами та запровадити механізм співпраці між платформами та виборчими органами для оперативного реагування на особливо шкідливий контент, що порушує правила чесних виборів.

Шостим напрямом є зміцнення інституційних механізмів. З урахуванням проведеного аналізу та рекомендацій IFES для України [16, с. 25-29], доцільним є запровадження таких інституційних інновацій: по-перше, створення міжвідомчого координаційного центру з питань дезінформації у виборчому процесі на базі ЦВК або у форматі постійно діючої міжвідомчої групи. По-друге, розроблення механізму швидкого реагування на дезінформаційні кампанії з чіткими часовими стандартами реагування під час виборчого процесу. По-третє, запровадження систематичного моніторингу цифрового інформаційного простору під час виборів. По-четверте, розбудова потенціалу Національної ради, ЦВК та інших органів у сфері проведення тренінгів з цифрової медіаграмотності та протидії дезінформації для суспільства.

Окремим напрямом є розвиток медіаграмотності як запобіжного механізму. Як зазначається у Законі “Про медіа”, медіаграмотність визначається як навички та знання, які надають користувачам можливість ефективно і безпечно користуватися медіа-сервісами відповідно до ст. 1 п. 29 [60]. Розвиток медіаграмотності є важливим аспектом державної політики у сфері медіа, який може знизити вразливість виборців до дезінформаційних кампаній. Проте на рівні Виборчого кодексу відсутні будь-які норми щодо медіаграмотності у виборчому контексті. Включення відповідних положень, включаючи фінансування освітніх програм та вимоги щодо інформування виборців про ознаки дезінформації, посилює правові основи для захисту демократичного волевиявлення.

Міністерство цифрової трансформації опублікувало Дорожню карту регулювання ІІІ, побудовану за принципами балансу між регулюванням та інноваціями, культури саморегулювання та висхідного підходу. Хоча Дорожня карта поки не передбачає конкретних елементів, безпосередньо пов'язаних з виборами, очікується, що в майбутньому буде запроваджено категоризацію ризиків, подібну до Акту про штучний інтелект [16, с. 20]. Міністерство також опублікувало “Керівні принципи 2024” щодо відповідального використання ІІІ медіакомпаніями, які передбачають прозорість використання систем ІІІ та чітке

розмежування між контентом, створеним людиною, і контентом, створеним ШІ

Важливим застереженням при розробці всіх зазначених механізмів є необхідність суворого дотримання принципу пропорційності та збереження свободи вираження поглядів як фундаментального права, гарантованого Конвенцією. Про необхідність такого балансу свідчить і практика ЄСПЛ, зокрема рішення у справі “Бредшоу та інші проти Сполученого Королівства”, де Суд визнав позитивний обов’язок держави захищати виборчий процес від дезінформації, водночас наголосивши на широких межах розсуду держав у виборі конкретних інструментів захисту з урахуванням балансу зі свободою вираження поглядів [26].

Варто також відзначити специфічний контекст, в якому відбуватиметься реформування виборчого законодавства України. Як підкреслює К. Філіпчук, радикальні, особливо стрімкі зміни нормативно-правового регулювання створюють загрозу виборчому процесу, за таких умов сам інститут виборів може делегітимізуватися, оскільки руйнуються демократичні принципи ведення виборчого процесу [5, с. 290]. Отже, реформа має здійснюватися поступово, із широким залученням зацікавлених сторін та з урахуванням повоєнних умов, в яких Україна матиме проводити перші вибори після завершення воєнного стану. Пріоритетом у короткостроковій перспективі має бути підготовча правотворча діяльність, а не поспішне ухвалення законодавства.

Таким чином, вдосконалення правового регулювання протидії дезінформації у виборчому процесі України потребує комплексного підходу, що охоплює нормативне визначення ключових понять, регулювання онлайн-агітації та мікротаргетингу, встановлення вимог до систем ШІ у виборчому контексті, зміцнення відповідальності цифрових платформ та розбудову інституційних механізмів. При цьому реформа має здійснюватися відповідно до курсу на євроінтеграцію, в напрямку адаптації до *acquis* ЄС у сфері цифрових послуг, штучного інтелекту та прозорості політичної реклами.

