

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Факультет історії, політології та міжнародних відносин
Кафедра міжнародних відносин та суспільних комунікацій

**Правове регулювання діяльності соціальних мереж та
протидія маніпуляціям в Інтернет-просторі США**

Кваліфікаційна робота

Рівень вищої освіти – другий (магістерський)

Виконала:

студентка 6 курсу, 604 групи

Павчук Ангеліна Василівна

Керівник:

кандидатка політичних наук,
доцентка **Макух-Федоркова І. І.**

До захисту допущено

на засіданні кафедри

протокол №_____ від _____ 2024 р.

Зав. кафедрою _____ проф. Макар В.Ю.

Чернівці – 2024

Анотація

У роботі розглядається правове регулювання діяльності соціальних мереж в Інтернет-просторі США та протидія маніпуляціям, що здійснюються через ці платформи. Актуальність теми зумовлена стрімким розвитком цифрових технологій, що призводить до нових викликів для правових систем, зокрема в контексті захисту прав і свобод користувачів та боротьби з маніпуляціями в медіа-просторі.

Ключові слова: *регулювання інтернет-відносин, правові підходи, маніпуляція в інтернет-просторі, свобода слова, соціальні мережі, дезінформація, захист персональних даних, прозорість політичної реклами, інформаційна безпека, США, фейкові новини.*

Summary

Die Arbeit befasst sich mit der rechtlichen Regulierung sozialer Netzwerke im Internetraum der USA und der Bekämpfung von Manipulationen, die durch diese Plattformen durchgeführt werden. Die Relevanz des Themas ergibt sich aus der raschen Entwicklung digitaler Technologien, die zu neuen Herausforderungen für Rechtssysteme führen, insbesondere im Hinblick auf den Schutz der Rechte und Freiheiten der Nutzer sowie die Bekämpfung von Manipulationen im Medienraum.

Schlüsselwörter: *Regulierung von Internetbeziehungen, rechtliche Ansätze, Manipulationen im Internetraum, Meinungsfreiheit, soziale Netzwerke, Desinformation, Schutz personenbezogener Daten, Transparenz politischer Werbung, Informationssicherheit, USA, Fake News.*

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів наукових досліджень інших авторів мають посилання на відповідне джерело.

_____ Павчук А.В.
(підпис)

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ АСПЕКТИ ДОСЛІДЖЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ В ІНТЕРНЕТ ПРОСТОРИ США.....	7
1.1. Теоретико-методологічні підходи регулювання інтернет-відносин в США	7
1.2. Характеристика джерельної бази дослідження	15
Висновки до 1 розділу.....	22
РОЗДІЛ 2. ПРАВОВІ ПІДХОДИ ДО ПОЛІТИКИ РЕГУЛЮВАННЯ СОЦІАЛЬНИХ МЕРЕЖ У США	26
2.1. Вплив медійних транснаціональних корпорацій на регуляторні процеси інтернет простору США та світу	26
2.2. Нормативно-правове регулювання діяльності американських соціальних мереж	33
2.3. Роль Верховного суду США та інших правоохоронних органів щодо політики контролю соціальних мереж	40
Висновки до 2 розділу.....	48
РОЗДІЛ 3. ПРОТИДІЯ МАНІПУЛЯЦІЙНИМ ВПЛИВАМ В СУЧАСНОМУ ІНТЕРНЕТ-ПРОСТОРИ	51
3.1 Характеристика методів маніпуляційної діяльності в соціальних мережах	51
3.2. Роль регуляторів та провідних компаній у запобіганні маніпуляціям..	66
3.3. Вплив правового регулювання на діяльність соціальних мереж та маніпулятивні впливи	75
Висновки до 3 розділу.....	88
ВИСНОВКИ	90
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	93
Zusammenfassung	102

ВСТУП

Актуальність теми. У сучасному світі соціальні мережі стали невід'ємною частиною повсякденного життя, маючи величезний вплив на особисті відносини, економіку, політику та культуру. Водночас, разом з безсумнівними перевагами, вони породжують і численні загрози, зокрема, в аспектах інформаційної безпеки та етики. Завдяки швидкому розвитку технологій, соціальні мережі стали потужним інструментом для поширення різноманітних ідей, але водночас вони стали платформами для маніпуляцій, фальшивих новин та пропаганди.

Особливо важливим аспектом є розуміння правових норм, які регулюють діяльність цих платформ. Законодавство США з приводу прав і обов'язків у цифровому середовищі є одними з найбільш обговорюваних у світі, що пов'язано з глобальним впливом таких великих технологічних компаній, як Facebook, Twitter, Google. Вони мають величезний доступ до даних користувачів, а також велику роль у формуванні громадської думки. У свою чергу, така концентрація влади над інформацією ставить під сумнів ефективність національних і міжнародних правових механізмів, спрямованих на захист прав людини, особливо в контексті маніпуляцій у політичних кампаніях, де роль соціальних мереж часто виступає вирішальною.

Небезпека маніпуляцій через соціальні мережі вимагає уваги і з боку державних структур, і з боку міжнародної спільноти. Маніпуляції можуть виражатися в різноманітних формах — від фальсифікації новин до організації цілеспрямованих кампаній для впливу на виборців. Ситуація ускладнюється тим, що, на відміну від традиційних медіа, соціальні мережі не підпорядковуються чітким правилам та нормативам, а їхній алгоритм функціонування є закритим та непрозорим. Ці фактори ставлять під загрозу демократичні процеси та права громадян на чесну та об'єктивну інформацію.

Актуальність дослідження цих питань зростає не лише у контексті національних законодавчих ініціатив, але й у рамках міжнародного співробітництва. Важливою частиною цього процесу є питання забезпечення захисту приватних даних та підвищення рівня обізнаності громадян щодо кіберзагроз. Підвищення цифрової грамотності стає ключовим елементом у боротьбі з маніпуляціями та фейковими новинами. Користувачі Інтернету повинні володіти навичками критичного мислення, щоб вміти розпізнавати та адекватно реагувати на інформаційні атаки, не піддаючись маніпуляціям.

Таким чином, питання правового регулювання соціальних мереж у США та забезпечення ефективної протидії маніпуляціям в Інтернет-просторі є багатограним і потребує комплексного підходу, що включає вдосконалення правової бази, розвиток міжнародних стандартів та зусилля в напрямку підвищення обізнаності користувачів.

Об’єкт дослідження: система правового регулювання та соціальні мережі в Інтернет-просторі Сполучених Штатів Америки.

Предмет дослідження: механізми правового захисту від маніпуляцій та негативного впливу в соціальних мережах США.

Мета дослідження: аналіз правових інструментів, спрямованих на регулювання функціонування соціальних мереж та протидію маніпуляціям в Інтернет-просторі США.

У відповідності до зазначеної мети було поставлено наступні **завдання** роботи:

1. Розглянути теоретико-методологічні підходи регулювання інтернет-відносин в США.
2. Охарактеризувати джерельну базу дослідження.
3. Дослідити історію становлення соціальних мереж в США.
4. Вивчити законодавство, що впливає на діяльність соціальних мереж.
5. Розкрити роль Верховного суду США та інших органів у контролі за діяльністю соціальних мереж.

6. Обґрунтувати розбір методів маніпуляційної діяльності в соціальних мережах.

7. Розглянути зусилля регуляторів та компаній у запобіганні маніпуляціям.

8. Охарактеризувати вплив правового регулювання на соціальні мережі та маніпуляції.

Теоретичне та практичне значення теми. Дослідження в сфері правового регулювання соціальних мереж відкриває нові перспективи для розвитку інформаційного права та сприяє формуванню теоретичних концепцій у цій області. Аналіз правового статусу соціальних мереж допомагає виявити невизначеності та прогалини в законодавстві, що потребують подальшого вивчення та регулювання. Практично це дослідження має на меті розробку та удосконалення законодавства щодо соціальних мереж в США, забезпечення прав та свобод користувачів та боротьби з маніпуляціями в Інтернеті. Результати можуть слугувати основою для створення механізмів протидії маніпуляціям та формування етичних стандартів використання соціальних мереж.

Методи дослідження. Методологічна основа обумовлена об'єктом та предметом дослідження. За для ефективного вивчення та вирішення поставлених завдань доцільно використати загальнонаукові та спеціальні методи. В дослідженні буде використано такі методи: формально-логічні методи (аналіз, синтез, дедукція, індукція для дослідження сучасних наукових підходів до розуміння сутності поняття «маніпуляція», «дезінформація», «вплив соціальних мереж»; «правове регулювання соціальних мереж»); загальнонауковий метод (використання обумовлене вивченням особливостей організації та здійснення державного контролю в соціальних мережах та запобігання поширенню дезінформації); системно-структурний метод (дослідження особливостей впливу нормативно правових актів на процес протидії маніпуляціям в Інтернет просторі США). Важливе місце посідають спеціально-наукові методи дослідження, що дозволять проаналізувати

законодавство США в процесі боротьби з маніпуляцією та дезінформацією в соціальних мережах.

Апробація результатів дослідження. Павчук А. В. Кібербезпека в правовому регулюванні безпекової політики США // XVII Міжнародна науково-практична конференція студентів та молодих вчених «Актуальні проблеми зовнішньої політики України». Чернівці, 30 листопада 2023. С. 93 – 97.

Структура роботи відображає логіку дослідження та складається з вступу, трьох основних розділів, кожен з яких присвячений окремим аспектам правового регулювання діяльності соціальних мереж та протидії маніпуляціям в Інтернет-просторі США, висновків, що підсумовують результати дослідження та списку використаних джерел.

РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ АСПЕКТИ ДОСЛІДЖЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ В ІНТЕРНЕТ ПРОСТОРИ США

1.1. Теоретико-методологічні підходи регулювання інтернет-відносин в США.

Інформаційне право в США є складною та різноманітною галуззю, яка регулює широкий спектр аспектів, пов'язаних з обміном інформацією в цифровому середовищі. Його особливості визначаються якістю правового регулювання, принципами, що йому притаманні, а також специфікою сучасних технологічних викликів та інформаційних потреб суспільства. Для кращого розуміння особливостей інформаційного права в США слід розглянути його ключові аспекти та характеристики.

По-перше, варто відзначити, що інформаційне право в США базується на низці джерел, включаючи конституційні норми, федеральні закони, судову практику та адміністративні положення. Конституція США, зокрема, гарантує свободу слова та преси, яка є важливою складовою інформаційного права. Законодавство, таке як Закон про свободу інформації, Закон про захист авторського права в цифрову епоху та інші, визначає правові стандарти щодо доступу до інформації, захисту авторських прав, конфіденційності даних та інших аспектів, пов'язаних з обміном інформацією в Інтернеті та інших медіа [1, с. 99].

Другим важливим аспектом інформаційного права в США є його функції та цілі. Однією з ключових функцій є забезпечення прав людей на свободу висловлювання, доступ до інформації та приватність. Інформаційне право також спрямоване на захист прав та інтересів індивідів, компаній та держави в цифровому середовищі. Воно регулює взаємодію між користувачами та провайдерами інформації, забезпечуючи рівний доступ до неї та захист від недобросовісної діяльності.

Третім аспектом є особливості інформаційного права, які визначаються швидким розвитком технологій та постійною зміною суспільних потреб. Інформаційне право постійно адаптується до нових викликів та можливостей, які виникають у зв'язку з впровадженням новітніх технологій, таких як штучний інтелект, блокчейн та Інтернет речей. Воно також реагує на нові види кіберпротиправності та загрози кібербезпеці, забезпечуючи відповідні заходи захисту та протидії [29, с. 89].

Четвертим аспектом є принципи, що лежать в основі інформаційного права в США. До таких принципів відносяться принцип свободи висловлювання, прозорості, конфіденційності даних, захисту авторських прав та приватності користувачів. Ці принципи відображають ключові цінності американського суспільства та стандарти, які визнаються як основоположні для забезпечення ефективного та справедливого інформаційного середовища.

Поняття регулювання інтернет-відносин визначає основні принципи, правила та механізми контролю, які встановлюються для забезпечення порядку, безпеки та ефективності в діяльності, пов'язаній з використанням Інтернету. Це поняття включає в себе широкий спектр аспектів, від правових норм до технічних стандартів, які регулюють взаємодію користувачів, компаній, урядових органів та інших учасників цифрового простору. Для кращого розуміння цього поняття, слід розглянути його ключові складові та історію розвитку.

Спочатку варто зазначити, що інтернет є глобальною мережею, що перетинає національні кордони та об'єднує мільярди користувачів по всьому світу. У зв'язку з цим виникає необхідність у створенні універсальних правил та стандартів, які б визначали права та обов'язки усіх учасників цієї мережі. Регулювання інтернет-відносин має на меті забезпечити безпеку, захист прав та інтересів користувачів, а також збереження функціонування мережі в цілому [7, с. 56].

Однією з ключових складових регулювання інтернету є правові норми та законодавство. Кожна країна має свої закони, які регулюють використання

Інтернету на своїй території. Ці закони можуть стосуватися таких питань, як захист персональних даних, авторських прав, боротьба з кіберпротиправністю тощо. Однак через глобальний характер Інтернету, часто виникають ситуації, коли законодавство однієї країни суперечить законодавству іншої або міжнародним нормам [2, с. 77].

Крім правових норм, до складових регулювання інтернет-відносин також входять технічні стандарти та протоколи. Це включає в себе розробку та впровадження технічних стандартів для мережевого обладнання, програмного забезпечення та інфраструктури, які забезпечують сумісність та ефективну роботу мережі. Технічне регулювання також може включати заходи забезпечення кібербезпеки та захисту від кібератак [7, с. 77].

Інтернет-відносини — це складний комплекс взаємодії між користувачами, компаніями, урядовими органами та іншими суб'єктами в інтернет-середовищі. Цей екосистема включає в себе різноманітні елементи, які формують спосіб функціонування та розвитку Інтернету як технологічного, соціального та економічного явища. Давайте розглянемо основні складові інтернет-відносин [2, с. 56]:

1. Основним елементом інтернет-відносин є самі користувачі — люди, які використовують Інтернет для отримання інформації, спілкування, розваг та інших потреб. Користувачі можуть бути різного віку, соціального статусу, культурного та географічного походження, що робить інтернет-середовище дуже різноманітним та динамічним.

2. Інтернет-відносини включають взаємодію з різноманітними веб-сайтами та онлайн-платформами, які надають різні сервіси та послуги. Це можуть бути соціальні мережі, електронна комерція, новинні портали, блоги, форуми, відеохостинги та багато іншого. Веб-сайти та платформи створюють простір для спілкування, обміну інформацією, здійснення покупок та виконання різних дій в Інтернеті.

3. Оскільки Інтернет є технологічним явищем, важливим елементом його функціонування є різноманітні технології, що використовуються для

передачі, збереження та обробки інформації. Це включає в себе сервери, мережеве обладнання, програмне забезпечення, протоколи передачі даних та інші технічні складові.

4. З огляду на зростання кількості кіберправопорушень та загроз безпеці в інтернет-середовищі, кібербезпека стає ключовим елементом інтернет-відносин. Це включає в себе заходи з захисту від вірусів, шпигунського програмного забезпечення, хакерських атак, крадіжок особистих даних та інших кіберзагроз.

Регулювання інтернет-відносин в США визначається різними чинниками, які включають правові, політичні, економічні, технологічні та соціокультурні аспекти. Ці чинники взаємодіють між собою та впливають на формування стратегій та політик регулювання в цілому:

1. Законодавство є одним з основних чинників, що впливає на регулювання Інтернету в США. Правові норми, такі як Digital Millennium Copyright Act (DMCA), Communications Decency Act (CDA) та Children's Online Privacy Protection Act (COPPA), встановлюють правила та обмеження, що стосуються авторських прав, відповідальності за контент, захисту конфіденційності тощо.

2. Політичний контекст також впливає на регулювання інтернет-відносин в США. Політичні партії, вибори, лобіювання та діяльність урядових органів формують політику в галузі інтернету, включаючи прийняття нових законодавчих актів та регулятивних ініціатив.

3. Економічні інтереси впливають на регулювання інтернет-відносин через вплив великих корпорацій, які надають послуги в Інтернеті. Боротьба за ринкову частку, конкуренція та питання економічної вигоди визначають рішення щодо регулювання, включаючи політику конкуренції та захист прав споживачів.

4. Швидкий розвиток технологій впливає на способи використання Інтернету та породжує нові виклики для регулювання. Питання кібербезпеки,

захисту даних, шифрування та інші технологічні аспекти потребують постійного оновлення політик та правових норм.

5. Суспільні цінності, норми та переконання також впливають на регулювання інтернет-відносин. Питання приватності, свободи слова, доступності та рівності в Інтернеті відображають соціальні дискусії та визначають напрямки політики регулювання.

6. У зв'язку з глобалізацією Інтернету регулювання в США також підлягає впливу міжнародних стандартів та конвенцій. Участь у міжнародних організаціях та спільні ініціативи впливають на формування політики регулювання.

Історія регулювання інтернет-відносин відображає процес становлення та розвитку правового та технічного середовища мережі. Перші кроки у цьому напрямку були зроблені в 1990-2000-х роках, коли почали виникати перші закони та стандарти, спрямовані на регулювання діяльності в Інтернеті. Протягом наступних років цей процес продовжувався, із зростанням числа користувачів та розвитком нових технологій виникала потреба у постійному оновленні та адаптації правових та технічних засобів регулювання [5, с. 55].

Сьогодні регулювання інтернет-відносин залишається однією з найактуальніших тем у сфері інформаційних технологій. З появою нових викликів, таких як штучний інтелект, Інтернет речей та блокчейн-технології, стає очевидною потреба у постійному вдосконаленні правового та технічного регулювання [6, с. 66].

Функції регулювання інтернет-відносин є важливими складовими частинами забезпечення стабільності, безпеки та розвитку цифрового простору. Ці функції мають на меті забезпечити ефективне та етичне використання Інтернету, захист користувачів від загроз і кіберпротиправності, а також створення сприятливого середовища для розвитку технологій та інновацій.

Захист прав користувачів є однією з ключових функцій регулювання інтернет-відносин [5, с. 63]. Ця функція передбачає забезпечення

конфіденційності особистих даних користувачів, запобігання дискримінації в мережі, а також захист від кібербулінгу та інших форм цифрового насильства. Однією з важливих функцій є також забезпечення кібербезпеки. Це включає в себе розробку технічних та організаційних заходів для захисту від кібератак, вірусів, шпигунського програмного забезпечення та інших кіберзагроз [6, с. 90].

Створення правового середовища є ще однією функцією регулювання інтернет-відносин. Це передбачає розробку та впровадження законодавства, яке визначає правові стандарти та правила використання мережі, такі як закони про авторські права, конфіденційність даних тощо. Регулювання доступу до контенту також є важливою функцією. Це включає в себе фільтрацію небажаного або шкідливого контенту, а також регулювання діяльності онлайн-платформ з метою запобігання поширенню незаконного або шкідливого вмісту [30, с. 77].

Забезпечення етичного використання мережі також є важливою функцією регулювання. Це передбачає встановлення правил та норм поведінки в Інтернеті, що сприяє запобіганню цифрового насильства, булінгу та інших форм онлайн-експлуатації. Окрім цього, функція регулювання інтернет-відносин включає сприяння інноваціям та розвитку технологій. Це означає підтримку стартапів, розвиток цифрової грамотності, а також створення сприятливого середовища для розвитку та впровадження нових технологій. Крім того, функція регулювання інтернет-відносин передбачає координацію дій різних суб'єктів, таких як урядові органи, приватні компанії та громадські організації, з метою вирішення спільних проблем та досягнення спільних цілей у сфері Інтернету [5, с. 78].

В США регулювання інтернет-відносин здійснюється через різні підходи, які враховують технічні, правові, економічні та соціальні аспекти функціонування мережі. Одним з ключових підходів є комбінація регулювання через технології та правове регулювання. Такий підхід дозволяє поєднати технічні інструменти з нормативно-правовими актами для

забезпечення безпеки, захисту прав користувачів та ефективного функціонування Інтернету.

У США також існують саморегулювальні організації та ініціативи, які співпрацюють з урядом та приватним сектором для розробки стандартів безпеки та етики в Інтернеті. Ці організації часто виступають ініціаторами розробки технічних та правових рішень і активно сприяють вирішенню проблем, пов'язаних з кібербезпекою, захистом авторських прав, конфіденційністю даних та іншими аспектами регулювання Інтернету.

Одним з ключових аспектів стратегії регулювання інтернет-відносин урядом США є створення спеціалізованих урядових агентств та комісій, які відповідають за контроль за дотриманням законодавства у сфері інтернет-технологій. Ці агентства і комісії виконують широкий спектр функцій для забезпечення правового, економічного та технічного регулювання відносин в Інтернеті [5, с. 99]. Перш за все, такі урядові структури відповідають за моніторинг діяльності компаній, які надають послуги в Інтернеті. Це охоплює перевірку відповідності їхніх дій чинному законодавству, включаючи закони про конфіденційність даних, захист особистої інформації користувачів, а також права інтелектуальної власності. Крім того, ці урядові органи встановлюють стандарти безпеки та етики для компаній, які працюють в онлайн-середовищі, з метою забезпечення безпеки та захисту прав користувачів. Додатково, спеціалізовані агентства та комісії виконують функції з вирішення суперечок та конфліктів у сфері інтернет-технологій. Вони розглядають скарги та звернення від користувачів, компаній та інших зацікавлених сторін та приймають відповідні рішення з урахуванням законодавства та принципів справедливості. Крім того, ці урядові структури активно співпрацюють з іншими країнами та міжнародними організаціями для розробки спільних стратегій регулювання інтернету та вирішення глобальних проблем, таких як кібербезпека, захист прав людини в Інтернеті та боротьба з кіберпротиправністю. Не менш важливою функцією цих урядових структур є здійснення просвітницької діяльності та інформаційної кампанії щодо безпеки

та етики в Інтернеті. Вони надають користувачам і компаніям необхідну інформацію про правила використання мережі, небезпеки онлайн-середовища та способи захисту від потенційних загроз.

Окремим аспектом регулювання інтернету в США є захист конкуренції на ринку інтернет-послуг. Уряд та антимонопольні органи активно контролюють за діяльністю великих технологічних компаній, що надають послуги в Інтернеті, та при необхідності вживають заходів для запобігання монополізації ринку та забезпечення конкурентної середовища для інновацій та розвитку [5, с. 101].

Регулювання інтернет-відносин в США здійснюється за допомогою різноманітних методів, що включають законодавчі ініціативи, технологічні стандарти, адміністративні політики та інші заходи. Ось огляд найбільш поширених методів регулювання в даній сфері:

1. Законодавчі ініціативи включають у себе прийняття законів та постанов, які встановлюють правила, обов'язки та відповідальність для суб'єктів, що діють в Інтернеті. Наприклад, Digital Millennium Copyright Act (DMCA) регулює авторські права в онлайн-середовищі, а закони про захист приватності визначають права користувачів та обов'язки компаній щодо збереження конфіденційності даних.

2. Технологічні стандарти встановлюють вимоги до програмного та апаратного забезпечення з метою забезпечення безпеки, приватності та інших аспектів функціонування Інтернету. Наприклад, стандарти шифрування даних допомагають захищати інформацію від несанкціонованого доступу.

3. Адміністративні – включають у себе набір правил, процедур та рекомендацій, які встановлюються урядовими агентствами та регуляторами для забезпечення дотримання законодавства та нормативних вимог. Наприклад, Федеральна торговельна комісія (FTC) в США встановлює правила щодо реклами та захисту споживачів в Інтернеті.

4. Саморегулювання включає в себе ініціативи, прийняті самими галузевими гравцями з метою забезпечення етичної поведінки та відповідності

вимогам законодавства. Наприклад, технологічні компанії можуть розробляти свої власні кодекси поведінки та механізми врегулювання спірних питань між користувачами.

5. Публічне наглядання та звітність передбачають відкритий обмін інформацією між урядовими агентствами, приватним сектором та громадськістю щодо питань, пов'язаних з регулюванням інтернету. Цей підхід сприяє прозорості та відкритості процесів регулювання та сприяє залученню громадськості до вирішення спірних питань.

Нарешті, міжнародна співпраця включає у себе спільні ініціативи та домовленості між країнами з метою вирішення глобальних проблем та встановлення загальних стандартів. Наприклад, держави можуть укладати міжнародні угоди щодо боротьби з кіберпротиправністю або забезпечення кібербезпеки [2, с. 89].

Використання цих методів регулювання сприяє стабільності, безпеці та розвитку інтернету в США, забезпечуючи баланс між інноваціями, свободою відомостей та захистом прав користувачів.

1.2. Характеристика джерельної бази дослідження

Перший етап у формуванні джерельної бази регулювання інтернету в США можна пов'язати з початком появи мережі Інтернет. На початку 1960-х років у США була розроблена концепція мережі ARPANET, яка лягла в основу сучасного Інтернету. Перші кроки у створенні правового фундаменту для Інтернету відображені у документах, які регулювали комунікаційні технології та телекомунікаційну інфраструктуру.

Другий етап пов'язаний з поширенням доступу до Інтернету серед широкого загалу населення. У 1990-2000-х роках відбувся бурхливий розвиток Інтернету, що призвело до зростання числа користувачів та компаній, які використовували мережу. На цьому етапі виникала потреба у новому законодавстві та політиці, спрямованій на регулювання цифрового простору.

З'явилися перші закони, які регулювали питання конфіденційності даних, електронної комерції, авторських прав та інші аспекти діяльності в Інтернеті [20, с. 89].

Третій етап відзначається загостренням питань безпеки в Інтернеті. З появою нових технологій з'явилися нові загрози, такі як кіберпротиправність, кібертероризм та шпигунство. У зв'язку з цим урядові органи США посилили свою діяльність у сфері кібербезпеки та прийняли нові закони та положення, спрямовані на боротьбу з цими загрозами та захист критично важливих інформаційних систем.

Четвертий етап характеризується стрімким розвитком електронної комерції та поширенням соціальних мереж. З появою онлайн-магазинів, цифрових платіжних систем та соціальних платформ зросла необхідність у вдосконаленні правового регулювання для захисту прав споживачів, захисту персональних даних та боротьби зі спамом та шахрайством в Інтернеті [17, с. 66].

Сьогоднішній етап відзначається постійними змінами та адаптацією до нових викликів та технологічних тенденцій. Урядові органи, законодавці та регулювальні органи продовжують розробляти нові закони та стандарти, спрямовані на забезпечення безпеки, конфіденційності та захисту прав учасників цифрового простору.

Джерельна база регулювання інтернет-простору в США є основою для стабільного та безпечного функціонування цифрового середовища. Вона визначає права та обов'язки усіх учасників інтернет-спільноти, сприяє розвитку електронної комерції, інновацій та кібербезпеки.

Сьогодні діючі організаційно-правові принципи захисту національного інформаційного простору мають коріння у стратегічному забезпеченні політики безпеки та експлуатації оборонних та управлінських систем у інтересах вищих державних органів. Основні законодавчі засади забезпечення інформаційної безпеки США сформувалися після Другої світової війни, коли американська інформаційна система зіткнулася з негативним впливом

радянської пропаганди. У структурі законодавства США щодо забезпечення інформаційної безпеки відображаються як федеральні, так і штатні закони. Незважаючи на різність законів штатів, акти інформаційного законодавства мають високий рівень уніфікації, оскільки в американському суспільстві розуміють, що безпека інформації держави є важливим засобом гарантування безпеки кожного громадянина [3, с. 44].

Правове регулювання інтернет-простору у Сполучених Штатах Америки (США) є складним та постійно змінюється відповідно до технологічного прогресу та вимог часу. Цей регуляторний механізм є ключовим для забезпечення прав та свобод користувачів, врегулювання електронної комерції, захисту конфіденційності та безпеки даних, боротьби з кіберпротиправністю, та забезпечення загального порядку у цифровому середовищі.

Одним з основних документів, який визначає принципи правового регулювання в інтернет-просторі США, є Конституція Сполучених Штатів. Зокрема, Перший поправка гарантує свободу слова, що має прямий вплив на обмеження регулювання контенту в Інтернеті. Верховний суд США у своїх рішеннях часто визначає права та обов'язки учасників цифрового простору на основі Конституції [20, с. 89].

Значну роль у регулюванні мають федеральні закони. Наприклад, Закон про телекомунікації (Telecommunications Act) містить положення про забезпечення доступу до Інтернету, захисту конфіденційності споживачів і боротьби зі спамом. Інший важливий документ – Закон про захист авторських прав в цифрову епоху (Digital Millennium Copyright Act), що регулює використання контенту в мережі, захищає авторські права та встановлює відповідальність за порушення авторських прав.

Федеральна Комісія з торгівлі (Federal Trade Commission, FTC) відповідає за захист прав споживачів у цифровому середовищі. FTC втручається в справи, пов'язані з випадками обману, недостатньої

конфіденційності даних, порушення правил онлайн-реклами тощо. Діяльність FTC базується на законах про торгівлю та захист споживачів [8, с. 89].

У США також існують деякі спеціалізовані закони, спрямовані на боротьбу з кіберпротиправністю та забезпечення кібербезпеки. Наприклад, Комп'ютерний злочинний закон (Computer Fraud and Abuse Act) накладає кримінальну відповідальність за несанкціонований доступ до комп'ютерних систем. Крім того, існують закони, що регулюють збереження та обмін електронних доказів у кримінальних справах.

Урядові агентства, такі як Федеральна комісія зв'язку (Federal Communications Commission, FCC) та Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST), приймають нормативні акти та стандарти, спрямовані на розвиток та забезпечення безпеки телекомунікацій та інформаційних технологій.

Законодавство штатів також має значний вплив на правове середовище в інтернет-просторі. Багато штатів приймають свої власні закони про захист персональних даних, боротьбу з кіберпротиправністю та інші аспекти цифрової безпеки.

Наприклад, Каліфорнійський Закон про захист приватності споживачів (California Consumer Privacy Act, CCPA) надає споживачам право контролювати свої персональні дані та вимагати видалення цих даних зі зберігання. Цей закон має великий вплив на компанії, які збирають та обробляють особисту інформацію онлайн [31, с. 44].

Основними законами, які визначають адміністрування інформаційної безпеки в США, є закони «Про захист особистої інформації» (1974 р.), «Про таємниці» (1974 р.), «Про розкриття урядової діяльності», «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп'ютерних систем» (1987 р.), «Про комп'ютерні правопорушення та шахрайство» (1986 р.). З ініціативи президента США Р. Рейгана був прийнятий та реалізований Закон «Про свободу інформації», а забезпечення інформаційної безпеки стало пріоритетом

політики Державного департаменту. У 1987 році був ухвалений Закон H.R.-145 «Про забезпечення безпеки електронно-обчислювальних машин», норми якого лягли в основу майбутнього законодавства щодо кібернетичної безпеки. Цей закон вперше в США регламентував статус нового інституту – «інформація обмеженого доступу», що включає важливу, але не класифіковану інформацію для національної безпеки, що перебуває урядових організацій, а також інформацію, яка обробляється в інформаційних системах корпорацій і приватних фірм, які працюють на урядові замовлення [22, с. 122 ;14, с. 56].

Крім законів, велике значення для інформаційної безпеки мають директиви президента США, який керує Радою національної безпеки. Серед них найважливіші: Директива PD/NSC-24 1977 року «Політика щодо захисту систем зв'язку» (вперше зазначено необхідність захисту важливої не класифікованої інформації для національної безпеки), Директива SDD-145 1984 року «Норми національної політики США з питань безпеки систем зв'язку в автоматизованих інформаційних системах» (вперше надано агентству національної безпеки функції забезпечення безпеки інформаційних ресурсів, контролю за безпекою передачі інформації, ліцензування діяльності у сфері захисту інформації) [15, с. 88].

У 1990-х роках, коли інформаційні відносини стали активнішими та більш глобальними, були введені в дію федеральні закони, такі як «Про інформаційну безпеку» та «Про удосконалення інформаційної безпеки» у 1997 році. Додатково, протягом останнього десятиліття XX століття військові стали відігравати значну роль у розробці нормативних актів щодо забезпечення інформаційної безпеки, оскільки інформаційні технології стали важливою складовою військового потенціалу не лише США, але й інших країн, таких як Росія, Китай, Німеччина, Ізраїль та інші. У 1992 році було введено в дію Директиву Міністерства оборони США «Інформаційна війна», яка закріпила необхідність обліку інформаційних ресурсів для підвищення ефективності військових операцій у протидії потенційному супротивнику.

Ця Директива визначила різноманітні аспекти «інформаційної війни», включаючи психологічний вплив на супротивника, оперативну безпеку, дезінформацію, електронне втручання, розвідку, втручання в системи управління супротивника та захист власних систем управління в умовах бойових дій [32, с. 159].

Фактично, введення цієї Директиви прирівняло інформаційну безпеку до військової безпеки на юридичному рівні. Крім того, головним концептом управління інформаційною безпекою стало забезпечення безпеки власних інформаційних ресурсів, одночасно з виведенням з ладу інформаційних систем потенційного супротивника та контролем за його стратегічними комунікаціями.

Слід зазначити, що американська модель забезпечення інформаційної безпеки відкриває можливість ведення інформаційних війн, в яких використовуються активні інформаційно-психологічні операції як інструмент зовнішньої політики [1, с. 44].

Починаючи з 2001 року, під час виступу перед особовим складом ЦРУ, тодішній президент США Джордж Буш наголосив на тому, що забезпечення інформаційної безпеки є головним пріоритетом для національної безпеки країни. Це призвело до запровадження урядових програм захисту національного інформаційного середовища в комп'ютерних мережах. Метою таких програм є створення сприятливих умов для розвідувальних органів для добування та обробки інформації про загрози інформаційному потенціалу державних установ з боку інших держав та осіб. Особлива увага приділяється аналізу відкритих джерел та отриманню інформації із конфіденційних баз даних з використанням комп'ютерного обладнання [33, с. 166]. Це спричинило початок формування нормативно-правової бази для боротьби з протиправністю.

Наприклад, у 2003 році було введено в дію Національну стратегію безпечного кіберпростору, а пізніше були прийняті такі документи як Огляд політики кібербезпеки (2009 рік), Міжнародна стратегія для кіберпростору

(2011 рік), і Директива Президента США щодо стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2013 рік). Ці акти регулюють широкий спектр аспектів забезпечення безпеки електронних інформаційних мереж та ресурсів, а також визначають адміністративні форми взаємодії державних інституцій у боротьбі з кіберзагрозами.

Крім того, з 1997 по 2001 рік у США активно працювали над створенням загальнофедеральної системи електронної аутентифікації. Згідно з Директивою FIPS 186-2 (2000 рік), були введені стандартизовані процедури електронного підпису.

Зауважимо, що у 2009 році в Конгресі був представлений законопроект США «Акт про кібербезпеку» (The Cybersecurity Act of 2009), який надавав президентові повноваження обмежувати доступ до Інтернету у будь-якій місцевості США в разі загрози національній безпеці. Це відзначило початок нової епохи в історії державного регулювання інформаційної безпеки в США, де визначалася ключова роль глави держави в управлінні системою кібербезпеки з метою демонстрації значного управлінського потенціалу президента для розвитку інформаційної сфери та захисту інформаційних проектів на рівні загальнофедерального, регіонального та місцевого значення в галузі кібербезпеки.

Висновки до 1 розділу

Теоретико-методологічні підходи до регулювання інтернет-відносин в США визначаються різноманітними факторами, включаючи правові, політичні, економічні та соціокультурні аспекти. Регулювання інтернету в США базується на різних теоретичних та методологічних підходах, що враховують складність та динамічність цього середовища. Розкриємо ключові теоретико-методологічні підходи до регулювання інтернет-відносин в США:

1. Один із основних підходів полягає в тому, що регулювання інтернету в США базується на правовому реалізмі, який визнає значення закону в управлінні інтернетом. Законодавство, судова практика та правові прецеденти визначають рамки діяльності в Інтернеті, а правові норми встановлюють права та обов'язки різних суб'єктів цього середовища.

2. Інший підхід полягає в застосуванні децентралізованого підходу до регулювання, де влада та відповідальність розподіляються між різними галузевими органами, компаніями, користувачами та іншими зацікавленими сторонами. Цей підхід відображає складність та розмаїття інтернет-середовища, де немає єдиного центру контролю.

3. Принцип відповідальності. Згідно з цим підходом, відповідальність за регулювання інтернету покладається на різні суб'єкти, включаючи урядові органи, компанії, користувачів та громадські організації. Кожен суб'єкт має свої обов'язки та відповідальність за забезпечення безпеки, конфіденційності та етичності в інтернет-середовищі.

4. Ще одним ключовим принципом регулювання є прозорість, яка передбачає відкритість та доступність інформації про правила, політику та практики, які використовуються урядовими органами та іншими суб'єктами для регулювання інтернету. Це сприяє забезпеченню довіри та впевненості користувачів в інтернет-середовищі.

5. Оскільки інтернет постійно змінюється та розвивається, одним із ключових принципів регулювання є гнучкість та адаптивність до нових

технологій, викликів та можливостей. Регулятори повинні бути готові до швидких змін у регулюванні, щоб забезпечити ефективне та ефективне управління інтернетом.

Джерельна база дослідження регулювання інтернет-відносин в США включає різноманітні джерела інформації, які надають різні перспективи та аспекти цієї проблематики. Розглянемо характеристики цієї джерельної бази:

1. Офіційні законодавчі акти, прийняті Конгресом США, є основним джерелом інформації про правовий статус та регулювання інтернет-відносин в країні. Ці документи встановлюють правила, обов'язки та відповідальність стосовно різних аспектів використання Інтернету.

2. Рішення судів, в тому числі Верховного Суду США та окружних судів, надають інтерпретацію законів та вирішують спірні питання, пов'язані з регулюванням інтернету. Аналіз судових рішень дозволяє зрозуміти тенденції та зміни в правовому регулюванні даної галузі.

3. Урядові агентства, такі як Федеральна комісія зв'язку (FCC), Федеральна торговельна комісія (FTC) та інші, публікують звіти, документи та рекомендації щодо регулювання інтернет-відносин. Ці джерела містять аналіз сучасних тенденцій та проблем у галузі інтернету.

4. Академічні дослідження, аналітичні звіти від незалежних дослідницьких організацій та експертні оцінки надають додатковий інсайт у регулювання інтернету в США. Ці джерела можуть містити аналіз ефективності регулятивних заходів, оцінку їх впливу та рекомендації щодо поліпшення.

5. Поза національними джерелами інформації також є міжнародні документи та організації, такі як ООН, Європейський Союз, які розробляють стандарти та рекомендації щодо регулювання інтернет-відносин. Ці документи можуть впливати на регулювання в США через міжнародні зобов'язання та стандарти.

Загалом, джерельна база дослідження регулювання інтернет-відносин в США розмаїта та різноманітна, включаючи офіційні документи, судову

практику, урядові звіти, академічні дослідження та міжнародні документи. Ці джерела надають широкий обсяг інформації та аналізу, необхідного для розуміння регулятивного середовища в галузі інтернету.

Роль джерел права в регулюванні інтернет-відносин в США та в інших країнах з високорозвиненим інтернет-інфраструктурою вельми значима. Інтернет є динамічною сферою, що постійно змінюється, і ефективно регулювання цієї сфери вимагає наявності відповідного правового каркасу, який би враховував технологічні та соціальні аспекти використання Інтернету. Наведемо деякі ключові джерела права, які використовуються для регулювання інтернет-відносин:

1. Закони, прийняті на рівні держави або федерального уряду, визначають правові рамки для використання Інтернету. Це можуть бути закони, які стосуються авторських прав, захисту даних, кібербезпеки, електронної комерції тощо.

2. Рішення судів у справах, що стосуються Інтернету, можуть встановлювати нові юридичні прецеденти та інтерпретації законів. Судова практика може вирішувати питання про захист приватності, свободу слова, відповідальність за вміст інтернет-платформ та інші аспекти відносин в Інтернеті.

3. Урядові агентства та регулятори приймають рішення та розробляють правила, які стосуються використання Інтернету. Це можуть бути положення, стандарти, постанови або рекомендації, які регулюють різні аспекти діяльності в Інтернеті, такі як кібербезпека, адміністративні процедури та вимоги до технічних засобів.

4. Угоди між державами можуть встановлювати спільні стандарти та правила для використання Інтернету. Наприклад, Європейська конвенція про кіберпротиправність та інші міжнародні документи встановлюють правила стосовно кібербезпеки та попередження кіберпротиправності.

5. Великі технологічні компанії можуть розробляти власні кодекси поведінки та стандарти безпеки для користувачів Інтернету. Ці ініціативи

можуть доповнювати державне законодавство та сприяти забезпеченню високих стандартів безпеки та приватності.

6. Власники інтернет-платформ можуть встановлювати свої власні правила та політики використання платформи, які користувачі повинні дотримуватися. Це може включати умови користування, правила щодо вмісту, заходи безпеки тощо.

Загалом, ці джерела права виконують важливу роль у формуванні правового каркасу для регулювання інтернет-відносин, забезпечуючи захист прав користувачів, безпеку мережі та забезпечення ефективного функціонування Інтернету як глобального ресурсу.

РОЗДІЛ 2. ПРАВОВІ ПІДХОДИ ДО ПОЛІТИКИ РЕГУЛЮВАННЯ СОЦІАЛЬНИХ МЕРЕЖ У США

2.1. Вплив медійних транснаціональних корпорацій на регуляторні процеси інтернет простору США та світу

Сучасний розвиток медіа є складним та багатограним явищем, що відображає еклектичне поєднання креативного та фінансового капіталу. На перший погляд, цей процес може видатися суперечливим, проте з іншого боку, він відбувається в гармонії з потребами суспільства у різноманітних інформаційно-розважальних продуктах, що активно створюються на глобальному медійному ринку. Ця динаміка визначається різними структурними блоками сегментації ринку, які відображають емоції споживачів, їх морально-етичні уподобання та інші аспекти, що виникають внаслідок впливу різноманітних ЗМІ.

У світі сформувалися спеціалізовані наукові школи, які досліджують сучасні медіа з різних точок зору та з використанням відповідного інструментарію. Ці школи охоплюють широкий спектр аспектів, включаючи психологічні та біхевіористичні аспекти медіа, економіку медіа, медійний бізнес та інші. Різні дослідники підходять до вивчення медіа з різних точок зору, що сприяє розумінню їхньої складної природи та впливу на суспільство [50, с. 34].

Незважаючи на різноманітність підходів до вивчення медіа, слід відзначити, що сучасний медіа ринок є динамічним та постійно змінюється відповідно до потреб споживачів, політичних та технічних факторів. Великі медійні корпорації впливають на ці зміни шляхом трансферу форматів, продуктів та послуг, що створюються в їхніх межах. Технічні можливості цих корпорацій, такі як висока візуалізація та звукове оформлення, сприяють підвищенню рівня привабливості та доступності медійних продуктів. Однак, варто зазначити, що не всі стратегії та напрями діяльності медійних ТНК є

відкритими для громадськості, що створює виклик для дослідників у розумінні інноваційного та інвестиційного потенціалу цих компаній.

Традиційні методи визначення позицій транснаціональних корпорацій у світовій економіці можуть бути ефективними для ідентифікації медійних компаній. Однак важливо пам'ятати, що ці компанії створюють свої власні унікальні продукти, які через подальші адаптації та модифікації для різних національних ринків набувають нових якостей та споживчого попиту. У цьому контексті важливо враховувати вплив уподобань, емоцій та переконань споживачів, а також творче виконання та мистецтво тих, хто створює медійні продукти, такі як інформаційні блоги, телевізійні та радіо програми, книги та журнали. Ці фактори можуть значно впливати на аудиторію та відображати швидкі зміни у споживчих уподобаннях [50, с. 34].

Сучасна політична, економічна, ментальна та соціальна ситуація також має значний вплив на прибутковість медійних корпорацій, які здебільшого залежать від продажу креативних та інформаційних продуктів та рекламних послуг. Успішність кожної медійної корпорації визначається її здатністю залучити аудиторію, комерціалізувати свої продукти та привернути рекламні компанії. Таким чином, бізнесовий успіх кожної медійної компанії визначається її здатністю залучати аудиторію та ефективно комерціалізувати свої продукти, а також надати рекламодавцям можливість ефективно розміщувати рекламу на своїх платформах.

Отже, при ідентифікації медійних корпорацій дуже важливо з'ясувати їхні особливості [36, с. 65].

Серед найбільш суттєвих можна виділити наступні:

1. Зростання креативної та організаційної складової у створенні конкурентоспроможної бізнес-моделі, яка включає в себе структуру, стратегію та когнітивні підходи впливовості. Як зазначає відомий дослідник медіаіндустрії L. Küng, ключовими елементами цього процесу конгломерації можуть бути когнітивні карти, схеми та фрейми.

2. Збільшення локально-глобальної конкуренції, яка передбачає можливість колаборації між конкуруючими компаніями на різних етапах створення медійних продуктів; аутсорсинг, що дає можливість співпраці користувачів Інтернету з авторами і розробниками форматів, що знаходяться на великих відстанях; зростання доступності та якості глобальної інформаційно-креативної інфраструктури.