Як зазначається у рекомендаціях Громадянської мережі ОПОРА, повоєнні вибори в Україні стануть не лише символом відновлення демократії, а й головною мішенню гібридних атак Росії. Інформаційні кампанії, кібератаки, приховане фінансування - ось неповний перелік інструментів, за допомогою яких агресор намагатиметься вплинути на волевиявлення українців [26]. ОПОРА пропонує комплекс заходів, зокрема: налагодження діалогу з глобальними онлайн-платформами для блокування дезінформації та запровадження її маркування; адаптацію українського законодавства до норм ЄС, зокрема DSA та DMA; вивчення міжнародних практик, включно із заборonoю використання TikTok на робочих пристроях держслужбовців; посилений контроль над Telegram; впровадження довгострокових програм медіаграмотності у шкільній освіті [26].

Для унеможливлення прихованого фінансування з боку держави-агресора, необхідно вдосконалити законодавство у сфері політичних фінансів, запровадити пропорційні санкції за порушення та посилити механізми моніторингу витрат партій і виборчих кампаній. Окремий блок рекомендацій стосується запобігання політичному впливу Росії через кандидатів та організації, зокрема обов'язкове декларування відсутності зв'язків із державою-агресором та посилення кримінальної відповідальності у цій сфері [26].

Щодо регулювання ІІІ в контексті виборів, аналітичний документ IFES рекомендує Україні низку заходів:

- проводити пілотні випробування інструментів ІІІ до впровадження на виборах;
- протидіяти використанню ІІІ для дезінформації через інформаційні кампанії та співпрацю з фактчекерами;
- запровадити механізми м'якого регулювання для відповідального використання ІІІ; покращити грамотність у сфері ІІІ серед представників органів державної влади;
- зобов'язати ЦВК проаналізувати ризики та можливості, пов'язані зі штучним інтелектом на виборах; переглянути законодавство щодо захисту

персональних даних для приведення його у відповідність до стандартів ЄС

Висновки до Розділу 4. Чинне українське законодавство має суттєві прогалини у регулюванні онлайн-агітації та протидії дезінформації під час виборів. Закон України “Про медіа” передбачає, що користувачі платформ спільного доступу не є суб’єктами онлайн-медіа, крім випадків добровільної реєстрації, що створює ситуацію, коли особа може поширювати інформацію на значну аудиторію, не підпадаючи під встановлені для медіа обов’язки та обмеження. В умовах війни такі канали можуть використовуватися для розповсюдження дезінформації, прихованої російської пропаганди чи вигідних для агресора наративів.

Інституційні механізми протидії дезінформації під час виборів в Україні знаходяться лише на стадії формування. Дорожня карта регулювання ІІІ, опублікована Міністерством цифрової трансформації, та Керівні принципи 2024 року щодо відповідального використання ІІІ медіакомпаніями становлять перші кроки у формуванні національної політики, проте вони не передбачають конкретних елементів, безпосередньо пов’язаних з виборами. Очікується, що в межах процесу інтеграції в ЄС Україна імплементує Акт про штучний інтелект у своє національне законодавство.

Рекомендації громадських організацій вказують на сукупність заходів, необхідних для протидії гібридним загрозам у виборах після війни:

- налагодження діалогу з глобальними онлайн-платформами для блокування дезінформації та її маркування;
- адаптація українського законодавства до норм законодавства ЄС;
- вивчення міжнародних практик у сфері протидії дезінформації; впровадження програм медіаграмотності у шкільній та позашкільній освіті;
- перегляд законодавства щодо захисту персональних даних для приведення його у відповідність до стандартів ЄС.

Також важливими є заходи з унеможливлення прихованого фінансування з боку держави-агресора через вдосконалення законодавства у сфері фінансування політичних партій, запровадження пропорційних санкцій та посилення механізмів моніторингу витрат партій. Запропонованим підходом є також визнання користувачів з великим впливом суб'єктами онлайн-медіа, що адекватно відображало б ключову роль цих суб'єктів у медіаспоживанні українців.