3. Конгломерація виробництва, коли до наявного медійного капіталу додаються великі обсяги фінансового, промислового, інтелектуального та інших видів капіталу. Наприклад, компанія SONY розширила свою діяльність, додавши до виробництва традиційної техніки також продюсування музичних, телевізійних форматів та кіно [59, с. 43].

4. Поглинання медіа Інтернетом, яке стало можливим завдяки високій ємності, мобільності та доступності цього виду інформації. Унаслідок цього, протягом 2013-2014 років реклама на телебаченні втратила частку ринку на користь інтернет-реклами.

Дані з 1985 по 2018 рік свідчать про те, що кількість угод про злиття та поглинання у галузі медіа та розваг зростала із 264 до 3 386 щорічно, а їх загальна вартість збільшилася з 54,4 мільярдів до 336,3 мільярдів доларів США. Це стало наслідком значних технологічних змін у медійному бізнесі, особливо від цифровізації починаючи з кінця 1990-х років, швидкого розповсюдження широкосмугового Інтернету, цифрових технологій та медійних стандартів, а також з'явлення високотехнологічних електронних та мобільних медіа [35].

У результаті таких злиттів і поглинань виникли глобальні медіа-імперії, такі як «Time Warner», «Sony», «Bertelsmann», «Berlusconi», «News Corporation», які стали не лише основними гравцями на світовому медійному ринку, але й формували продуктову та географічну сегментацію ринку, розвивали глобальні конкурентні відносини і стали монополістами глобального інформаційного простору.

Прагнення медійних корпорацій постійно диверсифікувати джерела доходів мотивує їх до поглиблення співпраці з акціонерами або до публічного розміщення акцій. Однак міжнародний досвід показує, що публічне розміщення акцій медійних корпорацій часто стає серйозною помилкою для їхнього менеджменту та може загрожувати розвитку демократії.

Злиття та поглинання в галузі медіа індустрії великими за обсягом та вартістю стали результатом не лише фінансових, але й стратегічних цілей медіаконгломератів, які прагнуть максимізувати свою ринкову капіталізацію, підвищити прибутковість бізнесу та скористатися ефектом економії масштабів, консолідувати економічну силу для впливу на ринок та розширити ринкове середовище діяльності [35].

В сукупності зазначені мотиваційні фактори визначають, на нашу думку, умови та ключові параметри глобальної конкуренції у світовій медійній індустрії. Інвестиції у розширення бізнесу, витрати часу та фінансів, а також повне задоволення потреб і запитів споживачів інфотейнменту NTU є критичними для корпорацій у медійній сфері. Інфляційні темпи в їхніх країнах, динаміка процентних ставок на кредитному ринку та їхня волатильність також відіграють важливу роль у прийнятті рішень ППІ медіа компаній. Вони мають значний вплив на прибуток від інвестицій та здатність корпоративних медіа структур реалізувати здорові фінансові стратегії та бізнес-моделі для концентрації колосальної влади та політичного впливу, формування стратегій розвитку провідних газет та журналів, телебачення та радіо.

У наступних десятиліттях кількість корпорацій у медіа бізнесі може навіть зменшитися під впливом наростаючих злиттів та поглинань як одного з найефективніших механізмів забезпечення своєї глобальної конкурентної лідерності.

Щодо угод злиття та поглинань у світовій медіа індустрії, найбільшими за обсягом у 2018 році були купівля компанією «АТ&Т» (другим за величиною ринкової капіталізації американський провайдер бездротового зв'язку) компанії «Time Warner» (найбільший у світі виробник телевізійних шоу і

фільмів та власник «HBO» і «CNN») за 79,1 мільярд доларів США; поглинання компанією «Disney» компанії «Fox» за 71,3 мільярд доларів; придбання компанією «Comcast» компанії «Sky» за 39 мільярдів доларів, а також придбання компанією «T-Mobile» компанії «Sprint» за 26 мільярдів доларів.

З іншого боку, постійне загострення міжнародної конкурентної боротьби між медійними корпораціями за глобального споживача змушує їх знижувати або навіть скасовувати абонентську плату за споживання медійних продуктів. Основні мотиви цього полягають, по-перше, у розгляді медіакомпаніями своєї аудиторії як споживачів реклами, що стимулює їх до покупки рекламованих товарів; по-друге, у швидкому розвитку технологій потокового та мобільного відео, що призводить до зростання популярності відмови від платного телебачення через його недостатнє задоволення медійних потреб і запитів споживачів [49, с. 83].

Вплив медійних транснаціональних корпорацій на регуляторні процеси в Інтернет-просторі США та по всьому світу є предметом значного дослідження і обговорення. Ці корпорації, такі як Google, Facebook, Amazon та інші, займають домінуючі позиції в інтернет-індустрії і мають значний вплив на контент, який ми споживаємо, та на спосіб, яким ми сприймаємо інформацію. Їхні дії та рішення часто мають великий вплив на політичну, соціальну та економічну ситуацію в країні та світі.

Поза лобіюванням законодавства, медійні транснаціональні корпорації також мають значний вплив на регулювання Інтернет-простору через свої взаємодії з урядовими органами і регуляторами. Вони активно співпрацюють з різними групами та комітетами, які відповідають за розробку і впровадження правил і політик у цій сфері. Ця співпраця може призвести до створення різних ініціатив та програм, спрямованих на підтримку або регулювання ринку, що може відображати інтереси цих корпорацій. Крім того, через свій вплив на галузеві асоціації та стандартизаційні організації, вони можуть впливати на встановлення технічних стандартів і правил, які визначають, як саме працює Інтернет. Це може включати розробку стандартів щодо безпеки, приватності,

доступності та інших аспектів, які впливають на користувачів інтернет-сервісів. Такі взаємодії можуть відбуватися як на національному, так і на міжнародному рівнях, враховуючи глобальну природу інтернету та медійних корпорацій.

Безумовно, медійні транснаціональні корпорації не лише впливають на законодавство та регуляторні процеси, але й мають значний контроль над формуванням внутрішніх правил і політик платформ Інтернету. Вони часто встановлюють власні правила щодо контенту, який може бути опублікований на їхніх платформах, і мають повноваження видаляти чи блокувати контент, який вони вважають неприйнятним або порушуючим їхні правила користування. Це ставить під загрозу свободу слова та доступ до різноманітної інформації, оскільки медійні корпорації можуть встановлювати власні стандарти та цензурувати контент відповідно до своїх власних інтересів або політичних переконань. Такий контроль може мати серйозні наслідки для суспільства, включаючи обмеження доступу до інформації, цензуру та викривлення публічного діалогу. Тому важливо виробляти механізми контролю за впливом медійних корпорацій на формування правил та політик платформ Інтернету з метою забезпечення захисту свободи слова та доступу до об'єктивної інформації для всіх користувачів [48].

Безумовно, одним зі значущих аспектів впливу медійних транснаціональних корпорацій є їхня роль у зборі та використанні особистих даних користувачів. Ці корпорації активно збирають величезні обсяги даних про своїх користувачів на своїх платформах, включаючи інформацію про їхній вік, зацікавленості, розташування, інтеракції з контентом та інше. Ці дані потім використовуються для персоналізації рекламних кампаній, аналізу поведінки користувачів та інших комерційних цілей. Проте, цей підхід також може породжувати серйозні питання щодо приватності користувачів та етики використання їхніх особистих даних. Збір та використання великих обсягів особистої інформації без належного контролю та дозволу може призвести до порушення приватності та конфіденційності користувачів. Крім того, існує

ризик використання цих даних для маніпуляції поведінкою користувачів або здійснення впливу на їхні вподобання та переконання. У зв'язку з цим, важливо розвивати ефективні механізми захисту приватності та контролю за використанням особистих даних користувачів медійними корпораціями. Це може включати в себе встановлення строгих правил щодо збору та використання особистих даних, забезпечення прозорості та доступу до інформації про те, яким чином дані збираються та використовуються, а також механізми контролю та забезпечення згоди користувачів на обробку їхніх особистих даних [16 с. 78].

Медійні транснаціональні корпорації мають потужний вплив на розвиток технологій та інновацій в інтернет-індустрії. Вони володіють значними фінансовими ресурсами і можуть інвестувати у стартапи та нові технології, що сприяє швидкому розвитку і впровадженню інноваційних рішень. Крім того, ці корпорації активно здійснюють придбання інших компаній, що сприяє консолідації галузі та стимулює конкуренцію через створення синергії та об'єднання технологічних ресурсів. Однак, великий вплив медійних корпорацій на інновації може мати як позитивні, так і негативні наслідки. З одного боку, їхня активна участь у фінансуванні та розвитку нових технологій може стимулювати конкуренцію та сприяти розвитку новаторських ідей. Вони можуть створювати умови для зростання маленьких інноваційних підприємств шляхом інвестування у них та надання доступу до своїх ресурсів та експертизи. З іншого боку, домінування великих медійних корпорацій може пригнічувати конкуренцію та інновації в галузі. Вони можуть використовувати свою фінансову потужність для придбання конкуруючих компаній або блокування виходу нових учасників на ринок. Це може призвести до зниження рівня конкуренції та інноваційного розвитку, оскільки менші гравці можуть мати обмежений доступ до ресурсів та можливостей.

Отже, важливо збалансувати вплив медійних транснаціональних корпорацій на розвиток технологій та інновацій, забезпечивши належний

рівень конкуренції та зберігаючи простір для малих та середніх підприємств. Це може вимагати розвитку ефективного регулювання, що сприяє захисту конкуренції та сприяє розвитку інноваційних рішень в інтересах суспільства в цілому.

2.2. Нормативно-правове регулювання діяльності американських соціальних мереж

Регулювання кібербезпекових питань в Сполучених Штатах Америки є однією з ключових сфер, яка потребує уваги, особливо в контексті їхнього статусу як однієї з провідних країн у світі як в економічному, так і військовому аспектах. Система нормативно-правового регулювання кіберзахисту в США варто ретельно розглянути, оскільки ця країна визнана лідером у галузі інформаційної безпеки. Навіть у порівнянні з Японією, яка вважається своєрідною меккою цифрових технологій, США опережають її більш ніж на п'ять років у сфері поширення персональних комп'ютерів, кабельного телебачення та інших аспектів інформаційної політики.

Законодавство Сполучених Штатів визначає кібербезпеку як захист інформаційних систем та збереження або передачу інформації через них від кіберзагроз або порушень безпеки. Важливо враховувати, що контроль безпеки, визначений як управління, експлуатаційний і технічний контроль, використовується для захисту від несанкціонованих втручань з метою негативного впливу на конфіденційність, цілісність та доступність інформаційної системи або її інформації [19].

Законодавство у сфері забезпечення інформаційної безпеки в США базується на федеральних і штатových законах, які встановлюють правову основу для розвитку єдиної державної політики з метою захисту інтересів національної безпеки. Серед таких законів можна виокремити «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997

р.), «Про комп'ютерне шахрайство та зловживання» (1986 р.), «Про свободу інформації» (1967 р.), та інші.

Таким чином, система регулювання кібербезпекових питань в США є складною та деталізованою, і вона базується на ретельно розроблених законах і нормативах, спрямованих на забезпечення захисту інформаційних систем та даних від кіберзагроз та інших порушень безпеки [4, с. 133].

У практичному плані кіберзахисту у США, до нещодавнього часу головним виконавчим органом в цій сфері був Центр комп'ютерної безпеки (National Computer Security Center, NCSC), який був створений на базі Агенції національної безпеки (National Security Agency, NSA) у червні 2003 року та був підпорядкований Міністерству внутрішньої безпеки (Department of Homeland Security, DHS). Недавно, у 2018 році, цей центр було реорганізовано в Національний центр кібербезпеки й інтеграції зв'язку (National Cybersecurity and Communications Integration Center, NCCIC), який став складовою частиною новоствореного Агентства з кібербезпеки та інфраструктурної безпеки (Cybersecurity and Infrastructure Security Agency, CISA). CISA став головним органом у координації питань кіберзахисту та інфраструктурної безпеки в Сполучених Штатах. Він розвиває національні можливості з протидії кібератакам, співпрацює з федеральними установами для забезпечення кібербезпеки та надає технічну допомогу та оцінку для власників інфраструктури та операторів у всій країні. Співпрацюючи з публічним та приватним секторами, CISA забезпечує безпеку та стійкість мережі та надає необхідні ресурси для захисту державних інформаційних мереж [4, с. 134]. Законодавство у сфері зовнішньої інформаційної безпеки в США представлено рядом федеральних законів, законів штатів та нормативних актів, які формують правову базу для створення та реалізації державної політики у цій сфері. До найважливіших з них належать «Національна стратегія захисту кіберпростору» (2003 р.), «Огляд з кібербезпеки» (2009 р.), «Ініціатива зі всебічної національної кібербезпеки» (2010 р.), Стратегія

кібербезпеки США (2011 р.) та Закон CISPА (2012 р.) (Cyber Intelligence Sharing and Protection Act).

У вересні 2018 року в Сполучених Штатах була ухвалена Національна кіберстратегія, яка визначає основні завдання у цій області. Серед них:

- захист Батьківщини шляхом забезпечення безпеки мереж, систем, функцій та даних;
- сприяння розвитку безпечної, розвинутої цифрової економіки та сильних інновацій;
- збереження миру та безпеки через зміцнення здатності США, узгодженої з союзниками та партнерами, до стримування та, за необхідності, покарання тих, хто використовує кіберзасоби у шкідливих цілях;
- розширення американського впливу за кордоном, спрямованого на поширення основних принципів відкритої, сумісної роботи та надійного та безпечного Інтернету.

Ця стратегія також визначає, що Сполучені Штати перебувають у постійній конкуренції зі стратегічними противниками, шахраями, терористичними та протиправними мережами. Зокрема, Китай, Іран і Північна Корея використовують кіберпростір для виклику США та їхніх союзників, часто з великою обачністю. Ці противники використовують кіберзасоби для підриву американської економіки та демократії, крадіжки інтелектуальної власності та посіву розбрату у демократичних процесах [21, с. 6].

Окрім цього, важливим елементом цієї стратегії є визначення та встановлення неприйнятної поведінки в кіберпросторі. Сполучені Штати продовжують розвивати консенсус щодо відповідальної державної поведінки в цьому просторі та працюють над забезпеченням наслідків для неприйнятної поведінки, яка завдає шкоди США та їхнім партнерам. Для цього використовуються всі інструменти національної влади, включаючи дипломатичні, інформаційні, військові та правоохоронні можливості.

Іншим важливим законом є Закон про захист електронних комунікацій, який має на меті захист інформації як у сховищах, так і під час передавання.

Згідно з цим законом та розділом 17 Кодексу Сполучених Штатів, параграф 20702 кримінальною дією вважається навмисний доступ без авторизації або обхід авторизованого доступу до послуг електронної комунікації, що може включати провайдерів електронної пошти або навіть роботодавців, які надають своїм працівникам електронну пошту. Однак персональні комп'ютери не вважаються послугами електронної комунікації. Такі порушення підлягають покаранню, яке може варіюватися від одного року за перше порушення без протиправної мети (а також порушення, що здійснюються не з комерційною метою або для завдання знищення інформації), до 10 років за повторне порушення або порушення з протиправною метою [19].

Також варто відзначити, що законодавство США містить окремі норми, які регулюють такі правопорушення, як хакерство (тобто несанкціонований доступ). Згідно з цими законами покарання можуть бути до 10 років за доступ до національної секретної інформації або, наприклад, лише до одного року ув'язнення за просте отримання інформації, або до п'яти років, якщо існують обтяжуючі обставини.

Іншим видом правопорушення є здійснення атаки на відмову обслуговування (DOS-атака), яка спрямована на припинення роботи сервісів. Залежно від наслідків та завданої шкоди, термін ув'язнення може бути до 10 років. Ще одним видом порушення є фішинг. Згідно з різними законами потенційне покарання може сягати до 20 років ув'язнення.

Також варто зазначити, що зараження комп'ютерних систем шкідливим програмним забезпеченням, таким як шпигунські програми або віруси, також може бути кваліфіковано як правопорушення згідно з нормами законодавства США. Проте для цього необхідно довести, що порушення було здійснене навмисно й завдано шкоду. Покарання за такі дії може бути до 10 років ув'язнення.

Також важливо відзначити правопорушення, яке в Україні не є широко поширеним, а саме електронну крадіжку. Це означає порушення безпеки

чинного або колишнього працівника, або порушення прав інтелектуальної власності, таке як порушення прав авторського права. Згідно з деякими умовами та законодавчими актами це порушення може також включати компоненти крадіжки інтелектуальної власності та комерційних таємниць відповідно до законодавства США. Це правопорушення вважатиметься правопорушенням, якщо, по-перше, доступ до мережі був здійснений без відповідної авторизації, і по-друге, комерційні таємниці були передані з користю для іноземного уряду, а також якщо така крадіжка може призвести до економічних вигід для інших або завдати шкоду ринку, на якому відбулася крадіжка [34, с. 67].

Отже, з проведеного аналізу можна зробити висновок, що законодавство Сполучених Штатів Америки є досить ретельним та всебічним у справах кіберзахисту та забезпечення кібербезпеки. На федеральному рівні існує загальний рівень законодавства та політики в цьому питанні, який відображає важливість забезпечення кібербезпеки як для всієї країни, так і для її установ, громадян, а також виражає рішучість щодо протистояння в цьому полі. До цього питання також входить забезпечення кібероборони країни. Як показує аналіз, в США створено потужну систему державних органів, які забезпечують кібербезпеку країни та протистоять викликам у кіберпросторі. Щодо регулювання діяльності у кіберпросторі на федеральному та штатному рівнях, певні правопорушення підпадають під юрисдикцію всієї країни, що регулюється Кодексом США та відповідними законами, які діють на всій території країни. Однак аналіз показує, що майже неможливо знайти правопорушення, які класифіковані як правопорушення лише у певних штатах.

Нормативно-правове регулювання діяльності американських соціальних мереж в останні роки стало предметом широкого дискурсу і публічного обговорення. З появою та стрімким розвитком цих платформ, законодавчі органи змушені були адаптуватися до нових викликів та реалій цифрового

світу. В цьому контексті виявляються як певні тенденції розвитку, так і недоліки у нормативному регулюванні.

Однією з основних тенденцій є зростання уваги до захисту приватності користувачів у соціальних мережах. В останні роки стали відомі випадки порушень конфіденційності даних, які стосуються великих платформ соціальних мереж. Ці скандали породили серйозні обговорення та вимоги до законодавчих органів з прийняття нових законів та політичних регуляцій.

Одним із яскравих прикладів такої реакції є вступ в дію Загальної регламентації щодо захисту даних (GDPR) у 2018 році в Європейському Союзі. Цей закон встановлює вимоги до компаній, які обробляють особисті дані, щоб забезпечити високий рівень захисту цих даних та отримувати згоду від користувачів на їх обробку. Відтак, цей приклад суттєво вплинув на законодавство інших країн, зокрема США, де було запропоновано кілька законопроектів, спрямованих на зміцнення захисту особистої інформації на соціальних мережах. Другою тенденцією є збільшення уваги до боротьби з дезінформацією та фейковими новинами. Після того, як стало відомо про вплив фейкових новин на громадську думку, законодавці активно обговорювали можливості регулювання цього явища. Низка законопроектів, спрямованих на боротьбу з дезінформацією, була запропонована та обговорена в Конгресі. Однак, прийняття ефективних законів у цій сфері є складним завданням, оскільки важко визначити межу між свободою слова та поширенням шкідливої інформації. З іншого боку, одним з недоліків нормативного регулювання є недостатня реакція на антимонопольні практики великих соціальних мереж. Попри те, що платформи, такі як Facebook, Twitter та Instagram, мають домінуюче становище на ринку соціальних мереж, реальних заходів для запобігання монополізації цього сектору поки що не приймалося. Більше того, існуючі закони про антимонопольну діяльність часто виявляються недостатніми для ефективного контролю над діяльністю цих компаній.

Таким чином, усвідомлення значення захисту приватності та боротьби з дезінформацією стає все більшим у контексті регулювання діяльності соціальних мереж. Однак, існують проблеми, такі як недостатня реакція на антимонопольні практики, які потребують уваги та вирішення з боку законодавців. Ще однією тенденцією є збільшення уваги до боротьби з дезінформацією та фейками. Після виборів у США 2016 року, коли було виявлено значний вплив фейкових новин у соціальних мережах на громадську думку, законодавці розпочали активно обговорювати можливість регулювання цього явища. Низка законопроектів, спрямованих на боротьбу з дезінформацією, була запропонована та обговорена в Конгресі. Проте, прийняття ефективних законів у цій сфері стикається зі складнощами, оскільки не завжди чітко визначається межа між свободою слова та поширенням шкідливої інформації [19].

Розглядаючи іншу сторону медалі, можна зазначити, що одним з недоліків нормативного регулювання є недостатня реакція на антимонопольні практики великих соціальних мереж. На сьогоднішній день платформи, такі як Facebook, Twitter та Instagram, належать до лідерів на ринку соціальних мереж, володіючи домінуючим становищем. Проте, дійсні заходи для запобігання монополізації цього сектору поки що не були належним чином реалізовані. Зокрема, це стосується того, як влада взаємодіє з цими компаніями і контролює їхню діяльність на ринку. Незважаючи на те, що деякі країни приймають закони про антимонопольну діяльність, які мають на меті обмеження домінуючого становища таких компаній, існуючі правові норми не завжди вистачають для ефективного контролю за їхніми діями [4, с. 136].

У зв'язку з цим, виникає необхідність у вдосконаленні законодавства і прийнятті нових заходів для регулювання діяльності соціальних мереж з погляду антимонопольних аспектів. Наприклад, можуть бути розроблені нові закони, які обмежують здатність компаній до придбання конкурентів або об'єднання з іншими компаніями, які мають потенційний конкурентний вплив.

Також можуть бути встановлені більш жорсткі вимоги щодо дотримання антимонопольних правил у сфері цифрових технологій та соціальних мереж.

Загалом, недостатня реакція на антимонопольні практики великих соціальних мереж є серйозним недоліком у сфері нормативного регулювання. Це питання потребує уваги з боку законодавців та вимагає прийняття конкретних заходів для забезпечення конкурентного середовища на ринку соціальних мереж.

2.3. Роль Верховного суду США та інших правоохоронних органів щодо політики контролю соціальних мереж

При обговоренні модерування контенту в Інтернеті часто звертають увагу на два ключові юридичні документи в Сполучених Штатах: Першу поправку до Конституції США та розділ 230 Закону про порядну комунікацію (Communications Decency Act) прийнятого в 1996 році.

Перша поправка до Конституції гарантує свободу слова, преси та зборів, та забороняє державній владі втручатися у інформаційний простір та запроваджувати цензуру, включаючи й інтернет. З іншого боку, розділ 230 Закону про порядну комунікацію надає онлайн-платформам, таким як Twitter і Facebook, імунітет від відповідальності за контент, який розміщують їхні користувачі, і дає їм право самостійно модерувати спілкування, видаляти недоречний контент.

Законодавство у США не дозволяє державним органам впливати на те, що публікують користувачі у соціальних мережах. Тому модерування контенту стає відповідальністю компаній-провайдерів. Twitter, Meta, Google та інші платформи встановили внутрішні правила, які визначають допустимі норми поведінки на їхніх сервісах. Якщо користувач порушує ці правила, йому може бути обмежено доступ до функцій платформи або навіть заблоковано обліковий запис. Соціальні мережі регулярно видаляють тисячі дописів, коментарів та згадок, переважно використовуючи штучний інтелект, а іноді й

живих модераторів. Деякі компанії звертаються до зовнішніх експертів, таких як фактчекери, для перевірки інформації на достовірність. Деякі соціальні мережі також мають незалежні наглядові органи, які переглядають рішення компаній щодо модерування контенту [70].

Протягом тривалого часу такий стан речей в основному задовольняв користувачів, соціальні мережі та уряд США. Однак протягом останнього десятиліття соціальні мережі все частіше потрапляли під критику через те, що стали зручним майданчиком для поширення дезінформації: від фейкових новин про COVID-19 до масових кампаній впливу на виборчі процеси. У той же час, виникли свідчення експертів компаній, які наголошували, що соціальні мережі навмисно налаштовують свої алгоритми так, щоб найчастіше пропонувати користувачам суперечливий або токсичний контент і, внаслідок цього, підвищити їхню залученість. Крім того, час від часу надходить інформація про те, що через дію алгоритмів Facebook, Twitter і YouTube можуть пропонувати екстремістський контент або теорії змов, що спонукають потенційних терористів до дій.

Незважаючи на всі ці свідчення про нездатність соціальних мереж самостійно регулювати контент, якщо будь-який американець подає позов через порушення його прав проти компаній Meta або Twitter, він майже завжди отримує відмову. Судова система США, посилаючись на розділ 230 Закону про порядну комунікацію, стверджує, що платформи не несуть відповідальності за контент, який на них публікується. Проте зараз, коли події в Інтернеті можуть мати серйозні наслідки в реальному світі, все більше позовів потрапляють до Верховного суду США, чия реакція може змінити цю ситуацію [70].

Головною темою двох судових позовів, які Верховний суд США розглянув у кінці лютого 2023 року, є право соціальних мереж не нести відповідальності за контент, що розміщується на їхніх платформах.

У першому з цих позовів, Гонсалес проти «Гугл», сім'я американця, що загинув у 2015 році внаслідок нападу прихильників «Ісламської держави» у

Парижі, стверджує, що «YouTube», який є власником «Google», частково несе відповідальність за цей напад. Вони аргументують, що «YouTube» сприяє тероризму та порушує антитерористичне законодавство США, рекомендуючи користувачам відео, що пропагують діяльність «Ісламської держави» [9, с. 49].

Другий позов, Таамнех проти «Твіттер», звинувачує цю соціальну мережу в сприянні поширенню екстремістських ідей. Родичі загиблого під час нападу «Ісламської держави» на нічний клуб у Стамбулі у 2017 році стверджують, що «Twitter» пропонував користувачам відео та твіти прихильників терористичної організації, що підбурювало їх приєднатися до терористів. У обох справах позивачі настоюють на тому, що алгоритми «YouTube» та «Twitter» є роботою самої компанії, а не просто контентом, створеним користувачами. Вони наголошують, що ці соціальні мережі не є лише нейтральними платформами, але й активно визначають, що рекомендувати для перегляду конкретним користувачам. Через це, на думку позивачів, вони несуть відповідальність за поширення незаконного контенту на своїх платформах.

Соціальні мережі вже відреагували на судові позови, застерігаючи, що вироки проти «YouTube» і «Twitter» можуть призвести до припинення всіх алгоритмічних рекомендацій в Інтернеті. Це може негативно вплинути на функціонування більшості інтернет-сервісів, включаючи пошукові системи, які використовують алгоритми для надання точної відповіді на запити користувачів. Проте Міністерство юстиції США зазначило, що будь-які обмеження будуть застосовані лише до конкретних запитів користувачів (наприклад, «ІДІЛ» або «тероризм»), тому вплив на інтернет загалом ймовірно буде обмеженим [66].

У той час як попередні справи стосувалися права соцмереж на розміщення контенту для користувачів, два інші кейси, які потрапили на розгляд Верховного суду США, мають справу з цензурою. Після подій, які відбулися поблизу Капітолію у січні 2021 року, коли «Facebook» та «Twitter» заблокували акаунт Дональда Трампа, політика модерування соціальних

мереж стала предметом критики. Деякі користувачі вважали, що такі дії компаній порушують свободу слова, а інші вважали, що соціальні мережі не мають права втручатися у вибір контенту для користувачів. Проте найбільш голосно критикувала Республіканська партія, звинувачуючи соцмережі у «придушенні голосів консерваторів і приховуванні правдивих новин та інформації». Щоб уникнути подібних блокувань у майбутньому, Техас та Флорида, традиційно консервативні штати, прийняли закони, що забороняють будь-яку форму цензури у соцмережах. Обидва штати посилаються на Першу поправку до Конституції США, яка гарантує свободу слова, як обґрунтування цих законів.

Закон Техасу має за мету запобігти великим соціальним мережам дискримінувати користувачів за їхніми переконаннями. Він містить кілька винятків, таких як можливість видалення контенту, що підбурює до насильства або порушує антидискримінаційне законодавство. Також вимагається, щоб соцмережі розробляли прозорі процедури для подання скарг користувачами, розкривали свою політику модерування контенту та публікували «Звіт про прозорість» не рідше, ніж раз на два роки. Цей закон поширюється на платформи з більш як 50 мільйонами користувачів, що охоплює технологічних гігантів, таких як «Мета», але не застосовується до соцмережі Truth Social, створеної Дональдом Трампом [66].

Закон Флориди передбачає, що кожна соцмережа повинна детально обґрунтовувати свої рішення щодо модерації контенту. Це вимагає, щоб платформи пояснювали кожне рішення, яке призводить до виключення користувача, цензури або застосування тіньового бану. Закон також забороняє платформам блокувати політичних кандидатів та журналістів. У Флориді цей закон також обмежений на великі платформи, залишаючи поза межами менш популярні соціальні мережі.

Після ухвалення законів у Флориді та Техасі у 2021 році представники великих соціальних мереж подали до суду, спробуючи блокувати це законодавство. Вони посилаються на Першу поправку до Конституції США,

стверджуючи, що мають право самостійно вирішувати, який контент розміщувати на своїх платформах. У Флориді суд прийняв їхню сторону, визнавши, що закон порушує права платформ. Але в Техасі суддя підтримав законодавців, заявивши, що «корпорації не мають права цензурувати те, що говорять люди». Різні рішення судів у різних штатах заставляють Верховний суд втрутитися та вирішити, чи мають соціальні мережі право необмежено модерувати контент.

На сьогоднішній день очевидно, що інтернет став не лише майданчиком для вільного вираження думок та знаходження однодумців, але й простором для поширення дезінформації, впливу на політичні процеси та поширення ненависті та заговорів. Свобода слова, яка раніше була невід'ємною частиною інтернет-спілкування, тепер піддається сумнівам. Оскільки соціальні мережі самостійно модерують контент, вони можуть видаляти матеріали, спираючись на власні переконання щодо цих ідей чи подій, замість того, щоб діяти як нейтральні платформи [78].

Останні кілька років свідчать про значні зміни у поглядах законодавців різних країн на автономію соціальних мереж. Якщо раніше вони розглядались як приватні компанії, над якими держава не має влади, то сьогодні в багатьох демократичних країнах поступово встановлюються обмеження для їхньої самостійності. Наприклад, в Індії було введено прямий урядовий контроль над іноземними соціальними мережами, такими як Twitter або Facebook, зобов'язавши їх допомагати правоохоронним органам у виявленні порушників закону. Недавно Європейський Союз прийняв Загальний регламент про захист даних (GDPR), який розширює повноваження держав у сфері соціальних мереж, дозволяючи видаляти незаконний контент і зобов'язуючи платформи докладати більше зусиль у боротьбі з небезпечними матеріалами. У свою чергу, британський уряд з 2019 року працює над широкомасштабним законопроектом, спрямованим на максимальне регулювання діяльності соціальних мереж.

Майбутнє рішення Верховного суду США у вищезгаданих справах також визначатиме курс дії соціальних мереж. Якщо суд підтримає позивачів у справах Гонсалеса і Таамнеха, це може призвести до того, що «Гугл», «Твіттер» і «Мета» втратять свою правову імунітетність відносно контенту, що публікується на їхніх платформах. Крім того, їхня відповідальність за розповсюдження незаконної або неправдивої інформації може значно зрости [67, с. 56]. У кінцевому підсумку рішення Верховного суду допоможе визначити, чи є соціальні мережі просто нейтральними платформами для обміну інформацією згідно з американським законодавством, чи все ж вони компаніями, які активно беруть участь у створенні контенту за допомогою своїх алгоритмів. З іншого боку, якщо Верховний суд прийме сторону Техасу і Флориди з приводу законодавства, соціальні мережі, навпаки, будуть змушені дозволяти будь-який контент на своїх платформах, щоб уникнути звинувачень у цензурі. Водночас модерація контенту буде проводитися лише в найекстремальніших випадках, що стосуються правопорушень чи правопорушень проти дітей. За словами журналістів, це може призвести до того, що інтернет-простір стане місцем необмеженого поширення інформації, що зруйнує всі зусилля соціальних мереж у боротьбі з дезінформацією (Official website of the Department of Homeland Security)

Безумовно, в умовах конфлікту між Росією та Україною, який не менш активно розгортається й на інформаційному полі, Україна також повинна уважно спостерігати за рішеннями Верховного суду США. Перш за все, вирок щодо відповідальності соціальних мереж за контент може виявитися корисним у протистоянні російській пропаганді на платформах, таких як Facebook та Twitter. У такому випадку соціальні мережі будуть нести більшу юридичну відповідальність, що змусить їх уважніше фільтрувати інформацію та детальніше розглядати скарги, щоб уникнути спрощених звинувачень у спонуканні до насильства або поширенні дезінформації. Однак, якщо йти далі і розглядати рішення стосовно законів Техасу та Флориди, відмова Верховного суду у праві соцмереж на самостійне модерування контенту може негативно

вплинути і на нашу здатність протистояти російським наративам. Зрештою, досвід США та інших країн свідчить про те, що соціальні мережі можна регулювати на рівні законодавства. Це стане важливою передумовою для нашої інформаційної стійкості після завершення війни.

Роль Верховного суду США та інших правоохоронних органів у сфері політики контролю соціальних мереж в сучасному світі набуває все більшої важливості і значущості. Спілкування через соціальні мережі стало не лише популярним засобом обміну інформацією, але й важливим фактором впливу на громадську думку, формування політичних переконань та мобілізацію громадськості. Проте разом із зростанням впливу соціальних мереж з'являються й питання стосовно їхньої відповідальності, ролі у формуванні громадської думки, а також необхідності контролю за їхньою діяльністю з точки зору закону та прав людини.

Спроби заборони та регулювання діяльності соціальних мереж стали об'єктом уваги багатьох країн у світі. В такому контексті роль Верховного суду США, який є вищим органом судової влади у Сполучених Штатах, визначається не лише у вирішенні конкретних правових питань, а й у встановленні прецедентів, які мають велике значення для суспільства в цілому.

Одним із ключових аспектів ролі Верховного суду США є його вплив на визначення обсягу відповідальності соціальних мереж за контент, який з'являється на їхніх платформах. Питання про те, чи мають соціальні мережі бути відповідальними за контент користувачів, стало предметом активних обговорень і судових процесів у США та інших країнах. Верховний суд вирішує, наскільки широко має тягнутися відповідальність соціальних мереж за контент, який публікують їхні користувачі[71].

Зважаючи на потенційні наслідки для свободи слова та прав людини, рішення Верховного суду в цьому питанні може мати значний вплив на діяльність соціальних мереж як у США, так і в інших країнах світу. Крім того, Верховний суд має важливу роль у вирішенні конкретних судових справ,

пов'язаних з діяльністю соціальних мереж. У процесі розгляду справ про порушення законодавства щодо контенту, Верховний суд приймає рішення, які можуть визначити стандарти та правила, якими мають керуватися соціальні мережі у своїй діяльності. Ці рішення можуть визначити, які види контенту можуть бути видалені, які – залишені, і які заходи повинні бути вжиті для боротьби з незаконним або шкідливим контентом. Крім Верховного суду, правоохоронні органи також відіграють ключову роль у контролі за діяльністю соціальних мереж. Поліція, прокуратура та інші правоохоронні органи мають повноваження вживати заходів щодо запобігання та розслідування правопорушень, пов'язаних з використанням соціальних мереж. Вони також можуть взаємодіяти з платформами, щоб виявити та видаляти контент, який порушує законодавство.

У висновку слід зазначити, що роль Верховного суду США та інших правоохоронних органів у політиці контролю соціальних мереж виявляється ключовою для забезпечення правового регулювання їхньої діяльності. Вирішення судових справ та встановлення прецедентів Верховним судом, спільно з діями правоохоронних органів, визначає обсяг відповідальності соціальних мереж, стандарти контролю за контентом і заходи щодо боротьби з порушеннями законодавства. Це важлива складова для забезпечення безпеки, прав людини та захисту громадської думки в онлайн середовищі, що має вирішальне значення для функціонування сучасного суспільства.

Висновки до 2 розділу

Вплив медійних транснаціональних корпорацій на регуляторні процеси в інтернет-просторі США та на світовому рівні є значущим і багатогранним. З одного боку, ці корпорації мають значні фінансові та технологічні ресурси, які надають їм можливість активно впливати на формування політики у сфері інтернету через лобістську діяльність, фінансовий тиск та ініціативи в регуляторній сфері. Водночас вони стикаються з численними викликами й обмеженнями, що виникають унаслідок правових вимог, суспільного тиску та конкурентної боротьби. Такий вплив може призводити до різних наслідків: з одного боку, завдяки економічній та політичній силі медійні корпорації здатні зміщувати пріоритети регуляторів у бік власних інтересів, що може бути небезпечним з точки зору інтересів користувачів та суспільства в цілому. З іншого боку, вони активно підтримують інновації та сприяють підвищенню якості інтернет-послуг через власні ініціативи та інвестиції у дослідження і розробки, що позитивно впливає на розвиток цифрових технологій.

Збалансований підхід до впливу медійних корпорацій на регуляторні процеси є критично важливим для збереження рівноправності всіх зацікавлених сторін. Забезпечення прозорості, відкритості та залучення громадськості у процес ухвалення рішень є необхідними елементами ефективної регуляторної політики в інтернет-сфері. Регулювання, яке враховує інтереси всіх учасників ринку і суспільства загалом, дозволить створити більш справедливе і безпечне інтернет-середовище, де буде досягнуто балансу між комерційними інтересами корпорацій та правами і свободами користувачів.

Роль Верховного суду США та інших правоохоронних органів у контролі за діяльністю соціальних мереж є особливо важливою для забезпечення правової стабільності, справедливості та захисту прав громадян у цифровому просторі. Верховний суд, виступаючи як вирішальний орган, формує ключові правові принципи та стандарти, які регулюють діяльність соціальних мереж у США. Його рішення мають значний вплив на політику

контролю за контентом, відповідальність платформ за поширення незаконного чи шкідливого матеріалу, а також на права користувачів, включаючи свободу вираження думок і захист приватності. Така роль Верховного суду забезпечує регулювання цифрового простору в рамках загальних правових норм та стандартів, що є важливим для формування стійкої правової системи у сфері інтернету.

Водночас, діяльність Верховного суду США не лише забезпечує правову основу для контролю над соціальними мережами, а й відіграє важливу роль у створенні прецедентів, які стають орієнтирами для правозастосування у сфері інтернет-комунікацій. Судові рішення з таких питань, як свобода слова, захист особистих даних, а також відповідальність платформ за контент, слугують основою для подальшого розвитку законодавства та його адаптації до змін у цифровому середовищі. Зокрема, Верховний суд, оцінюючи дії соціальних мереж у конкретних справах, впливає на формування правової доктрини щодо меж допустимого контенту, а також встановлює стандарти для захисту громадськості від неправдивої інформації, маніпуляцій та порушень прав користувачів.

Інші правоохоронні органи також беруть активну участь у забезпеченні дотримання нормативно-правових актів, спрямованих на регулювання діяльності медійних корпорацій у США. Федеральна комісія з питань комунікацій, Федеральна торгова комісія та Міністерство юстиції здійснюють нагляд за дотриманням вимог щодо конфіденційності, чесної конкуренції та прозорості роботи інтернет-платформ. Ці органи мають право надавати рекомендації та проводити розслідування діяльності соціальних мереж, зокрема у випадках можливих зловживань або порушень прав користувачів.

Отже, комплексний підхід до регулювання соціальних мереж в інтернет-просторі США базується на співпраці різних правових та інституційних механізмів. Верховний суд, правоохоронні органи та законодавчі ініціативи створюють спільну систему контролю, яка прагне забезпечити дотримання прав і свобод користувачів та зменшити ризики, пов'язані з маніпуляціями в

інтернет-просторі. Водночас для збереження ефективного балансу необхідно постійно вдосконалювати правові механізми, адаптуючи їх до швидкого розвитку цифрових технологій та змін у суспільстві. Такий підхід забезпечить стабільний розвиток інтернет-середовища як прозорого, безпечного та правового простору для всіх його учасників.

РОЗДІЛ 3. ПРОТИДІЯ МАНІПУЛЯЦІЙНИМ ВПЛИВАМ В СУЧАСНОМУ ІНТЕРНЕТ-ПРОСТОРИ

3.1 Характеристика методів маніпуляційної діяльності в соціальних мережах.

Явище маніпуляції давно привертає увагу науковців — як теоретиків, так і практиків у різних галузях. Воно й досі викликає їхній інтерес, особливо в умовах інформаційного вибуху, новітніх інформаційних технологій та індустріального розвитку, під час стрімкого технічного і технологічного прогресу, в період переорієнтації людини на ринковий тип взаємодії та трансформації системи цінностей особистості. У світлі цього ми вважаємо за необхідне розглянути маніпуляцію як засіб прихованого контролю та визначити ключові ознаки, за якими її можна відрізнити від інших методів впливу; порівняти підходи різних авторів до розуміння маніпуляції, а також проаналізувати причини формування особистості сучасного маніпулятора і його типові психологічні характеристики [37].

Намагаючись визначити поняття «вплив», дослідники часто звертаються до такої наукової категорії, як «взаємодія», і похідного від неї поняття «взаємовплив».

Психологічний вплив передбачає вплив на свідомість, почуття, дії іншої особи з використанням виключно психологічних засобів (вербальних, паралінгвістичних, невербальних) та надання часу для реагування на цей вплив. Маємо справу з психологічним впливом, коли він має зовнішнє походження по відношенню до реципієнта, і, відбиваючись у ньому, призводить до зміни психологічних регуляторів діяльності людини [38].

Феномен впливу розглядається з онтологічної точки зору і визначається як спосіб суб'єктивно-поведінкової дії на іншу людину, як особлива дія, що породжує подію буття.

Існують численні спроби розробити типологію психологічного впливу, здійснені різними авторами. Одним із критеріїв класифікації методів психологічного впливу є залежність від відкритості для реципієнта засобів впливу та його мети.

За цим критерієм психологічний вплив можна поділити на експліцитний (відкритий) та імпліцитний (прихований або латентний). Психологічний вплив є явним, коли його цілі повідомляються заздалегідь і не приховуються. Імпліцитна або прихована психологічна взаємодія — це вплив, цілі якого не декларуються або маскуються під цілі відкритої взаємодії, тому реципієнт приймає рішення (або виконує дію), заплановане ініціатором впливу [10, с. 29].

Вчені детально проаналізували характеристики маніпуляцій та узагальнили їх в інтегральні критерії, на які можна спиратися при визначенні самого поняття міжособистісної маніпуляції:

1) узагальнюючий показник — психологічний вплив. Цей критерій охоплює такі ознаки, як: «непрямий вплив», «духовний вплив», «програмування думок і намірів», «спрямованість на духовний стан, внутрішній світ»;

2) ставлення до об'єкта маніпуляції як до засобу досягнення власних цілей, при цьому досягаються приховані цілі маніпулятора та реалізуються його інтереси і потреби без урахування інтересів, волі та бажань іншої сторони — людини, яка виступає об'єктом маніпуляції;

3) прагнення отримати односторонній виграш. Цей критерій є досить суперечливим, оскільки маніпулятивний вплив може здійснюватися в інтересах іншої особи. Наприклад, дружина маніпулює, щоб змусити чоловіка припинити вживати алкоголь, що шкодить його здоров'ю. Звичайно, вона переслідує власні інтереси, але в підсумку прагне запобігти деградації його особистості та втраті здоров'я [34, с. 66];

4) прихований характер впливу. Такий критерій також є суперечливим. Спроба маніпуляції має шанси на успіх, якщо факт впливу не усвідомлюється реципієнтом. Людина може інтуїтивно відчувати, що стає жертвою

маніпуляції, але з різних причин не дозволяє сигналам про небезпеку стати усвідомленими;

5) використання психологічної сили, гра на слабкостях. Цей критерій є відносним, оскільки сила є необхідним елементом будь-якого впливу, тому він не є показником, який би дозволяв чітко розмежовувати типи впливу [11, с. 122].

Методи маніпулятивної діяльності в соціальних мережах стають дедалі витонченішими, впливаючи на свідомість користувачів у різних аспектах їхнього життя. Соціальні мережі, як простір, де інформація поширюється швидко та масово, надають маніпуляторам можливість використовувати різні тактики для досягнення власних цілей. Особливість цього явища полягає в тому, що часто люди не усвідомлюють, що ними маніпулюють, і піддаються впливу непрямо. Розглянемо основні аспекти таких методів.