ВИСНОВКИ

Аналіз теоретико-правових засад дозволяє зробити висновок, що класична парадигма виборчого права, побудована на регулюванні традиційних медіа та лінійній моделі пропаганди, є неспроможною протистояти сучасним гібридним загрозам. На відміну від масової пропаганди минулого століття, сучасна дезінформація діє через мікротаргетинг, фрагментуючи суспільство на ізольовані "інформаційні бульбашки", що знищує змагальність ідей як базовий принцип вільного волевиявлення. З цього випливає ключовий висновок: цифрові платформи остаточно втратили статус нейтральних технічних посередників і перетворилися на активних суб'єктів виборчого процесу, чії алгоритми здатні системно керувати поведінкою виборців та викривляти результати виборів.

Окремим висновком є те, що практика Європейського суду з прав людини концептуально змінила підхід до ролі держави в епоху цифрових платформ. Рішення ЄСПЛ у справі "Бредшоу та інші проти Сполученого Королівства" формує нову правову доктрину: право на вільні вибори вимагає від держави не просто пасивного невтручання, а виконання позитивного обов'язку щодо проактивного захисту демократичного процесу від іноземної дезінформації та кібератак. Отже, відсутність у національному законодавстві ефективних механізмів регулювання цифрових платформ відтепер може трактуватися як порушення державою своїх позитивних зобов'язань перед виборцями.

Аналіз досвіду ЄС також показує, що ефективна боротьба з дезінформацією виявилась неможливою виключно шляхом м'якого права та саморегулювання корпорацій. Відтак, Європейський Союз здійснив необхідний еволюційний перехід до багаторівневої системи спільнорегулювання та жорстких нормативних вимог, втіленої у Digital Services Act (DSA), Регламенті про політичну рекламу та Акті про штучний інтелект. З цього випливає критично важливий висновок для архітектури виборчого права: правове регулювання виборів має інтегрувати норми законодавства про цифрові послуги та штучний інтелект. Перенесення тягаря відповідальності на дуже великі онлайн-платформи, які тепер зобов'язані самотійно оцінювати та пом'якшувати ризики

для виборчого процесу під загрозою мільярдних штрафів, є одним з найефективніших інструментів. Більше того, класифікація систем штучного інтелекту, що використовуються для виборчого впливу, як “систем високого ризику”, закладає новий стандарт прозорості, який запобігатиме алгоритмічному маніпулюванню та поширенню зловмисних дипфейків.

Порівняльний аналіз правових систем окремих держав свідчить, що світовий досвід пропонує спектр моделей реагування, кожна з яких має свої переваги та ризики. Зокрема, акцент виключно на криміналізації певних видів контенту, як у Німеччині, частково перекладає функцію нагляду на соціальні платформи. Британська модель “обов’язку турботи”, передбачена Online Safety Act, також зміщує фокус з покарання окремих користувачів на відповідальність платформ за структурні недоліки платформ.

Попри це слушним буде зауваження, що жодна з наведених країн не перебуває в стані війни, яка ставить під особливу загрозу демократичність виборчих процесів після війни і створює необхідність протидіяти загрозам дезінформації, що можуть вплинути на вибори. Тому найбільш збалансованими для українського правового регулювання видаються моделі, що фокусуються на прозорості процесів, оперативності судового реагування та інституційній стійкості, до прикладу французький механізм прискореного судового блокування неправдивої інформації в період виборів. Попри це варто пам’ятати, що будь-які заходи щодо обмеження контенту повинні відповідати критеріям законності, необхідності в демократичному суспільстві та легітимної мети, визначеними практикою ЄСПЛ. Таким чином важливим є передбачити чіткі випадки та механізми обмеження здійснення свободи вираження поглядів, а також належне обґрунтування при такому обмеженні. Адже існує дуже тонка грань між сатирою щодо окремих кандидатів на виборах та свідомим введенням в оману суспільства з метою зменшення рейтингів тих чи інших кандидатів чи зниження явки на виборах. Тому при з’ясуванні мотивів створення дописів, важливим є моніторинг обсягів поширення та кількості охоплень серед користувачів соціальних мереж.

Оцінка чинного законодавства України дозволяє стверджувати, що вітчизняна нормативно-правова база не відповідає актуальним технологічним викликам та перебуває у стані формування. Можна виділити такі системні недоліки:

- відсутність у Виборчому кодексі та Законі “Про медіа” легального визначення дезінформації, місінформації та операцій інформаційного впливу, що унеможлиблює чітку правову кваліфікацію цифрових загроз.
- законодавство про медіа залишає поза своїм регулюванням діяльність звичайних користувачів платформ, які мають мільйонні аудиторії, що створює сіру зону для поширення прихованої російської пропаганди лідерами думок без будь-якої юридичної відповідальності.
- абсолютна неврегульованість передвиборної агітації в інтернет та відсутність запобіжників щодо використання політичного мікротаргетингу і збору персональних даних виборців.
- недостатні повноваження та ресурси Центральної виборчої комісії та Національної ради телебачення та радіомовлення щодо моніторингу цифрового простору у реальному часі.