Одним із найпоширеніших методів є емоційна маніпуляція, яка ґрунтується на викликанні у аудиторії певних емоцій для досягнення бажаної поведінки. У цьому контексті маніпулятори активно використовують контент, що провокує страх, гнів або співчуття. Відповідно, користувачі схильні швидше реагувати на емоційні заклики і менш критично осмислювати інформацію, що робить цей метод ефективним у короткостроковій перспективі. Такі маніпуляції часто використовуються в політичних кампаніях або маркетингових стратегіях, коли важливо швидко сформувати ставлення до конкретного продукту чи ідеї [30, с. 56].

Наступний метод, тісно пов'язаний з емоційною маніпуляцією, — це інформаційна насиченість, або «інформаційний шум». Велика кількість інформації, часто суперечливої, заплутує користувачів і ускладнює процес критичного осмислення отриманих даних. У соціальних мережах цей підхід використовують для того, щоб приховати важливу інформацію серед дріб'язкових новин або, навпаки, щоб підвищити видимість неперевіраних чи спотворених фактів. В умовах інформаційного шуму користувачам важко відокремити істину від маніпуляцій, що надає маніпуляторам перевагу.

Фейкові новини, або дезінформація, є ще одним ключовим методом маніпуляції в соціальних мережах. Цей метод полягає в поширенні навмисно неправдивої або спотвореної інформації з метою введення людей в оману. Фейкові новини здатні впливати на громадську думку, провокувати соціальні конфлікти або навіть сприяти маніпуляції виборчим процесом. Завдяки швидкості поширення інформації в мережах фейкові новини можуть за лічені години охопити мільйони користувачів, що робить їх одним із найефективніших інструментів для маніпуляторів [40, с. 109].

Маніпуляція через алгоритми — це ще один інструмент, який набуває дедалі більшого значення. Соціальні мережі використовують алгоритми для персоналізації контенту, який бачить кожен користувач, ґрунтуючись на його вподобаннях і попередній активності. Ці алгоритми можуть бути використані для маніпуляції користувачами, просуваючи певні теми або блокуючи інші. Наприклад, політичні сили можуть використовувати ці алгоритми для того, щоб досягти певної аудиторії та впливати на її переконання через цілеспрямовану рекламу або підбір контенту, що підтримує потрібну точку зору. Таким чином, люди, які не мають доступу до альтернативної інформації, піддаються односторонньому впливу [30, с. 64].

Ще одним поширеним методом є створення «ехо-камер», коли користувачі взаємодіють переважно з тими, хто поділяє їхні погляди. Це досягається за допомогою алгоритмів, що пропонують контент, схожий на той, який користувач уже споживав, що підсилює їхні переконання та закріплює їх у власній інформаційній бульбашці. У таких умовах відбувається ізоляція від альтернативних поглядів, що знижує рівень критичного мислення і сприяє маніпуляціям.

«Тролінг» та «боти» є ще одними важливими елементами маніпулятивної діяльності в соціальних мережах. Тролі — це користувачі, які свідомо провокують інших, викликаючи конфлікти та агресію. Вони використовують емоційні та образливі висловлювання для впливу на обговорення та зміну його напрямку. Часто такі дії є частиною ширшої стратегії

дестабілізації, мета якої полягає у розколі спільнот, руйнуванні конструктивних дискусій або відволіканні уваги від важливих тем. У свою чергу, боти — це автоматизовані програми, що імітують діяльність реальних користувачів. Вони можуть поширювати дезінформацію, створювати враження масової підтримки певної ідеї чи бренду або, навпаки, дискредитувати опонентів через спам-коментарі та підроблені новини [42].

Не можна не згадати методику соціального доказу, яка часто використовується в соціальних мережах. Соціальний доказ — це явище, коли люди схильні вважати правильним те, що підтримує більшість. У контексті соціальних мереж це виражається через кількість лайків, репостів, коментарів і підписників. Маніпулятори можуть використовувати цей механізм для створення штучного враження популярності певної ідеї або особи. Наприклад, за допомогою ботів можна швидко збільшити кількість лайків чи підписників, що створює ілюзію популярності продукту або політичної фігури. Люди, схильні до впливу соціального доказу, часто починають підтримувати такі ініціативи, не замислюючись над їхньою справжністю.

Окрім цього, часто застосовують техніку «наклепу» та «чорного піару». У соціальних мережах легше, ніж будь-де інде, поширювати негативні чутки, брехливу інформацію або компрометуючі матеріали про конкурентів чи опонентів. Це робиться для того, щоб послабити їхню репутацію в очах громадськості або викликати недовіру до них. Цей метод може бути особливо ефективним у політичній боротьбі, коли результат залежить від того, як швидко та масштабно можна поширити дискредитуючу інформацію [43].

Соціальні мережі також є ідеальним середовищем для поширення прихованої реклами або пропаганди. Часто така реклама маскується під звичайний контент або новини, що ускладнює її виявлення користувачами. Наприклад, це можуть бути спонсоровані пости блогерів, які нібито безкорисливо рекомендують певні товари або послуги, чи політичні заяви, що видаються за особисті думки впливових осіб. Такі маніпуляції формують у

користувачів хибні уявлення про реальні мотиви та приховані інтереси за опублікованим контентом.

Інструменти соціальних мереж, такі як масова сегментація аудиторії, надають маніпуляторам нові, значно потужніші можливості для впливу на свідомість користувачів. Масова сегментація базується на використанні величезних обсягів даних, які соціальні мережі збирають про своїх користувачів: їхні вподобання, поведінку в мережі, географічне розташування, інтереси, вік, стать і навіть емоційний стан. Ці дані дозволяють маніпуляторам створювати надзвичайно точні та персоналізовані стратегії впливу, адаптовані під конкретні групи людей [45, с. 66].

Одним з головних інструментів сегментації є таргетинг, який дозволяє налаштовувати рекламні або інформаційні кампанії так, щоб вони досягали максимальної кількості потенційно зацікавлених осіб. Наприклад, політичні сили можуть використовувати таргетинг для поширення своїх ідей серед певних демографічних груп, які схильні підтримувати їхні погляди. Це дозволяє значно зменшити витрати на рекламу, оскільки кожне повідомлення націлене на конкретну аудиторію, що є більш ефективним, ніж масова неперсоналізована реклама. У цьому процесі ключову роль відіграють алгоритми, що аналізують поведінку користувачів і обирають категорії, які найбільше схильні до впливу.

Однак, ця персоналізація має і свою темну сторону. Використання детальних даних про користувачів дозволяє маніпуляторам націлюватися на найбільш уразливі групи населення, які можуть мати обмежену здатність до критичного осмислення отриманих даних або бути схильними до впливу певних емоційних чи соціальних тригерів. Наприклад, люди, що перебувають у стані емоційного стресу або соціальної ізоляції, можуть бути більш схильними до впливу через повідомлення, які апелюють до їхніх страхів, занепокоєння або почуття несправедливості. Таким чином, маніпулятори можуть створювати цілеспрямовані інформаційні атаки на вразливі категорії

людей, використовуючи таргетинг для посилення їхніх емоційних реакцій та маніпулювання їхньою поведінкою.

Важливо зазначити, що маніпуляційний вплив через соціальні мережі часто залишається непоміченим користувачами. Один із найпотужніших аспектів такої маніпуляції полягає в тому, що люди рідко усвідомлюють, наскільки глибоко їхня поведінка і світогляд можуть змінюватися під впливом контенту, який вони споживають у соціальних мережах. Це створює ілюзію самостійності у виборі інформації та формуванні думок, хоча насправді ними керують приховані алгоритми та добре сплановані маніпуляції.

Ще однією важливою технікою маніпуляції є використання психологічного профілювання. Психологічне профілювання користувачів соціальних мереж дозволяє маніпуляторам і рекламодавцям розуміти психологічні особливості, емоційний стан і потреби кожного окремого користувача. Зокрема, аналітика поведінки в інтернеті дає можливість визначити рівень стресу, соціальні зв'язки, інтереси та вподобання користувачів. Це дозволяє маніпуляторам використовувати не лише емоційні чи раціональні аргументи, але й глибші психологічні тригери, які впливають на поведінку людей на підсвідомому рівні [53, с. 12].

Окрім таргетингу, важливим елементом сегментації є створення «інформаційних бульбашок». Це явище, за якого користувачі взаємодіють з інформацією, що відповідає їхнім власним уподобанням та переконанням, при цьому відсікаючи альтернативні погляди. Алгоритми соціальних мереж сприяють цьому процесу, оскільки вони підбирають контент на основі того, що користувачі вже вподобали або поділилися раніше. Таким чином, людина потрапляє у замкнене коло, де вона постійно отримує підтвердження своїх власних переконань, не стикаючись із альтернативними точками зору. Це веде до поляризації суспільства та посилення розбіжностей між різними соціальними групами, оскільки кожна з них ізолюється у власній інформаційній бульбашці.

Ця ізоляція також створює сприятливі умови для поширення фейкових новин і дезінформації, оскільки користувачі менш схильні перевіряти достовірність інформації, яка відповідає їхнім уподобанням. У таких умовах фейкові новини можуть швидко поширюватися в межах інформаційних бульбашок, де вони не зустрічають опору у вигляді критичного мислення чи альтернативних джерел інформації. Це посилює маніпулятивний вплив, оскільки користувачі починають вірити в неправдиву інформацію і, як наслідок, приймати рішення на основі дезінформації.

Іншим важливим аспектом маніпуляційної діяльності в соціальних мережах є використання впливу лідерів думок або інфлюенсерів. Інфлюенсери мають велику аудиторію, яка довіряє їхнім рекомендаціям та думкам. Це робить їх ідеальними каналами для маніпуляції, особливо коли інфлюенсери просувають певні продукти, політичні погляди або соціальні рухи, приховуючи при цьому свої справжні мотиви або фінансові вигоди. Маніпулятори можуть використовувати інфлюенсерів для непрямого впливу на їхню аудиторію, створюючи ілюзію автентичності та щирості [54].

Крім того, інфлюенсери можуть використовувати свою популярність для нормалізації певних ідей чи поведінки, що сприяє їх поширенню в суспільстві. Наприклад, якщо популярний інфлюенсер підтримує певну політичну ідею або соціальну ініціативу, це може створити враження, що ця ідея є загальноприйнятою або морально правильною, навіть якщо вона може бути спірною чи маніпулятивною. У свою чергу, аудиторія інфлюенсера, яка вже має до нього високий рівень довіри, рідко піддає сумніву його рекомендації чи думки, що робить цей метод особливо ефективним для маніпуляції.

Маніпуляції в соціальних мережах також часто використовують техніки соціального доказу. Це поняття базується на тому, що люди схильні вважати правильним те, що підтримує більшість. У соціальних мережах це виражається через кількість лайків, репостів, коментарів або підписників. Маніпулятори можуть використовувати соціальний доказ для створення ілюзії популярності

певної ідеї або продукту, навіть якщо насправді підтримка може бути штучно створеною. Використання ботів, які автоматично додають лайки та коментарі, або купівля фейкових підписників дозволяє маніпуляторам створювати видимість масової підтримки і тим самим впливати на сприйняття користувачів.

Ще одним цікавим методом маніпуляції є використання техніки «темного патерну» (dark pattern), коли інтерфейси соціальних мереж спеціально розробляються так, щоб користувачі підсвідомо виконували дії, які не планували. Це може бути непомітна активація підписки на платні сервіси, випадкові лайки певного контенту або навіть участь у голосуваннях, де результати легко маніпулюються.

Найуразливіші групи населення щодо маніпуляцій у соціальних мережах відрізняються за віком, рівнем освіти, психологічними особливостями, соціальним статусом та іншими чинниками. Вони більш схильні до впливу через певні фактори, які роблять їх менш здатними до критичного мислення або більш емоційно залежними від інформації, що поширюється в цифровому просторі. Маніпуляції через соціальні мережі можуть бути спрямовані на різні групи, але існують особливі категорії населення, які є найбільш вразливими через свою специфіку. Далі розглянемо ключові групи, що мають високий рівень сприйнятливості до маніпуляцій [54].

Однією з найуразливіших груп є молодь та підлітки. Ця категорія населення зазвичай активно використовує соціальні мережі для спілкування, самовираження та отримання інформації про світ. Водночас молодь ще не має достатнього життєвого досвіду, щоб адекватно оцінювати інформацію та виявляти маніпуляції. Підлітки часто перебувають у пошуках своєї ідентичності та соціальної приналежності, що робить їх легкою мішенню для маніпуляторів, які можуть пропонувати їм вигадані ідеали чи моделі поведінки. Вплив через соціальні мережі часто побудований на емоційних повідомленнях, що викликають сильні почуття або бажання бути частиною

певної групи чи руху. Молоді люди, схильні до наслідування модних тенденцій та популярних інфлюенсерів, можуть бути введені в оману або навіть долучитися до небезпечних для їхнього життя чи психіки рухів. Крім того, молодь часто недостатньо обізнана про правила безпеки в інтернеті, що підвищує ризик бути втягнутою в маніпулятивні ігри.

Люди похилого віку також є однією з найбільш вразливих груп до маніпуляцій у соціальних мережах. Вони меншою мірою володіють цифровою грамотністю і, як правило, мають обмежений досвід використання сучасних технологій. Це ускладнює їм можливість відрізнити правдиву інформацію від фейкових новин або дезінформації. До того ж старші люди часто прагнуть знайти підтримку в інтернеті, оскільки можуть відчувати соціальну ізоляцію або самотність. Це робить їх більш уразливими до маніпуляцій через групи в соціальних мережах, де можуть активно поширюватися різні ідеології чи псевдонаукові теорії. Зважаючи на те, що люди похилого віку часто довіряють авторитетам, їм важко піддавати сумніву інформацію, що походить від джерел, які видаються їм надійними. У зв'язку з цим маніпулятори можуть використовувати фейкові новини, побудовані на страхах або упередженнях старшого покоління, щоб впливати на їхню поведінку чи політичні переконання [45, с. 88].

Люди з низьким рівнем освіти або ті, хто має обмежений доступ до надійної інформації, також входять до числа найуразливіших до маніпуляцій у соціальних мережах. Освіта відіграє ключову роль у формуванні критичного мислення та здатності оцінювати інформацію з різних джерел. Особи, які мають низький рівень освіти, можуть бути менш здатними до аналізу отриманих даних і частіше приймають на віру те, що їм пропонують через соціальні мережі. Відсутність доступу до якісної освіти та обмежені можливості для підвищення свого рівня обізнаності у складних питаннях роблять таких людей легкою мішенню для дезінформаційних кампаній. Це може бути використано маніпуляторами як у комерційних, так і в політичних цілях. Наприклад, люди з низьким рівнем освіти можуть стати жертвами

фальшивих рекламних кампаній або підтримувати політиків, чиї обіцянки є нереалістичними, але добре поданими.

Іншою вразливою групою є люди, які переживають емоційний або психологічний стрес. У складних життєвих ситуаціях люди стають менш стійкими до маніпуляцій, оскільки їхнє сприйняття інформації піддається впливу емоцій. Соціальні мережі можуть пропонувати емоційні рішення, що на перший погляд здаються простими та логічними, але насправді можуть бути маніпулятивними. Наприклад, у моменти соціальних або економічних криз люди шукають підтримки та стабільності, що робить їх більш відкритими до прийняття радикальних або популістських ідей, які можуть надходити через соціальні мережі. Маніпулятори використовують цю емоційну вразливість для просування своїх інтересів, намагаючись викликати у людей почуття страху, ненависті або відчаю, що сприяє їхній подальшій маніпуляції [52, с. 501].

Також серед найуразливіших груп до маніпуляцій слід виділити людей, які перебувають у складній економічній ситуації. Соціальні мережі, надаючи доступ до різних форм контенту, часто стають платформою для поширення маніпулятивних повідомлень, що обіцяють швидкі рішення економічних проблем або вигідні пропозиції. Люди, які стикаються з фінансовими труднощами, можуть стати жертвами шахрайства або фінансових пірамід, що пропагуються через соціальні мережі. Крім того, економічні труднощі можуть підвищувати їхню чутливість до політичної пропаганди, яка обіцяє швидкі зміни та покращення. У цьому контексті маніпулятори можуть використовувати економічні страхи та невпевненість людей, щоб спрямовувати їхню увагу на певні політичні або соціальні рішення [54].

Крім того, уразливими є люди, які відчувають соціальну або культурну ізоляцію. Це можуть бути представники національних меншин, мігранти або особи, що живуть у віддалених регіонах. Такі люди часто мають обмежений доступ до широкого кола джерел інформації і можуть покладатися на соціальні мережі як на основне джерело новин і соціальних контактів. Маніпулятори можуть використовувати їхнє почуття ізоляції для поширення неправдивої

інформації або для просування ідей, які можуть сприяти їхній подальшій ізоляції від суспільства. Наприклад, мігранти можуть стати жертвами дезінформації, що закликає їх уникати певних соціальних інститутів або підтримувати радикальні рухи.

Не можна також не згадати про людей, які мають обмежені соціальні зв'язки або ті, хто перебуває в умовах соціальної ізоляції. Ці люди можуть бути більш схильними до споживання інформації з соціальних мереж, оскільки вони шукають взаємодії з іншими людьми. Соціальні мережі можуть стати для них єдиним джерелом спілкування та інформації, що робить їх особливо вразливими до маніпуляцій. Відчуття самотності та соціальної ізоляції може підштовхнути таких людей до пошуку належності в групах або рухах, які можуть бути маніпулятивними або деструктивними.

Ще однією вразливою групою є люди з обмеженими можливостями, які можуть мати труднощі з доступом до традиційних джерел інформації та бути залежними від соціальних мереж для отримання новин і соціальної взаємодії. Через специфіку їхніх обмежень такі люди можуть стати об'єктами маніпуляцій з боку шахраїв або дезінформаторів, які використовують їхню залежність від онлайн-середовища. Наприклад, люди з фізичними або психічними вадами можуть бути залучені до різних шахрайських схем або неправдивих пропозицій.

Методи маніпуляційної діяльності в соціальних мережах у Сполучених Штатах мають свої унікальні особливості, зумовлені як культурними, так і політичними та технологічними чинниками. У порівнянні з іншими країнами, американський підхід до використання соціальних медіа для маніпуляцій має певні відмінності, проте багато загальних рис залишаються спільними для глобального простору соціальних мереж. Соціальні мережі, такі як Facebook, Twitter, Instagram і TikTok, є не лише платформами для особистого спілкування, але й важливими інструментами для впливу на масову свідомість. У США цей процес став особливо помітним у контексті політичних кампаній, виборів та соціальних рухів; однак методи маніпуляцій використовуються й в

інших сферах, таких як маркетинг та пропаганда. Розглянемо специфіку маніпуляційної діяльності в США в порівнянні з іншими країнами.

Однією з ключових особливостей маніпуляцій у соціальних мережах у США є високий рівень політизації контенту. Політична боротьба в країні постійно перебуває в центрі уваги, і це значною мірою відображається на способах впливу на аудиторію через соціальні мережі. Політичні партії, кандидати та різні громадські організації активно використовують соціальні мережі як платформу для поширення своїх меседжів і впливу на електорат. При цьому вони не завжди використовують легальні або етичні методи. Наприклад, під час президентських виборів 2016 року стало відомо про використання соціальних медіа для поширення фейкових новин та дезінформації, що сприяло маніпуляції виборчими процесами. Залучення іноземних акторів, таких як російські тролі або боти, для впливу на громадську думку в США також стало однією з найпомітніших рис американської політичної реальності.

Ще однією важливою особливістю є використання мікротаргетингу в політичних кампаніях. Соціальні мережі дозволяють політичним силам у США сегментувати аудиторію на основі величезної кількості критеріїв, таких як вік, стать, інтереси, географічне розташування, поведінка в мережі та навіть політичні вподобання. Ця сегментація дає можливість політикам створювати максимально персоналізовані рекламні кампанії, які апелюють до емоцій, страхів або надій певних груп виборців. Наприклад, кампанія Дональда Трампа у 2016 році активно використовувала цей метод для впливу на різні сегменти населення, зокрема на групи, які відчували економічну невпевненість або соціальну ізоляцію. У порівнянні з іншими країнами, мікротаргетинг у США набув величезних масштабів завдяки високому рівню збору даних про користувачів соціальних мереж і використанню цих даних для маніпуляції виборцями.

Окрім політичних кампаній, маніпуляції в соціальних мережах у США також активно використовуються в маркетингу. Американські корпорації

активно застосовують соціальні мережі для створення ілюзії популярності продуктів, маніпулюючи думками споживачів. Використання інфлюенсерів, блогерів та інших лідерів думок для просування товарів або послуг стало звичайною практикою. Однак це також створює ризик маніпуляцій, оскільки багато таких рекламних кампаній приховують свої комерційні мотиви, видаючи рекламу за особисту думку або рекомендацію. У деяких випадках корпорації використовують боти або фейкові акаунти для збільшення видимості своїх продуктів, що робить споживачів більш схильними до покупки через так званий «соціальний доказ». У порівнянні з іншими країнами, у США маркетингова маніпуляція через соціальні мережі є однією з найбільш розвинених завдяки величезному ринку споживачів і високому рівню цифрової грамотності компаній.

Також варто зазначити важливість культурного контексту в США. Американське суспільство є дуже різномірним, що робить його більш уразливим до маніпуляцій через соціальні мережі. Під час соціальних рухів, таких як Black Lives Matter або рухи за права ЛГБТ+, соціальні мережі стали ключовим полем битви за увагу суспільства. Маніпулятори, як правило, використовують поляризаційні теми для того, щоб ще більше розділити суспільство та викликати конфлікти. У цьому контексті особливо поширеними є тактики поширення фейкових новин та емоційної дезінформації, що апелює до страхів або ненависті певних груп населення. Такі методи маніпуляцій менш поширені в країнах з меншим рівнем соціальної поляризації; проте вони також застосовуються в умовах культурних або політичних конфліктів.

Іншою важливою рисою американської маніпуляційної діяльності є участь великих технологічних компаній у процесі контролю та впливу на інформаційні потоки. Facebook, Google, Twitter та інші компанії відіграють ключову роль у поширенні інформації в США і мають значний контроль над тим, що бачать користувачі на своїх платформах. У той час як ці компанії заявляють про боротьбу з фейковими новинами та дезінформацією, їхні алгоритми часто сприяють поширенню емоційно насиченого контенту, який

привертає більше уваги користувачів, незалежно від його правдивості. Така ситуація відрізняється від деяких інших країн, де соціальні мережі контролюються більш суворо з боку держави, наприклад, у Китаї або Росії. У США маніпуляції часто залишаються в руках приватних компаній, які керуються власними комерційними інтересами.

У порівнянні з іншими країнами, у США існує значна свобода слова, що робить контроль над маніпуляціями складнішим завданням. У країнах з авторитарними режимами, таких як Китай, Іран або Північна Корея, уряди контролюють соціальні мережі та використовують їх для просування державної пропаганди. В таких умовах маніпуляції з боку держави стають основною загрозою для інформаційної безпеки громадян. Натомість у США основну роль у маніпуляціях грають приватні компанії, політичні групи та іноземні актори. Це робить американську систему більш відкритою для зовнішніх маніпуляцій, оскільки контроль за інформаційним простором є менш централізованим.

З іншого боку, Сполучені Штати також стали епіцентром боротьби з маніпуляціями в соціальних мережах. Після виборів 2016 року американський уряд і великі технологічні компанії почали активніше вживати заходів для боротьби з поширенням дезінформації та маніпуляцій через соціальні мережі. Були створені спеціальні алгоритми для виявлення фейкових акаунтів, ботоферм та дезінформаційних кампаній. У порівнянні з іншими країнами, США інвестують більше ресурсів у розробку технологій для протидії маніпуляціям, хоча результати цих зусиль не завжди є задовільними.

Таким чином, маніпуляції в соціальних мережах у США є багатограним явищем, яке має свої унікальні риси, зумовлені культурними, політичними та технологічними чинниками. Порівняно з іншими країнами, США вирізняються високим рівнем політизації контенту, використанням мікротаргетингу, активним залученням технологічних компаній до контролю інформаційних потоків і великою свободою слова. Це створює як можливості для маніпуляцій, так і виклики для їхнього контролю.

3.2. Роль регуляторів та провідних компаній у запобіганні маніпуляціям

Запобігання маніпуляціям у світі, включаючи США, стало однією з найважливіших тем у сфері інформаційної безпеки та регулювання інтернету. Зі зростанням впливу соціальних мереж, таких як Facebook, Twitter, Instagram і TikTok, світ зіткнувся з новими викликами у боротьбі з дезінформацією, пропагандою та іншими формами маніпуляцій. Важливим аспектом є той факт, що маніпуляції можуть суттєво впливати на громадську думку, політичні вибори, економічну поведінку людей та їх соціальні стосунки. У зв'язку з цим країни по всьому світу, включаючи США, розробляють та впроваджують загальні правила, спрямовані на боротьбу з маніпуляціями у цифровому середовищі.

Одним з основних інструментів запобігання маніпуляціям є впровадження законодавчих актів і регулюючих механізмів на державному рівні. У багатьох країнах приймаються закони, що передбачають відповідальність за поширення неправдивої інформації та дезінформації. У Європейському Союзі, наприклад, діє Загальний регламент захисту даних (GDPR), що регулює збір та використання персональних даних громадян. Це має важливе значення для запобігання маніпуляціям, оскільки зловживання персональними даними може використовуватися для цілеспрямованих атак на користувачів, включаючи політичні кампанії, що апелюють до їхніх страхів або упереджень. Такі регулювання покликані забезпечити більшу прозорість у тому, як компанії збирають та використовують інформацію про користувачів, що є важливим кроком для зменшення ризику маніпуляцій [12, с. 41].

США, у свою чергу, також активно працюють над розробкою законодавства для боротьби з маніпуляціями в соціальних мережах. Одним із основних напрямків є посилення контролю за політичною рекламою, особливо після скандалу з втручанням Росії у вибори 2016 року. Одним з ключових

аспектів американської системи боротьби з маніпуляціями є вимоги щодо прозорості рекламних кампаній у соціальних мережах. Компанії, такі як Facebook і Google, зобов'язані розкривати інформацію про те, хто фінансує політичні оголошення, а також на яку аудиторію вони спрямовані. Це дозволяє користувачам краще розуміти, хто намагається вплинути на їхню думку і чому. Крім того, американські регулятори активно досліджують роль алгоритмів у поширенні маніпулятивного контенту та розглядають можливість більш суворого контролю над їхньою роботою.

Іншим важливим аспектом запобігання маніпуляціям є співпраця між державами та технологічними компаніями. Багато країн розуміють, що жодна держава не може самотійно впоратися з глобальними викликами маніпуляцій у соціальних мережах, тому міжнародна співпраця є необхідною. Наприклад, країни Європейського Союзу активно співпрацюють з технологічними гігантами для розробки інструментів, які дозволяють боротися з поширенням фейкових новин і дезінформації на платформах соціальних мереж. Ця співпраця включає в себе обмін інформацією між державами та компаніями щодо можливих загроз, таких як втручання іноземних акторів у виборчі процеси або поширення небезпечної пропаганди [13, с. 91].

Важливим елементом співпраці є також розробка спільних стандартів щодо роботи соціальних мереж з точки зору регулювання контенту. Держави та технологічні компанії працюють над створенням механізмів модерації контенту, які дозволяють швидко виявляти та видаляти маніпулятивний або шкідливий контент. Це включає в себе створення автоматизованих систем, які використовують штучний інтелект для виявлення фейкових акаунтів, ботів або поширення фальшивих новин. Наприклад, компанії, такі як Facebook і Twitter, активно розробляють такі алгоритми для виявлення маніпуляцій у реальному часі. Крім того, компанії співпрацюють з незалежними організаціями, що займаються фактчекінгом, для перевірки правдивості інформації, що поширюється на платформах [44, с. 191].

США стали епіцентром боротьби з маніпуляціями після того, як виборчий процес 2016 року продемонстрував масштабну проблему втручання в політику через соціальні медіа. Окрім розслідувань, що проводяться Конгресом та спеціальними комісіями, основну увагу було звернено на впровадження технологічних рішень для запобігання повторенню подібних інцидентів. Технологічні гіганти, такі як Facebook, Twitter та Google, почали впроваджувати нові правила та інструменти, спрямовані на запобігання зовнішнім впливам на вибори, а також на боротьбу з поширенням неправдивої інформації в соціальних мережах. У рамках цих ініціатив було розроблено спеціальні системи для виявлення та блокування акаунтів, які ведуть себе підозріло або поширюють дезінформацію. Крім того, було впроваджено спеціальні механізми для моніторингу політичної реклами та розширено прозорість щодо того, хто фінансує такі рекламні кампанії [56, с. 430].

Не менш важливим є розвиток освіти та підвищення рівня цифрової грамотності серед населення. Держави та компанії по всьому світу розуміють, що запобігання маніпуляціям можливе лише тоді, коли користувачі здатні критично оцінювати інформацію, яку отримують через соціальні мережі. Це включає навчальні програми, спрямовані на підвищення обізнаності про ризики фейкових новин, методи перевірки джерел інформації та розуміння того, як працюють алгоритми, які визначають, що саме користувачі бачать у своїх стрічках новин. У США та в багатьох інших країнах вже впроваджуються подібні освітні програми, особливо серед молоді, яка є найбільш активною аудиторією соціальних мереж [60].

Крім того, великі компанії зосереджуються на тому, щоб надати користувачам більше інструментів для захисту від маніпуляцій. Наприклад, Facebook впровадив функцію, яка дозволяє користувачам бачити, які саме джерела інформації використовуються в новинах, а також хто фінансує ту чи іншу рекламу. Google створив спеціальну панель інструментів, яка дозволяє користувачам перевіряти факти й швидко знаходити достовірні джерела

інформації. Це допомагає користувачам приймати більш обґрунтовані рішення про те, чи варто довіряти тій чи іншій новині.

Проте, попри всі зусилля, боротьба з маніпуляціями у світі та США залишається надзвичайно складним завданням. Однією з головних проблем є швидкість поширення інформації в соціальних мережах. Маніпулятивні кампанії можуть за лічені години охопити мільйони користувачів, і навіть найкращі технології виявлення та блокування не завжди здатні реагувати на такі загрози вчасно. Крім того, постійний розвиток технологій надає маніпуляторам можливість створювати нові методи впливу, такі як дипфейки або використання штучного інтелекту для генерації фальшивих новин [65].

Роль регуляторів та провідних технологічних компаній у запобіганні маніпуляціям у соціальних мережах стає дедалі більш важливою в сучасному інформаційному світі. Соціальні медіа стали невід'ємною частиною повсякденного життя мільйонів людей, але водночас вони відкрили нові можливості для маніпуляцій громадською думкою. Ці маніпуляції можуть мати різні форми, включаючи поширення фейкових новин, дезінформації, пропаганди, а також спроби впливати на політичні вибори, економічну поведінку та соціальні конфлікти. У цьому контексті роль державних регуляторів та провідних компаній, таких як Facebook, Google, Twitter та Instagram, є вирішальною для забезпечення інформаційної безпеки та захисту користувачів від маніпуляцій.

По-перше, слід зазначити, що державні регулятори мають відповідальність за створення правової бази для контролю за діяльністю соціальних мереж та боротьби з дезінформацією. Однією з основних функцій регуляторів є встановлення правил відповідальності за поширення неправдивої інформації та запровадження заходів для її виявлення і запобігання. У багатьох країнах світу вже ухвалені закони, спрямовані на боротьбу з маніпуляціями у соціальних медіа. Наприклад, у Європейському Союзі діє Загальний регламент захисту даних (GDPR), який не лише регулює питання конфіденційності, але й забезпечує контроль над збором і

використанням даних користувачів для маніпуляцій. Крім того, у деяких країнах були ухвалені закони про боротьбу з фейковими новинами, які передбачають штрафи або інші санкції за поширення неправдивої інформації, особливо під час виборів або інших політичних подій [68].

Важливою складовою регулювання є також контроль за алгоритмами, що використовуються соціальними мережами для поширення контенту. Регулятори повинні впливати на компанії, щоб забезпечити прозорість в роботі алгоритмів, які визначають, який контент бачать користувачі. Алгоритми часто сприяють поширенню маніпулятивного або емоційного контенту, оскільки він привертає більше уваги та генерує більше взаємодій. Однак ці алгоритми рідко враховують достовірність інформації. У відповідь на це регулятори мають розробляти вимоги до алгоритмів, щоб вони не лише сприяли збільшенню взаємодії користувачів, але й відсіювали фейкові новини та маніпулятивний контент. Наприклад, у Німеччині було запроваджено закон про боротьбу з ненависницькими висловлюваннями та фейковими новинами, згідно з яким компанії можуть бути оштрафовані, якщо не видаляють такий контент протягом 24 годин після повідомлення [79].

Регулятори також відіграють ключову роль у створенні механізмів співпраці з технологічними компаніями для боротьби з маніпуляціями. Важливим елементом є міжнародна співпраця, оскільки багато з найбільших соціальних мереж діють на глобальному рівні. Регулюючі органи різних країн можуть співпрацювати, обмінюватися інформацією та координувати зусилля з метою протидії міжнародним кампаніям дезінформації та маніпуляцій. Прикладом такої співпраці може бути об'єднання зусиль країн ЄС для боротьби з впливом іноземних акторів на вибори у різних країнах Союзу. Ця співпраця є важливою, оскільки дезінформація та маніпуляції часто поширюються через міжнародні мережі тролів, ботоферм та інших засобів впливу, які не завжди можна контролювати на рівні однієї держави.

Провідні технологічні компанії також мають значну роль у запобіганні маніпуляціям у соціальних мережах. Як власники платформ, на яких

відбувається більшість інформаційного обміну, вони мають можливість і ресурси для боротьби з дезінформацією та захисту своїх користувачів. Однак їхня відповідальність не завжди була чітко визначена. Протягом багатьох років компанії, такі як Facebook та Twitter, стикалися з критикою через те, що не приділяли достатньо уваги проблемі поширення фейкових новин та маніпуляцій. Тиск з боку урядів і громадськості змусив ці компанії вжити заходів для боротьби з цією проблемою [61, с. 179].

Одним з основних напрямків роботи технологічних компаній у запобіганні маніпуляціям стало створення інструментів для виявлення та блокування фейкових акаунтів і ботів. Автоматизовані акаунти, або боти, є одним з основних засобів поширення маніпулятивного контенту, оскільки вони можуть швидко та масово розповсюджувати інформацію, створюючи ілюзію широкої підтримки певних ідей чи подій. Компанії, такі як Facebook і Twitter, розробляють алгоритми, які дозволяють виявляти ботів і блокувати їх, перш ніж вони зможуть вплинути на користувачів. Наприклад, після скандалу з російським втручанням у вибори 2016 року Twitter активно почав видаляти акаунти, пов'язані з дезінформаційними кампаніями, що фінансуються з-за кордону [77, с. 53].

Іншим важливим заходом стало впровадження технологій фактчекінгу. Багато технологічних компаній почали співпрацювати з незалежними організаціями, що займаються перевіркою фактів, для виявлення та маркування фейкових новин. Ці організації аналізують контент, що поширюється в соціальних мережах, і позначають інформацію, яка є неправдивою або вводить в оману. Наприклад, Facebook запустив ініціативу «News Integrity Initiative», яка співпрацює з фактчекерами та медіаорганізаціями, щоб забезпечити перевірку та маркування фейкових новин. Це дає можливість користувачам отримувати попередження про можливу недостовірність інформації, яку вони бачать у своїй стрічці новин.

Важливою частиною боротьби з маніпуляціями є також покращення прозорості реклами в соціальних мережах. Під час політичних кампаній

маніпулятори часто використовують таргетовану рекламу для поширення дезінформації або впливу на електорат. Технологічні компанії, такі як Google і Facebook, почали впроваджувати нові правила щодо політичної реклами, які вимагають від рекламодавців вказувати, хто фінансує рекламу та для кого вона призначена. Це дає користувачам можливість бачити, звідки походить інформація і якими групами вона підтримується. Наприклад, Facebook створив бібліотеку політичної реклами, де користувачі можуть переглянути всі політичні оголошення, які були розміщені на платформі, а також інформацію про те, хто їх замовив і яку аудиторію вони таргетували.

Попри всі ці заходи, технологічні компанії продовжують стикатися з проблемами у боротьбі з маніпуляціями. Однією з головних труднощів є масштабність проблеми. Соціальні мережі використовуються мільярдами людей по всьому світу, і кількість контенту, який створюється щодня, є величезною. Це ускладнює виявлення та блокування фейкових новин і маніпуляцій у реальному часі. Крім того, маніпулятори постійно вдосконалюють свої методи, знаходячи нові способи обійти системи безпеки та алгоритми, що виявляють дезінформацію.

Регулятори та провідні технологічні компанії стикаються з численними проблемами у запобіганні маніпуляціям у соціальних мережах. Ця проблема є складною та багатогранною, оскільки маніпуляції можуть мати різні форми: від поширення фейкових новин до таргетованих кампаній, спрямованих на вплив на політичні вибори або соціальні рухи. Технології, що розвиваються, зокрема штучний інтелект та автоматизація, надають нові можливості для маніпуляторів, і це ускладнює завдання регуляторів та компаній. Важливо також враховувати, що питання маніпуляцій тісно пов'язане з питаннями свободи слова, приватності та конфіденційності даних, що робить його ще більш складним для вирішення.

Однією з ключових проблем для регуляторів є створення ефективних законодавчих механізмів, які могли б не тільки запобігати маніпуляціям, але й відповідати принципам демократичного суспільства. У багатьох країнах

свобода слова є основоположним правом, і регулятори мають обмежені можливості для втручання в контент, який поширюється в соціальних мережах. Будь-які спроби жорсткішого регулювання можуть викликати обурення з боку громадськості, що вбачатиме у цих заходах спробу цензури. Це особливо складне питання в демократичних країнах, таких як США, де Конституція гарантує свободу вираження думок. Через це регулятори часто стикаються з дилемою: як контролювати поширення маніпулятивного контенту, не обмежуючи при цьому права на свободу слова.

Ще одна проблема полягає в тому, що маніпуляції в соціальних мережах часто мають міжнародний характер. Багато з найбільш масштабних маніпулятивних кампаній організовані іноземними акторами, які використовують соціальні медіа для втручання у внутрішні справи інших держав. Відомим прикладом є втручання Росії у президентські вибори в США 2016 року через поширення дезінформації в соціальних мережах. Регуляторам важко протистояти таким загрозам, оскільки вони виходять за межі їхньої юрисдикції. Це вимагає міжнародної співпраці та координації зусиль, що, у свою чергу, ускладнюється різними законодавчими та культурними особливостями країн. Не всі держави готові співпрацювати з іншими у питаннях інформаційної безпеки, а деякі, навпаки, використовують маніпуляції як інструмент зовнішньої політики.

Ще одна серйозна проблема полягає у складності виявлення та ідентифікації маніпулятивного контенту. Соціальні мережі містять величезну кількість інформації, і навіть найсучасніші алгоритми та інструменти штучного інтелекту не можуть виявляти та блокувати маніпуляції на 100%. Часто маніпулятивний контент виглядає цілком правдоподібно і важко відрізнити від достовірних новин. Маніпулятори використовують витончені методи для поширення фейкових новин, зокрема замасковану рекламу, напівправду або маніпулятивні заголовки, що апелюють до емоцій користувачів. Алгоритми, які використовуються для моніторингу контенту,

ще не досконалі й часто пропускають маніпулятивні публікації або, навпаки, помилково блокують справжній контент.

Технологічні компанії, такі як Facebook, Twitter і Google, також стикаються з серйозними проблемами в боротьбі з маніпуляціями. Одна з головних проблем полягає в конфлікті між їхніми комерційними інтересами та суспільною відповідальністю. Мета цих компаній полягає в тому, щоб утримати користувачів на своїх платформах якомога довше, адже це сприяє зростанню їхнього прибутку. Однак алгоритми, які використовуються для цього, часто сприяють поширенню саме маніпулятивного або емоційного контенту, оскільки він привертає більше уваги користувачів. Це призводить до того, що фейкові новини або дезінформація поширюються швидше і ширше, ніж достовірний контент. Компанії намагаються знайти баланс між прибутком і безпекою, але цей процес є дуже складним і вимагає великих інвестицій у технології виявлення маніпуляцій.

Ще однією значною проблемою є роль автоматизації та ботів у поширенні маніпулятивного контенту. Боти – це автоматизовані акаунти, які можуть публікувати повідомлення, лайкати, коментувати та взаємодіяти з іншими користувачами. Вони активно використовуються для поширення дезінформації та створення ілюзії масової підтримки певних ідей або кампаній. Технологічні компанії намагаються розробити інструменти для виявлення та блокування ботів, але їх кількість і різноманітність постійно зростають. Маніпулятори використовують усе більш витончені технології для створення ботів, які виглядають і діють як справжні користувачі, що ускладнює їх виявлення.

Проблема таргетованої реклами також є важливою складовою у контексті маніпуляцій. Таргетована реклама дозволяє рекламодавцям налаштовувати кампанії на конкретні групи користувачів на основі їхніх вподобань, поведінки та особистої інформації. Це може бути використано як для добрих цілей, так і для маніпуляцій. Наприклад, маніпулятори можуть використовувати цю технологію для поширення фейкових новин або

дезінформації серед певних демографічних груп, що підсилює політичні розбіжності та соціальну напругу. Регулятори та технологічні компанії стикаються з викликами, пов'язаними із захистом приватності даних користувачів, що ускладнює контроль за цими практиками.

У результаті всіх цих проблем та викликів боротьба з маніпуляціями у соціальних мережах є складною та багатогранною задачею. Вона вимагає зусиль з боку всіх учасників процесу: технологічних компаній, регуляторів, громадянського суспільства та самих користувачів. Потрібно створювати інструменти для перевірки інформації, покращувати медіаосвіту та свідомість користувачів, а також активно працювати над законодавчими змінами, які могли б забезпечити безпечне та прозоре інформаційне середовище. Лише у такій співпраці можна досягти значного прогресу у боротьбі з маніпуляціями та дезінформацією в соціальних мережах.

3.3. Вплив правового регулювання на діяльність соціальних мереж та маніпулятивні впливи

У цифрову епоху соціальні медіа-платформи здійснили революцію в тому, як ми спілкуємося та взаємодіємо з іншими людьми. Ці платформи пропонують безпрецедентні можливості для обміну інформацією та спілкування з людьми по всьому світу. Однак, оскільки вплив соціальних мереж продовжує зростати, не можна ігнорувати їхній вплив на судочинство. Від впливу на громадську думку до надання потенційних доказів, соціальні медіа мають як позитивні, так і негативні наслідки для правової системи.

Соціальні медіа-платформи надали голос масам, дозволивши людям вільно і миттєво висловлювати свої думки. Ця свобода вираження поглядів має потенціал впливати на громадську думку і на судовий процес. Резонансні справи часто супроводжуються інтенсивними онлайн-дискусіями, дебатами, а іноді навіть кампаніями, які можуть чинити тиск на систему правосуддя. Хоча поінформованість і залучення громадськості можуть бути корисними для

забезпечення правосуддя, проблема полягає в тому, щоб відокремити факти від вигадок, оскільки дезінформація може швидко поширюватися [72].

Платформи соціальних мереж стали скарбницею інформації для юристів. Вони можуть бути цінними джерелами для збору доказів, особливо у справах, пов'язаних з кібербулінгом, наклепом чи переслідуванням. Фотографії, відео, пости та повідомлення в соціальних мережах можуть надати важливу інформацію про діяльність, наміри та зв'язки особи. Однак автентичність і допустимість таких доказів необхідно ретельно перевіряти, щоб запобігти маніпуляціям або спотворенню фактів [21, с. 5].

Використання соціальних мереж у судовому процесі викликає занепокоєння щодо конфіденційності та етичних дилем. Адвокати та слідчі повинні балансувати на тонкій грані між доступом до загальнодоступної інформації та порушенням права особи на приватність. Межі можуть бути розмитими, коли пости в соціальних мережах використовуються для того, щоб зробити висновки про характер або поведінку людини. Балансування між потребою в доказах і захистом приватного життя є постійним викликом.

Повсюдне поширення соціальних мереж створює виклики для забезпечення справедливого судового розгляду. Доступ присяжних до соціальних мереж під час судового процесу може вплинути на їхнє сприйняття справи та потенційно поставити під загрозу неупередженість. Правові системи в усьому світі намагаються запобігти проведенню присяжними незалежного дослідження або впливу на них дискусій у соціальних мережах, пов'язаних зі справою. Для вирішення цієї проблеми впроваджуються суворіші правила та проводяться інформаційні кампанії.

Вплив соціальних мереж на судочинство є незаперечним. Вони здатні формувати громадську думку, надавати докази та ставити етичні проблеми. Хоча вони пропонують безцінні можливості для збору інформації та забезпечення прозорості, вони також вимагають обережного підходу для забезпечення справедливості, захисту приватного життя та запобігання поширенню дезінформації. Оскільки цифровий ландшафт продовжує

розвиватися, правові системи повинні адаптуватися та встановлювати керівні принципи, які забезпечують баланс між використанням потенціалу соціальних медіа та дотриманням принципів справедливості.