Захист виборчого процесу як фундаменту здійснення демократії має стати результатом співпраці, а не монополією через зосередження надмірної кількості влади в одного органу державної влади. Доцільним є створення постійно діючої міжвідомчої оперативної групи за участі Центральної виборчої комісії, Міністерства цифрової трансформації України, Національної ради телебачення та радіомовлення та експертів громадянського суспільства, яка здійснюватиме моніторинг інформаційного простору під час виборчих кампаній та зможе оперативно ініціювати блокування незаконного дезінформаційного контенту.

Також варто звернути увагу, що лише юридичні механізми не можуть і не повинні обмежувати весь сумнівний контент через загрозу цензури, паралельним вектором політики має стати розвиток медіаграмотності виборців за прикладом скандинавських країн, оскільки запровадження програм медіаграмотності у сфері цифрової безпеки є надійним методом боротьби з оманливим контентом, а

також зменшує потребу залучати ресурси державного апарату у боротьбі з дезінформацією.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- Hotărârea nr. 32 din 6 decembrie 2024 privind anularea procesului electoral cu privire la alegerea Președintelui României din anul 2024 : Decizia Curții Constituționale a României. <https://legislatie.just.ro/Public/DetaliiDocument/290400> (дата звернення: 30.04.2026).
2. Casero-Ripollés A., Alonso-Muñoz L., Moret-Soler D. Spreading false content in political
- Iss. 4. P. 31–49.
- URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:790:FIN> (дата звернення: 30.04.2026).
5. Філіпчук К. Загрози дотриманню правових принципів виборів у глобалізованому цифровому суспільстві. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2025. № 3 (47). С. 288–294. DOI: <http://doi.org/10.23939/law2025.47.288>. <https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/elections-and-referendums/past-elections-and-referendums/eu-referendum/results-and-turnout-eu-referendum> (дата звернення: 30.04.2026). [Потребує уточнення — у роботі позначено як [6] без зазначення джерела даних про результати референдуму.]
7. Кадвалладр К., Грехем-Херрісон Е. Виявлено: 50 мільйонів профілів Facebook зібрано для Cambridge Analytica через серйозний витік даних. The Guardian. 17 трав. 2018. URL: [election](#) (дата звернення: 30.04.2026).
8. Людва А., Дворовий М. Цифрові технології та виборчий процес: стандарти ЄС на захисті демократичного вибору : аналіт. звіт / рец.: С. Савелій, В. Володовська. Київ : ГО «Лабораторія цифрової безпеки», 2022. 64 с.
9. Вулі С. С., Ховард Ф. Н. Комп'ютерна пропаганда: політичні партії, політики та політичні маніпуляції у соціальних мережах (витяг). 2018. URL: [en/library/2022-strengthened-code-practice-disinformation](#) (дата звернення: 30.04.2026).
11. Wakefield J. Deepfake presidents used in Russia-Ukraine war. BBC News. 18 March 2022. URL: <https://www.bbc.com/news/technology-60780142> (дата звернення: 30.04.2026).
- 11a. Herrero O. Le gouvernement embarrassé par un “deepfake” visant Marine Le Pen. Politico. 2024. (дата звернення: 01.05.2026). [result_details.aspx?ObjectId=090000168092dd4b](#) (дата звернення: 30.04.2026).
6. P. 965–998. DOI: <https://doi.org/10.1177/00104140231193008>.
- RL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804fa42d (дата звернення: 30.04.2026).
- igns : adopted on 6 April 2022 at the 1431st meeting of the Ministers' Deputies / Council of

Europe.

https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a61066
(дата звернення: 30.04.2026).