Правове регулювання має істотний вплив на діяльність соціальних мереж та на процеси маніпуляції в цифровому просторі. У сучасному світі соціальні мережі стали головним джерелом інформації та комунікації для мільйонів людей; проте вони також створюють нові виклики для суспільства, пов'язані з поширенням дезінформації, пропаганди та маніпуляцій громадською думкою. Ці виклики змушують уряди по всьому світу розробляти та впроваджувати правові механізми, спрямовані на регулювання діяльності соціальних медіа, зокрема на боротьбу з фейковими новинами та маніпуляціями [76].

Одним із головних аспектів впливу правового регулювання на діяльність соціальних мереж є встановлення правил щодо прозорості контенту та відповідальності платформ за поширення неправдивої інформації. У багатьох країнах ухвалено закони, які зобов'язують соціальні мережі вживати заходів для запобігання поширенню дезінформації. Наприклад, у Німеччині ухвалено закон Network Enforcement Act (NetzDG), який зобов'язує платформи видаляти нелегальний контент, включаючи мову ненависті та дезінформацію, протягом 24 годин після отримання повідомлення. За невиконання цих вимог компанії можуть бути оштрафовані на великі суми. Такий підхід має на меті стимулювати соціальні мережі до активнішої боротьби з маніпуляціями, забезпечуючи правові наслідки для компаній, які не виконують ці вимоги.

Крім того, в Європейському Союзі діє Загальний регламент захисту даних (GDPR), що також впливає на діяльність соціальних мереж у контексті збору та використання персональних даних користувачів. Згідно з цим регламентом, соціальні мережі зобов'язані забезпечити захист персональних даних користувачів і не можуть використовувати їх без належної згоди. Це має важливе значення для запобігання маніпуляціям, оскільки зловживання персональними даними може бути використане для таргетованих

інформаційних атак на користувачів, зокрема під час політичних кампаній. GDPR накладає суворі санкції на компанії, які порушують правила захисту даних, що підвищує рівень відповідальності соціальних мереж перед користувачами.

Водночас у США підхід до регулювання соціальних мереж відрізняється від європейського. У США, через велику роль першої поправки до Конституції, яка гарантує свободу слова, уряд має обмежені можливості для регулювання контенту в соціальних мережах. Однак останнім часом, особливо після скандалу з втручанням у вибори 2016 року, влада почала активніше досліджувати питання, пов'язані з прозорістю політичної реклами та використанням соціальних мереж для маніпуляцій громадською думкою. Одним із важливих кроків у цьому напрямку стало запровадження правил щодо прозорості політичної реклами, які вимагають від платформ, таких як Facebook і Google, надавати інформацію про те, хто фінансує політичні оголошення і на яку аудиторію вони таргетовані. Це дозволяє користувачам краще розуміти, хто намагається вплинути на їхню думку та з якою метою [73].

Однак, попри зусилля регуляторів, боротьба з маніпуляціями у соціальних мережах залишається надзвичайно складною. Одна з головних проблем полягає в тому, що соціальні мережі функціонують на глобальному рівні, що ускладнює питання правової юрисдикції. Багато з найбільших платформ, таких як Facebook, Twitter та Instagram, працюють у різних країнах і підпорядковуються різним правовим системам. Це створює ситуацію, коли регулювання в одних країнах може бути менш суворим, ніж в інших, що дозволяє маніпуляторам експлуатувати прогалини в законодавстві.

У підсумку, правове регулювання діяльності соціальних мереж має істотний вплив на забезпечення справедливості та запобігання маніпуляціям. Проте ефективність цих заходів залежить від їхньої адаптації до постійно змінюваного цифрового середовища. Уряди та міжнародні організації повинні працювати над розробкою нових механізмів регулювання, які відповідають викликам, що постають перед суспільством у цифрову епоху. Тільки шляхом

спільних зусиль можна забезпечити баланс між свободою слова та необхідністю захисту суспільства від маніпуляцій у соціальних мережах.

Іншим важливим аспектом правового регулювання є контроль за алгоритмами, які використовуються соціальними мережами для поширення контенту. Алгоритми є центральним елементом у функціонуванні платформ, оскільки вони визначають, який контент бачить користувач. Часто алгоритми налаштовані таким чином, щоб показувати користувачам контент, що викликає сильні емоційні реакції, оскільки це сприяє збільшенню кількості взаємодій і, відповідно, прибутків компаній. Проте такий підхід часто сприяє поширенню маніпулятивного або фейкового контенту, який швидко стає вірусним завдяки своїй емоційній природі. Регулятори у багатьох країнах почали досліджувати можливість контролю за роботою таких алгоритмів, зокрема вимагаючи від компаній забезпечити прозорість їхньої роботи та надавати звіти про те, як вони впливають на поширення інформації.

Окрім державного регулювання, важливу роль у запобіганні маніпуляціям відіграють самі технологічні компанії. Провідні соціальні платформи дедалі більше усвідомлюють свою відповідальність за контент, що поширюється через їхні мережі, і запроваджують власні правила та інструменти для боротьби з маніпуляціями. Наприклад, Facebook активно розробляє інструменти для виявлення та блокування фейкових акаунтів і ботів, які часто використовуються для поширення дезінформації.

Правове регулювання діяльності соціальних мереж в Україні є однією з ключових тем у контексті забезпечення інформаційної безпеки та боротьби з маніпуляціями в цифровому просторі. Соціальні мережі стали не лише засобом комунікації, а й важливим джерелом інформації для мільйонів українців. Проте вони також створюють нові загрози для суспільства, зокрема поширення дезінформації, фейкових новин та маніпуляцій громадською думкою, особливо в умовах війни з Росією та гібридних загроз. Україна як держава знаходиться на передовій у боротьбі з інформаційними атаками та

втручанням, що робить питання правового регулювання соціальних мереж особливо актуальним.

На сьогодні в Україні не існує спеціального закону, який би комплексно регулював діяльність соціальних мереж. Проте це питання частково регулюється низкою правових актів, таких як Закон України «Про інформацію», а також Законом «Про захист персональних даних». Ці закони створюють загальну рамку для функціонування соціальних мереж, зокрема щодо питань захисту даних, відповідальності за поширення неправдивої інформації та забезпечення права громадян на доступ до інформації.

Одним із важливих елементів регулювання є Закон України «Про інформацію», який визначає основні принципи поширення інформації в країні, включаючи цифровий простір. Згідно з цим законом, інформація повинна бути достовірною, а поширення неправдивої інформації може бути підставою для притягнення до відповідальності. Це стосується й соціальних мереж, де дезінформація та маніпуляції часто використовуються для впливу на громадську думку, зокрема в політичних та соціальних питаннях. Проте, попри наявність цього закону, його ефективне застосування у випадку соціальних мереж ускладнене через глобальний характер таких платформ і труднощі з визначенням юрисдикції.

У контексті інформаційної безпеки важливу роль відіграють також заходи щодо боротьби з пропагандою та дезінформацією, які активно використовуються в умовах гібридної війни з Росією. Пропагандистські кампанії, спрямовані на дестабілізацію українського суспільства та маніпуляцію громадською думкою, часто реалізуються через соціальні мережі. Україна вже кілька років стикається з організованими кампаніями дезінформації, що фінансуються та підтримуються з боку Росії. Для протидії таким загрозам уряд України запровадив кілька важливих заходів, включаючи блокування певних соціальних мереж, таких як «ВКонтакте» та «Однокласники», які мали значний вплив на поширення російської пропаганди в Україні.

Ці заходи викликали чимало дискусій у суспільстві щодо балансу між свободою слова та необхідністю забезпечення національної безпеки. Блокування доступу до російських соціальних мереж стало важливим кроком у боротьбі з дезінформацією, однак воно також підняло питання про доцільність таких заходів з точки зору демократичних цінностей. Свобода слова є однією з основних свобод в Україні, закріпленою в Конституції, тому будь-які обмеження повинні бути чітко обґрунтовані та відповідати принципам правової держави.

Однією з головних проблем, з якою стикається Україна у регулюванні діяльності соціальних мереж, є те, що більшість популярних платформ належать іноземним компаніям, таким як Facebook, Google та Twitter, які підпорядковуються іноземному законодавству. Це ускладнює можливість українських регуляторів ефективно контролювати їхню діяльність. Українське законодавство не завжди може бути застосоване до таких глобальних платформ, що створює прогалини у правовому регулюванні. Однак уряд України намагається розвивати співпрацю з міжнародними партнерами, зокрема з Європейським Союзом, для вирішення цих питань.

Важливу роль у контексті правового регулювання відіграє також питання захисту персональних даних. В Україні діє Закон «Про захист персональних даних», який регулює порядок збору, зберігання та використання даних громадян. Це особливо важливо для соціальних мереж, які збирають великі обсяги даних про своїх користувачів. Соціальні мережі використовують ці дані для таргетованої реклами та інших комерційних цілей, однак існують також ризики їх використання для маніпуляцій, зокрема у політичних кампаніях. Скандал з Cambridge Analytica, який розгорівся у 2018 році, показав, як персональні дані можуть використовуватися для маніпулювання виборцями. Україна, слідуючи прикладу Європейського Союзу, намагається удосконалити законодавство у сфері захисту даних, щоб зменшити можливості для їх зловживання.

Окремим аспектом є проблема відповідальності за поширення дезінформації в соціальних мережах. Законодавство України передбачає відповідальність за поширення неправдивої інформації, однак його застосування у випадку цифрового контенту є обмеженим. Соціальні мережі часто стають платформами для поширення фейкових новин, особливо під час політичних виборів або соціальних криз. У 2021 році в Україні було прийнято Закон «Про медіа», який частково регулює діяльність онлайн-платформ і передбачає заходи проти дезінформації, зокрема можливість штрафів для медіа, які систематично поширюють неправдиву інформацію. Однак це законодавство не охоплює всі аспекти діяльності соціальних мереж, особливо в частині відповідальності іноземних платформ.

Ще одним важливим аспектом є питання прозорості реклами у соціальних мережах, зокрема політичної реклами. В Україні діють закони, які регулюють фінансування політичних кампаній і передбачають певні вимоги до прозорості політичної реклами. Проте ці закони не завжди можуть бути ефективно застосовані до соціальних мереж, оскільки багато рекламних кампаній реалізуються через глобальні платформи, які не підпорядковуються українському законодавству. Це створює можливості для маніпуляцій, оскільки політичні сили можуть використовувати соціальні мережі для поширення таргетованих повідомлень, які не контролюються належним чином [24, с. 104].

Правове регулювання діяльності соціальних мереж в Україні стикається з низкою викликів. Основними проблемами є відсутність комплексного закону, який чітко регулював би діяльність соціальних медіа, а також обмежені можливості українських регуляторів у боротьбі з глобальними платформами. Однак уряд України активно працює над розвитком законодавства у цій сфері, зокрема в контексті захисту персональних даних та протидії дезінформації. Співпраця з міжнародними партнерами, зокрема з ЄС, також відіграє важливу роль у розробці ефективних механізмів правового регулювання діяльності соціальних мереж та забезпеченні інформаційної безпеки.

Судова практика. У березні 2020 року в Україні було запроваджено карантин у зв'язку з оголошенням пандемії коронавірусу Covid-19. Ця тема викликала значний резонанс і спричинила появу численних повідомлень, у тому числі й неправдивих, які активно поширювалися в соціальних мережах, зокрема у Facebook. У відповідь на це правоохоронні органи почали активно складати протоколи про адміністративні правопорушення, передбачені статтею 173-1 КУпАП (поширення неправдивих чуток), і передавати їх до суду. Це призвело до формування нової, місцями неоднозначної практики притягнення до відповідальності за поширення чуток в інтернеті. У квітні – липні 2020 року експерти ГО «Платформа прав людини» в рамках моніторингу цифрових прав проаналізували 145 судових постанов за статтею 173-1 КУпАП. У квітні в Єдиному державному реєстрі судових рішень було опубліковано 32 такі постанови, у травні їх кількість зросла до 48, а в червні та липні їх стало менше — 38 і 27 відповідно. Майже всі справи стосувалися тем, пов'язаних із Covid-19. Стаття 173-1 КУпАП передбачає адміністративну відповідальність за поширення неправдивих чуток, які можуть спричинити паніку або порушити громадський порядок, і накладає штраф у розмірі від 170 до 255 гривень або виправні роботи терміном до одного місяця з відрахуванням 20% заробітку. Протягом тридцяти років з моменту включення цієї статті до Кодексу вона майже не використовувалася і застосовувалася лише в окремих випадках. Однак із появою коронавірусу та запровадженням карантину ситуація змінилася. На початку червня 2020 року СБУ повідомила, що за період дії карантинних заходів її кіберфахівці виявили 393 особи, які поширювали фейки про Covid-19, і передали інформацію про 367 з них до Національної поліції. СБУ також повідомила, що у квітні-травні 2020 року до адміністративної відповідальності за статтею 173-1 КУпАП було притягнуто 160 осіб, хоча в ЄДРСР на той час було знайдено лише 80 справ, а за період з квітня по липень 2020 року загалом виявлено 145 рішень за цією статтею [39].

Правове регулювання діяльності соціальних мереж у США є складним і динамічним процесом, що постійно розвивається під впливом технічного

прогресу, соціальних змін та політичних подій. Оскільки Сполучені Штати є домом для найбільших світових соціальних платформ, таких як Facebook, Twitter, Instagram і TikTok, регуляторні підходи, які впроваджуються в цій країні, мають глобальний вплив. Однак характер американської системи правового регулювання відрізняється від багатьох інших країн через наявність сильного конституційного захисту свободи слова, закріпленого Першою поправкою до Конституції США. Це створює як можливості, так і обмеження для державного втручання в діяльність соціальних мереж.

Перша поправка до Конституції США гарантує свободу слова і значно обмежує можливості держави втручатися в контент, який поширюється в соціальних мережах. На відміну від багатьох європейських країн, де державні органи можуть запроваджувати суворі заходи щодо боротьби з дезінформацією та фейковими новинами, в США регулювання контенту є надзвичайно чутливим питанням. Держава не може безпосередньо цензурувати або контролювати висловлювання в соціальних мережах, якщо вони не порушують конкретні закони, такі як закони про наклеп, погрози або підбурювання до насильства [58].

Попри це, американське законодавство поступово адаптується до нових викликів, пов'язаних з діяльністю соціальних мереж. Однією з ключових правових норм, що регулює діяльність соціальних платформ, є розділ 230 Закону про порядність в комунікаціях (Communications Decency Act), ухваленого в 1996 році. Цей розділ надає соціальним мережам правовий захист від відповідальності за контент, що публікують користувачі. Відповідно до розділу 230, платформи не вважаються видавцями і, отже, не несуть відповідальності за матеріали, що створюються третіми сторонами. Це положення стало ключовим для розвитку інтернет-екосистеми в США, оскільки воно дозволило соціальним мережам вільно функціонувати без страху постійних судових позовів через контент користувачів [74].

Однак упродовж останніх років з'явилося чимало критики щодо розділу 230, оскільки багато хто вважає, що він надає платформам занадто великий

захист і не стимулює їх до активної боротьби з дезінформацією, мовою ненависті та іншими формами маніпуляцій. Ці дебати особливо загострилися після президентських виборів у США в 2016 році, коли було виявлено значне втручання іноземних акторів у виборчий процес через соціальні мережі. Багато хто вимагав реформування розділу 230, щоб зобов'язати платформи активніше контролювати контент, який може завдати шкоди суспільству. У відповідь на це деякі політики пропонували внести зміни до закону, щоб обмежити захист для платформ у випадках, коли вони не виконують своїх зобов'язань щодо видалення шкідливого або незаконного контенту [53].

Крім того, важливим напрямком регулювання діяльності соціальних мереж у США є питання прозорості реклами, особливо політичної реклами. Після виборів 2016 року та розслідування втручання Росії у виборчий процес стало очевидним, що соціальні мережі використовувалися для поширення таргетованої політичної реклами з метою впливу на виборців. Це викликало значні занепокоєння з приводу прозорості таких рекламних кампаній і призвело до запровадження нових вимог до платформ. Наприклад, Facebook і Twitter впровадили нові інструменти, які дозволяють користувачам бачити, хто спонсорує політичну рекламу, і які суми витрачаються на її просування [56].

Одним із найзначніших випадків правового регулювання соціальних мереж у США стало рішення Верховного Суду США у справі «*Packingham v. North Carolina*» у 2017 році. Суд постановив, що державний закон, який забороняє зареєстрованим сексуальним злочинцям користуватися соціальними мережами, порушує Першу поправку. Це рішення підкреслило важливість захисту прав користувачів у цифровому середовищі і вказало на необхідність дотримання конституційних норм при регулюванні діяльності соціальних платформ. Суд зазначив, що соціальні мережі стали важливими комунікаційними каналами в сучасному суспільстві і їх використання є важливим для реалізації свободи слова [69].

Правове регулювання соціальних мереж є складним та динамічним процесом, що постійно еволюціонує під впливом нових технологій та соціальних змін. В Україні існує потреба в удосконаленні законодавства щодо соціальних медіа, щоб забезпечити захист прав користувачів та протидію дезінформації. У США, попри потужний захист свободи слова, також ведеться активний діалог про необхідність реформування регулювання соціальних платформ. Обидві країни стикаються з подібними викликами, пов'язаними з боротьбою з дезінформацією та забезпеченням прозорості політичної реклами, що підкреслює глобальний характер проблеми.

Однак, попри ці зусилля, США поки що не мають загальнонаціонального закону про захист даних, подібного до європейського Загального регламенту захисту даних (GDPR). У деяких штатах, таких як Каліфорнія, вже ухвалені власні закони про захист персональних даних, зокрема Закон про захист приватності споживачів у Каліфорнії (California Consumer Privacy Act, CCPA), який надає жителям штату більше контролю над тим, як їхні дані збираються та використовуються. Цей закон став важливим кроком уперед для захисту прав користувачів, і його можна вважати прообразом національних законів, які можуть бути ухвалені в майбутньому.

Ще одним важливим напрямком правового регулювання соціальних мереж у США є боротьба з дезінформацією та маніпуляціями. Соціальні мережі, такі як Facebook і Twitter, відіграють центральну роль у поширенні новин, тому вони стають основною мішенню для дезінформаційних кампаній. Це особливо актуально під час виборчих кампаній та соціальних криз, коли поширення фейкових новин може мати серйозні наслідки для громадської думки та безпеки. Відповідно, уряд США почав активно вивчати можливості для регулювання поширення дезінформації у соціальних мережах; однак це завдання залишається складним через необхідність дотримання принципу свободи слова [57].

Технологічні компанії також почали вживати заходів для боротьби з дезінформацією, впроваджуючи системи перевірки фактів і маркування

контенту, який може бути неправдивим. Наприклад, Facebook створив програму співпраці з незалежними організаціями, що займаються перевіркою правдивості новин, які поширюються на платформі. Це дозволяє зменшити вплив фейкових новин, оскільки користувачі отримують попередження про можливу неправдивість інформації. Проте критики стверджують, що таких заходів може бути недостатньо для запобігання широкомасштабним маніпуляціям [55].

Незважаючи на всі зусилля, регулювання діяльності соціальних мереж у США стикається з низкою серйозних викликів. Один із них полягає в тому, що соціальні мережі є глобальними платформами, і багато дезінформаційних кампаній організовуються з-за кордону, що ускладнює контроль з боку національних органів. Це вимагає міжнародної співпраці та координації між державами для боротьби з глобальними загрозами.

Підсумовуючи, правове регулювання діяльності соціальних мереж у США розвивається під впливом численних викликів, таких як захист свободи слова, боротьба з дезінформацією, забезпечення прозорості політичної реклами та захист персональних даних. Попри наявність певних досягнень у цих сферах, подальші зусилля необхідні для адаптації законодавства до нових реалій цифрового світу.

Висновки до 3 розділу

Методи маніпуляційної діяльності в соціальних мережах ґрунтуються на використанні емоційного впливу, дезінформації, таргетованої реклами, ботів і фейкових акаунтів, а також на алгоритмах, які підсилюють маніпулятивний контент. Основна мета таких методів – вплинути на громадську думку або поведінку користувачів через спотворення реальності, апелювання до страхів, упереджень або емоцій. Поширення фейкових новин та дезінформації часто орієнтоване на специфічні групи, які є найбільш уразливими до певних типів контенту, що робить маніпуляцію ще більш ефективною. Використання ботів і автоматизованих акаунтів дозволяє створити враження масової підтримки або певної думки, що підсилює віру в правдивість інформації. Алгоритми соціальних мереж, які налаштовані на підвищення взаємодії користувачів, часто сприяють поширенню саме маніпулятивного контенту, оскільки він викликає більше емоційних реакцій.

Протидія маніпуляційним впливам у сучасному інтернет-просторі є надзвичайно важливим викликом, який потребує комплексного підходу з боку держав, міжнародних організацій, технологічних компаній та самих користувачів. Інтернет, зокрема соціальні мережі, став основним полем для поширення дезінформації, фейкових новин, пропаганди та інших форм маніпуляції, що може мати серйозні наслідки для суспільства, політики та безпеки. Держави повинні розробляти та впроваджувати ефективні правові механізми, які забезпечують боротьбу з маніпуляціями, але при цьому не порушують фундаментальні права на свободу слова та приватність.

Міжнародна співпраця також є ключовим елементом у протидії, оскільки маніпуляції часто мають глобальний характер. Технологічні компанії, володіючи величезними ресурсами та даними, повинні брати на себе відповідальність за захист користувачів від маніпулятивного контенту, вдосконалюючи алгоритми для виявлення фейкових новин, ботів і дезінформаційних кампаній. Водночас підвищення рівня цифрової

грамотності населення має важливе значення для зміцнення стійкості до маніпуляцій. Лише через спільні зусилля можна забезпечити безпеку інтернет-простору та захистити суспільство від маніпуляційних впливів, які стають дедалі складнішими й небезпечнішими в умовах постійного розвитку технологій.

ВИСНОВКИ

При написанні роботи відповідно до мети дослідження та поставлених завдань було сформульовано наступні висновки.

1. Теоретико-методологічні підходи до регулювання інтернет-відносин у США ґрунтуються на балансі між свободою слова, інноваціями та захистом прав користувачів. Ключовим принципом є Перша поправка до Конституції США, яка гарантує свободу висловлювань і обмежує державне втручання в контент, що поширюється онлайн. Водночас важливу роль у регулюванні інтернет-простору відіграє розділ Закону про порядність у комунікаціях (Communications Decency Act), який звільняє платформи від відповідальності за контент, створений користувачами, і надає їм право на модерацію. Цей підхід дозволив технологічним компаніям розвиватися, однак останніми роками викликає дискусії щодо його реформування через поширення дезінформації та маніпуляцій. Регуляція також включає спроби захисту приватності, як, наприклад, Закон про захист приватності споживачів у Каліфорнії (CCPA), що покликає захищати дані користувачів. Проте на загальнонаціональному рівні ще тривають обговорення щодо впровадження подібного законодавства.