URL:

(дата

16. Кастанья А., Меленчук А. Адаптація законодавства ЄС у сфері штучного інтелекту до виборчих процесів: шлях для України / співавт.: І. Ткаченко, О. Сидорчук ; рец.: Л. Реппелл, І. Біку. Київ : Міжнародна фундація виборчих систем (IFES) в Україні, 2024.
- 16а. Як відповідально використовувати штучний інтелект: розробили рекомендації для медіа. М
17. AI chatbots spread falsehoods about the EU election, report finds [Чат-боти зі штучним інтелектом поширюють неправду про вибори в ЄС, — звіт]. Politico. URL: <https://www.politico.com/news/2024/05/01/ai-chatbots-eu-election-falsehoods-000001> (дата звернення: 30.04.2026).
- URL: <https://www.ifes.org/publications/direct-democracy-progress-and-pitfalls-election-technology> (дата звернення: 30.04.2026).
18. Liebert, P., Politics, and Policy. 2020. Vol. 19, № 2. URL: <https://www.liebertpub.com/doi/abs/10.1089/elj.2019.0566> (дата звернення: 24.05.2025).
20. Гаркот А. І. Правовий статус користувачів із великим впливом на платформах спільного доступу до інформації: перспективи визнання суб'єктами онлайн-медіа в Україні. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 87, ч. 2. С. 322–328. DOI: <https://doi.org/10.24144/2307-3322.2025.87.2.48>.
21. Справлення населення до медіа та споживання різних типів медіа в Україні : річне дослідження-2024 / USAID-Internews. Київ : ГО «Інтерньюз-Україна», 2024. URL: <https://internews.in.ua/> (дата звернення: 30.04.2026).
22. Cano-Orón L., Calvo D., López García G., Baviera T. Disinformation in Facebook ads in the 2019 Spanish general election campaigns. Media and Communication. 2021. Vol. 9, Iss. 1. P. 217–230.
23. Facebook ads during the 2019 General Elections in Spain. Communication & Society. 2022. Vol. 35, No. 1. P. 1–15.
24. Directive (EU) 2018/1808 (recast of the Directive on the audiovisual Media Services Directive) in view of changing market realities. Official Journal of the European Union. L 303. 28.11.2018. P. 69–92. URL: <https://eur-lex.europa.eu/eli/dir/2018/1808/oj> (дата звернення: 30.04.2026).
25. United Kingdom : Judgment of the European Court of Human Rights of 22 July 2025, Application no. 15653/22. URL: <https://hudoc.echr.coe.int/eng?i=001-244218> (дата звернення: 30.04.2026).
26. Міхалевська К., Романюк П. Прецедент Бредшоу: висновки ЄСПЛ щодо протидії напівземному втручання у вибори. Громадянська мережа ОПОРА : вебсайт. 30 верес. 2025. URL: <https://opora.ua.org/article/vybory/bradshaw-precedent-conclusions-of-the-echr-regarding-the-counteraction-to-foreign-interference-in-elections-25818> (дата звернення: 30.04.2026).

27. Timpul Info-Magazin and Anghel v. Moldova : Judgment of the European Court of Human Rights of 27 November 2007, Application no. 42864/05. URL: <https://hudoc.echr.coe.int/eng?i=001-83574> (дата звернення: 30.04.2026).

28. Medžlis Islamske Zajednice Brčko and Others v. Bosnia and Herzegovina : Judgment of the Grand Chamber of the European Court of Human Rights of 27 June 2017, Application no. 17224/11. URL: <https://hudoc.echr.coe.int/eng?i=001-175180> (дата звернення: 30.04.2026).

lov v. Ukraine : Judgment of the European Court of Human Rights of 6 September 2005, Application no. 65518/01. URL: <https://hudoc.echr.coe.int/eng?i=001-70097> (дата звернення:

3

https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf (дата звернення: 30.04.2026).

ry 2025 (formerly Strengthened Code of Practice on Disinformation 2022). URL: <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation> (дата звернення: 30.04.2026).

ssment-code-practice-disinformation (дата звернення: 30.04.2026).

i). Official Journal of the European Union. L 277. 27.10.2022. P. 1–102. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> (дата звернення: 30.04.2026).

35. Romănishyn A. Enhancing election integrity by strengthening EU defences against disinformation D

European Union. L, 2024/900. 20.3.2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/900/oj> (дата звернення: 30.04.2026).

A intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. Official Journal of the European Union. L, 2024/1689. 12.7.2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 30.04.2026).

stering disinformation campaigns in Europe : офіційний вебсайт East StratCom Task Force / European External Action Service. URL: <https://euvdisinfo.eu/> (дата звернення: 30.04.2026).

Рійбур А. Веб-сайт ЄС для боротьби з дезінформацією під загрозою (EU website for fighting disinformation is in danger). EU Observer. 8 березня 2018 р. URL:

40. European Digital Media Observatory (EDMO) : офіційний вебсайт. URL: <https://edmo.eu/> (дата звернення: 30.04.2026).

9 juillet 1881 sur la liberté de la presse : Закон Французької Республіки від 29 лип. 1881 р. (зі змінами). URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000877119/> (дата звернення: 30.04.2026).

42. Code électoral : Виборчий кодекс Франції (зведений текст). URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/ (дата звернення:

Française. 23 déc. 2018. URL:

.

E
f

<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037847559/> (дата звернення:

Арком (Орган регулювання аудіовізуальної та цифрової комунікації) (Arcom - Autorité de

Fiorentino, Майкл-Росс. “У Франції ухвалили суперечливий закон про фейкові новини”.

Е

46. ^цNetzwerkdurchsetzungsgesetz (NetzDG) — Gesetz zur Verbesserung der Rechtsdurchsetzung in ^г

о

п

е

47. Germany: Flawed Social Media Law : Human Rights Watch report, 14 February 2018. URL: <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law> (дата звернення:

,

Репортери без кордонів. Російський законопроект є копією німецького закону про мову ²ненависті (Russian bill is copy-and-paste of Germany's hate speech law). 19 липня 2017 р.

2

^ЛОксфордський інтернет-інститут. Оцінка впливу NetzDG (The NetzDG Impact ^иAssessment). Липень 2018 р. URL: <https://www.oii.ox.ac.uk/research/projects/netzdg/> (дата ^сзвернення: 30.04.2026).

Т

^{ур} on the promotion and protection of the right to freedom of opinion and expression : OL DEU ^и2017 — communication of David Kaye, UN Special Rapporteur, to the Government of ⁶(дата звернення: 30.04.2026).

д

51. Online Safety Act 2023 : an Act of the Parliament of the United Kingdom, с. 50, 26 October 2023. ^а(дата звернення: 30.04.2026). URL: <https://www.legislation.gov.uk/ukpga/2023/50/contents> (дата звернення: 30.04.2026).

logue/dutch-code-of-conduct-transparency-online-political-advertisements (дата звернення:

ies. 2024. Vol. 62, Iss. 6. P. 1538–1559. DOI: <https://doi.org/10.1111/jcms.13601>.

(дата звернення: 30.04.2026).

Lithuania to block Russia's Sputnik news over copyright issues. Emerging Europe. URL: <https://emerging-europe.com/lithuania-to-block-russias-sputnik-news-over-copyright-issues/> (дата звернення: 30.04.2026).

de julio, General de Comunicación Audiovisual : Закон Королівства Іспанія. Boletín Oficial del Estado. 8.7.2022. № 163. URL: <https://www.boe.es/eli/es/l/2022/07/07/13/con> (дата звернення: 30.04.2026).

e regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma. Boletín Oficial del Estado. 1.5.2024. № 106. URL: <https://www.boe.es/eli/es/rd/2024/04/30/444/con> (дата звернення: 30.04.2026).

. Protection from Online Falsehoods and Manipulation Act 2019 (POFMA) : Act of the

Parliament of the Republic of Singapore, № 18 of 2019, 11 June 2019 (commenced 2 October 2019). URL: <https://sso.agc.gov.sg/Acts-Supp/18-2019/> (дата звернення: 30.04.2026).

ve-justice-collective (дата звернення: 30.04.2026).

. Виборчий кодекс України : Закон України від 19 груд. 2019 р. № 396-IX. Відомості Верховної Ради України. 2020. № 7, 8, 9. Ст. 48. URL: <https://zakon.rada.gov.ua/laws/show/396-20> (дата звернення: 30.04.2026).

. Про медіа: Закон України від 13 груд. 2022 р. № 2849-IX. Відомості Верховної Ради України. 2023. № 25–26. Ст. 78. URL: <https://zakon.rada.gov.ua/laws/show/2849-20> (дата звернення: 30.04.2026).