Загалом, джерельна база дослідження регулювання інтернет-відносин у США є різноманітною та розмаїтою, включаючи офіційні документи, судову практику, урядові звіти, академічні дослідження та міжнародні документи. Ці джерела надають широкий обсяг інформації та аналізу, необхідного для розуміння регулятивного середовища в галузі інтернету. Роль джерел права в регулюванні інтернет-відносин у США та в інших країнах із високорозвиненою інтернет-інфраструктурою є вельми значною. Інтернет є динамічною сферою, що постійно змінюється, і ефективне регулювання цієї сфери вимагає наявності відповідного правового каркасу, який би враховував технологічні та соціальні аспекти використання Інтернету.

2. Правові підходи до регулювання соціальних мереж у США характеризуються балансом між захистом свободи слова та необхідністю контролювати дезінформацію, маніпуляції й інші негативні явища в інтернет-просторі. Однією з ключових правових основ у регулюванні є Перша поправка до Конституції США, яка забезпечує сильний захист свободи висловлювань. Це означає, що державне втручання в контент, поширюваний на платформах соціальних мереж, є обмеженим. Держава не може прямо цензурувати висловлювання, навіть якщо вони є непопулярними чи спірними, за винятком тих випадків, коли контент порушує закони, наприклад, пов'язані з насильством або підбурюванням до протиправних дій.

Ще одним важливим напрямком регулювання є політика прозорості щодо політичної реклами в соціальних мережах. Після виборів 2016 року в США, коли було виявлено масштабне втручання в політичний процес через соціальні мережі, постало питання про те, наскільки користувачі обізнані про джерела фінансування політичної реклами, яку вони бачать. Це призвело до запровадження нових правил, які вимагають від платформ, таких як Facebook і Google, розкривати інформацію про те, хто фінансує політичні оголошення та кому вони таргетовані. Такі заходи спрямовані на забезпечення більшої прозорості та запобігання маніпуляціям з боку іноземних і внутрішніх акторів.

Окрім того, регулювання соціальних мереж у США також стосується питань захисту персональних даних користувачів. Незважаючи на те, що загальнонаціонального закону про захист даних на рівні всієї країни поки що не існує, певні штати, зокрема Каліфорнія, ухвалили власне законодавство, яке регулює цей аспект. Наприклад, Закон про захист приватності споживачів у Каліфорнії (California Consumer Privacy Act, CCPA) надає жителям штату право знати, які дані про них збираються, і вимагає від компаній прозорості в обробці цих даних. Хоча цей закон діє лише в межах одного штату, він став важливим кроком у напрямку посилення регулювання приватності в соціальних мережах і може слугувати зразком для впровадження загальнонаціональних норм.

3. Протидія маніпуляційним впливам у сучасному інтернет-просторі є однією з ключових проблем інформаційної безпеки. Соціальні мережі, блоги, новинні ресурси та інші цифрові платформи відіграють важливу роль у формуванні громадської думки, політичних переконань і соціальної поведінки. Однак водночас ці платформи стали простором для поширення дезінформації, фейкових новин і маніпуляцій, що має серйозні наслідки для суспільства та держав.

Одним із основних методів протидії маніпуляціям є правове регулювання діяльності цифрових платформ і впровадження політик боротьби з фейковими новинами. У багатьох країнах уряди розробляють закони та нормативні акти, спрямовані на запобігання поширенню неправдивої інформації в інтернеті.

Крім законодавчих заходів, важливу роль відіграють технологічні компанії, що володіють платформами соціальних мереж. Провідні технологічні корпорації, такі як Facebook, Twitter, Google, зобов'язані впроваджувати власні політики боротьби з дезінформацією, використовуючи автоматизовані системи для виявлення фейкових новин, ботів і дезінформаційних кампаній.

Отже, основною складовою протидії маніпуляціям є підвищення рівня цифрової грамотності населення. Навчання користувачів тому, як розпізнавати фейкові новини та критично оцінювати інформацію, яку вони отримують в інтернеті, є важливим інструментом захисту від маніпуляцій. Багато країн впроваджують освітні програми, спрямовані на підвищення обізнаності населення щодо дезінформації та цифрової безпеки. Крім того, міжнародні організації, такі як ООН і ЄС, активно підтримують ініціативи щодо розвитку цифрової грамотності на глобальному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонович М. М. Міжнародне право : навч. посіб. Київ : Юрінком Інтер, 2011. 384 с.
2. Баймуратов М. О. Міжнародне публічне право : підручник. Київ : Фенікс; 2018. 762 с.
3. Батрименко В. І. Міжнародне право : навч. посіб. Київ : Київ. нац. торговел.-економ. ун-т, 2012. 323 с.
4. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. *Громадська думка про правотворення*. 2017. С. 131-137.
5. Буткевич О. В. Історія міжнародного права : підручник. Київ : Ліра-Ка, 2018. 408 с.
6. Гавриленко О. А. Історія міжнародного права : хрестоматія-практикум. Харків : Вид-во Харків. нац. ун-ту ім. В. Н. Каразіна, 2016. 676 с.
7. Гердеген М. Міжнародне право. Київ : К.І.С., 2011. 516 с.
8. Голуб Н. В. Україна та міжнародні організації : інформ.-довід. вид. Київ : Кондор, 2010. 182 с.
9. Дейвид Патрикаракос. Війна у 140 знаках. Як соціальні медіа змінюють конфлікти у ХХІ столітті. Київ : Yakaboo Publishing, 2019. 352 с.
10. Дяченко О. Особливості мовно-маніпулятивного впливу за різних типів політичного режиму. *Актуальні проблеми політики*. Одеса, 58, 2016. С. 29–40.
11. Дяченко О. В. Політичне маніпулювання в США та Україні: порівняльна характеристика. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Історія. Філософія. Політологія: зб. наук. праць, Одеса, 12, 2016, С. 122–126.
12. Дяченко О. Стратегії та прийоми мовно-маніпулятивного впливу в ході політичного конфлікту. *Актуальні проблеми політики*. Одеса, 59, 2017, С. 41–53.

13. Дяченко О. Складові механізму реалізації мовної маніпуляції в політиці. *Політичне життя*, 2, 2018. С. 91–97.
14. Задорожній О. В. Від теорії міжнародного права до практики захисту прав людини : монографія. Київ : Фенікс, 2018. 718 с.
15. Задорожній О. В. Міжнародне право навколишнього середовища : підручник. Київ : Промені, 2010. 510 с.
16. Зафейсбучені. Як соціальна мережа штовхає світ до катастрофи. Письменник: Роджер Макнамі Рік: 2021. Видавництво: книголав. 376 с.
17. Кісілевич-Чорнойван О. М. Міжнародне інформаційне право : навч. посіб. Київ : Персонал, 2011. 160 с.
18. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата перегляду: 15.05.2024).
19. Кодекс Сполучених Штатів Америки (U. S. Code) URL: <https://www.law.cornell.edu/uscode/text/6/1501> (date of access: 21.02.2024).
20. Кормич Б. А. Інформаційне право : підручник. Харків : Бурун і К., 2011. 334 с.
21. Корченко О., Логінов І., Скворцов С. Стаціонарні системи виявлення і попередження кібератак в інтересах кіберзахисту та кіберконтррозвідки (на прикладі США). *Безпека інформації*. 2019, Т. 25. Вип. 1, С. 5–12.
22. Макаренко Є. А. Міжнародна інформаційна безпека: теорія і практика : підручник. Київ : Центр віл. преси, 2016. 417 с.
23. Митко А. М. Інформаційна демократія: реалії та виклики часу: монографія. Луцьк: Вежа-друк, 2014. 400 с.
24. Мишок Р. Р. Громадянська Інтернет-поведінка львівської студентської молоді: спроба визначення і класифікації. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2019. Випуск 3 (43). С. 104–110.
25. Мінченко О. 68% українських користувачів Facebook заходять в соцмережу виключно з мобільних телефонів. *Watcher*. 12 лютого 2019. URL:

<http://watcher.com.ua/2019/02/12/68-ukrayinskyh-korystuvachiv-facebook-zahodyat-v-sotsmerezhu-vyklyuchno-z-mobilnyh-telefoniv/> (дата перегляду: 07.06.2024).

26. Мороз О. 54% українців в Facebook публікують фейки, маніпуляції та сайти-сміттярки. Всеукраїнське дослідження. Українська правда. 14 вересня 2020. URL: <https://www.pravda.com.ua/articles/2020/09/14/7266269/> (дата перегляду: 07.06.2024).

27. Мудра І. Соціальні мережі в Інтернеті як інструмент просування «зараженої» інформації. *Теле- та радіожурналістика*. 2015. Випуск 14. С. 208–213.

28. Найпопулярніші соціальні мережі в Україні та країнах світу 2020. Український спектр. 23 червня 2020. URL: <https://uaspectr.com/2020/06/23/najpopulyarnishi-sotsialni-merezhi-v-ukrayini-ta-krayinah-svitu-2020/> (дата перегляду: 11.06.2024).

29. Нашинець-Наумова А.Ю. Інформаційна безпека суб'єктів господарювання: проблеми теорії та практики правозастосування : монографія; під заг. ред. д.ю.н. В.І. Курила. Херсон : Видавничий дім «Гельветика», 2017. 386 с.

30. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. К. : Видавничий дім «Гельветика», 2017. 169 с.

31. Нашинець-Наумова А.Ю. Основи інформаційного права навчальний посібник. К. : Вив-во «Сталь», 2015. 198 с.

32. Нашинець-Наумова А.Ю. Правове забезпечення інформаційної безпеки: міжнародний досвід і можливість використання. *Право і суспільство*. Дніпро, 2018. № 6. С. 159–164.

33. Нашинець-Наумова А.Ю. Світовий досвід законодавчої регламентації режимів конфіденційної інформації. *Підприємництво, господарство і право*. Київ, 2019. № 4. С. 166–171.

34. Ничипорчук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2018. № 1. С. 66–71.

35. Саморегуляція медіа світовий досвід. Detector.media. URL: <https://ms.detector.media/mediaanalitika/post/13308/2015-05-22-samoregulyatsiya-v-media-svitovyyu-dosvid/> (дата перегляду: 19.06.2024).

36. Сінек С. «Почни з ЧОМУ, або як відомі лідери надихають до дії кожного». Київ, «Основи», 2015. 256 с.

37. Половинчак Ю. Мобілізаційний та маніпулятивний потенціал дискурсу соціальних медіа в умовах перехідного суспільства. Центр досліджень соціальних комунікацій НБУВ. URL: http://nbuviar.gov.ua/index.php?option=com_content&view=article&id=446:s_220_otsialni-media&catid=8&Itemid=350 (дата перегляду: 14.07.2024).

38. Попова Т. Соціальні мережі, кібератаки та гібридні війни. Радіо Свобода. 6 липня 2017. URL: <https://www.radiosvoboda.org/a/28598299.html> (дата перегляду: 03.07.2024).

39. Постанова за справою №766/5783/20, Пров. №3/766/3210/20 від 05.05.2020. URL: <https://reyestr.court.gov.ua/Review/89027625> (дата перегляду: 04.06.2024).

40. Потіха А. Л. Засоби масової комунікації політичних партій в інформаційно-аналітичній діяльності бібліотек України (1990–2010-ті рр.). Дис. ... канд. наук із соціальних комунікацій за спеціальністю 27.00.03. Національна бібліотека України імені В. І. Вернадського. Київ, 2018. 234 с.

41. Почепцов Г. Медіа-культура у політичній сфері. *Політична думка*. 2015. № 4. С. 10–12.

42. Практика використання «мови ворожнечі» (hate speech) українськими ЗМІ: дослідження. MediaSapiens. Детектор.Медіа. 8 вересня 2015. URL: <https://ms.detector.media/mediadoslidzhennya/post/14140/2015-09-08-doslidzhennya-praktika-vikoristannya-movi-vorozhnechi-hate-speechukrainskimi-zmi/> (дата перегляду: 05.06.2024).

43. Практика використання інструментів електронної демократії громадськими організаціями в Україні. Результати експертного опитування, проведеного у січні-лютому 2016 р. URL: http://dialog.lviv.ua/wp-content/uploads/2016/03/Report_E-Democracy-Toolsfor-NGOs_1-1.pdf (дата перегляду: 05.06.2024).

44. Присяжнюк М. М., Христофорова О. Ф. Інтернет-простір як арена сугестії в інформаційних війнах сучасності. *Інформаційна безпека людини, суспільства, держави*. 2017. № 1 (21). С. 191–199.

45. Проблеми суспільної безпеки в процесі розвитку соціальних мереж: [монографія] / [В. І. Попик (керівник проекту) та ін.] ; НАН України, Нац. 221 б-ка України ім. В. І. Вернадського. Київ : НБУ ім. В. І. Вернадського, 2015. 199 с.

46. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата перегляду: 12.04.2024).

47. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 квіт. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата перегляду: 28.05.2024).

48. Ставлення населення до ЗМІ та споживання різних типів медіа у 2019 році. URL: <https://detector.media/infospace/article/171769/2019-10-22-stavlennya-naselennya-do-zmi-ta-spozhyvannya-riznykh-typiv-media-u-2019-r/> (дата перегляду: 30.05.2024).

49. Стасюк Т. Технології мовного впливу як компонент сучасної комунікації. *Українська правда*. 2010. № 1. С. 82–87.

50. Чужиков А. Поліструктурна динаміка глобалізованого медіаринку ЄС : монографія. Київ : КНЕУ, 2016. 367 с.

51. Як соціальні мережі впливають на політику в Україні: висновки дослідження. Інтерньюз Україна. 28 листопада 2019. URL:

<https://internews.ua/opportunity/social-network-research> (дата перегляду: 13.06.2024).

52. Якименко Ю. Соціальні медіа як інструмент дослідження проблем розвитку. *Центр досліджень соціальних комунікацій НБУВ*. 2016. Вип. 43. С. 501–516.

53. Carter-Parks A. E. The 21st Century Activist's Dilemma: Social Media's Impact on the Occupy and Tea Party Movements. New York: Annandale-onHudson, 2015. 64 p.

54. Casteltrione I. The Internet, social networking Web sites and political participation research: Assumptions and contradictory evidence. *First Monday*, Volume 20, Number 3–2. March 2015. URL: <https://firstmonday.org/article/view/5462/4403> (date of access: 11.07.2024).

55. Chagas V., Freire F., Rios D., Magalhães D. The political memes and the politics of memes: Methodological proposal for a content analysis of online political memes. *First Monday*. Vol. 24 (2–4). February 2019. URL: <https://firstmonday.org/ojs/index.php/fm/article/download/7264/7731> (date of access: 14.07.2024).

56. Chan M. Social Network Sites and Political Engagement: Exploring the Impact of Facebook Connections and Uses on Political Protest and Participation. *Mass Communication & Society*. 2016. Vol. 19(4). PP. 430–451.

57. Clement J. Global influence of social media on polarization in politics 2019, by country. Statista. 2020. September 11. URL: <https://www.statista.com/statistics/1015170/impact-of-social-media-polarization-in-politics-by-country/> (date of access: 17.05.2024).

58. Clement J. Global influence of social media on accountability in government 2019, by country. Share of internet users who believe that social media platforms have influenced accountability in government as of February 2019, by country Statista. 2020. September 11. URL: <https://www.statista.com/statistics/1015153/impact-of-social-media-accountability-in-government-by-country/> (date of access: 17.05.2024).

59. Cybersecurity and Cyberwar: What Everyone Needs to Know, P. W. Singer and Allan Friedman. Oxford University Press, 2015, 306 pp.
60. Clement J. Social media and politics in the United States – Statistics & Facts. Statista. 2020. 10 September. URL: <https://www.statista.com/topics/3723/social-media-and-politics-in-the-unitedstates/> (date of access: 22.05.2024).
61. Denk T., Christensen H. How to classify political cultures? A comparison of three methods of classification. *Quality & Quantity*, 2016, January, Vol. 50, Issue 1, P. 177–191.
62. Digital 2020: 3.8 billion people use social media. We are social. URL: <https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-usesocial-media> (date of access: 19.03.2024).
63. Freedom on the Net 2019. Freedom House. URL: <https://freedomhouse.org/country/ukraine/freedom-net/2019> (date of access: 10.03.2024).
64. Hoskins A., O'Loughlin, B. Arrested war: The third phase of mediatization. *Information, Communication & Society*. 2015. Vol. 18(11). P. 1320–1338.
65. Howard Ph. Is Social Media Killing Democracy? University of Oxford. 2016. 15 November. URL: <https://www.oii.ox.ac.uk/blog/is-social-mediakilling-democracy/> (date of access: 02.03.2024).
66. Josselyn S. The new trend of M&A in the media industry. URL: <https://www.deallawwire.com/2016/11/22/thenew-trend-of-ma-in-the-media-industry/> (date of access: 27.03.2024).
67. Like War – The Weaponization of Social Media, by P. W. Singer and Emerson T. Brooking, 2018, 180 p.
68. Media consumption survey-Ukraine 2016. Internews. URL: <https://internews.org/resource/media-consumption-survey-ukraine-2016> (date of access: 25.03.2024).

69. Muller K., Schwarz C. Fanning the Flames of Hate: Social Media and Hate Crime. SSRN. Electronic journal. 2017. January. URL: https://www.researchgate.net/publication/321959002_Fanning_the_Flames_of_Hate_ (date of access: 10.04.2024).

70. National Cyber Strategy of the United States of America / офіційний вебсайт Білого дому Сполучених Штатів Америки. URL: <https://elar.naiu.kiev.ua/server/api/core/bitstreams/cdb0e86f-9d10-489a-82a9-1e69c8737417/content> (date of access: 10.04.2024).

71. Official website of the Department of Homeland Security. URL: <https://www.cisa.gov/about-cisa> (date of access: 13.04.2024).

72. Owen D. The New Media's Role in Politics /The Age of Perplexity: Rethinking the World We Knew. Open Mind. URL: <https://www.bbvaopenmind.com/en/articles/the-new-media-s-role-in-politics/> (date of access: 21.04.2024).

73. Owen D. The Past Decade and Future of Political Media: The Ascendance of Social Media. Open Mind. URL: <https://www.bbvaopenmind.com/en/articles/the-past-decade-and-future-ofpolitical-media-the-ascendance-of-social-media/> (date of access: 21.04.2024).

74. Pierre C. What is the Difference between Social Media and Social Network? URL: https://medium.com/@christina_meyer/what-is-the-difference-between-social-media-and-social-network-e6dd5ad28d8f (date of access: 08.04.2024).

75. Roper W. Using Social Media for Political Issues. Statista. 2020. July 13. URL: <https://www.statista.com/chart/22264/social-media-for-cultural-socialissues/> (date of access: 08.04.2024).

76. Schauer P. 5 Biggest Differences between Social Media and Social Networking. *Social Media Today*. 2015. June 28. URL: <https://www.socialmediatoday.com/social-business/peteschauer/2015-06-28/5-biggest-differences-between-social-media-and-social> (date of access: 26.04.2024).

77. Solis B. Engage! The Complete Guide for Brands and Businesses to Build, Cultivate, and Measure Success in the New Web, Revised and Updated. New Jersey, Hoboken: John Wiley & Sons. 2014. 381 p.

78. The International comparative Legal Guides and the International Bussiness reports / вебсайт Global Legal Group URL: <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa> (date of access: 28.03.2024).

79. The world's most-used social platforms. Digital 2020. Global Overview/ 2020. January 25. URL: <https://wearesocial-net.s3-eu-west-1.amazonaws.com/wp-content/uploads/common/reports/digital-2020/digital-2020-global.pdf> (date of access: 20.03.2024).

80. Zhdanova M., Orlova D. Computational Propaganda in Ukraine: Caught Between External Threats and Internal Challenges / Working Paper 2017. 9 Oxford, UK: Project on Computational Propaganda. 27 p.

Zusammenfassung

Beim Verfassen der Arbeit wurden gemäß den Forschungszielen und den gestellten Aufgaben folgende Schlussfolgerungen formuliert:

1. Die theoretisch-methodologischen Ansätze zur Regulierung von Internetbeziehungen in den USA basieren auf einem Gleichgewicht zwischen Meinungsfreiheit, Innovationen und dem Schutz der Rechte der Nutzer. Das zentrale Prinzip ist der Erste Verfassungszusatz der Vereinigten Staaten, der die Meinungsfreiheit garantiert und staatliche Eingriffe in online verbreitete Inhalte einschränkt. Gleichzeitig spielt der Abschnitt des Gesetzes über Anstand in der Kommunikation (Communications Decency Act) eine wichtige Rolle bei der Regulierung des Internetraums. Dieser Abschnitt befreit Plattformen von der Verantwortung für von Nutzern erstellte Inhalte und gewährt ihnen das Recht auf Moderation. Dieser Ansatz hat es Technologieunternehmen ermöglicht, sich zu entwickeln, doch in den letzten Jahren wird über eine Reform diskutiert, insbesondere wegen der Verbreitung von Desinformationen und Manipulationen. Die Regulierung umfasst auch Versuche, die Privatsphäre zu schützen, wie etwa durch den California Consumer Privacy Act (CCPA), der den Schutz von Nutzerdaten gewährleisten soll. Auf nationaler Ebene werden jedoch noch Diskussionen über die Einführung ähnlicher Gesetzgebung geführt.

Insgesamt ist die Quellenbasis der Untersuchung zur Regulierung von Internetbeziehungen in den USA vielfältig und umfangreich. Sie umfasst offizielle Dokumente, Rechtsprechung, Regierungsberichte, akademische Studien und internationale Dokumente. Diese Quellen bieten eine Fülle von Informationen und Analysen, die notwendig sind, um das regulatorische Umfeld im Bereich des Internets zu verstehen. Die Rolle der Rechtsquellen bei der Regulierung von Internetbeziehungen in den USA und in anderen Ländern mit hochentwickelter Internetinfrastruktur ist von großer Bedeutung. Das Internet ist

ein dynamischer Bereich, der sich ständig verändert. Eine effektive Regulierung dieses Bereichs erfordert einen geeigneten rechtlichen Rahmen, der sowohl die technologischen als auch die sozialen Aspekte der Internetnutzung berücksichtigt.

2. Die rechtlichen Ansätze zur Regulierung sozialer Netzwerke in den USA zeichnen sich durch ein Gleichgewicht zwischen dem Schutz der Meinungsfreiheit und der Notwendigkeit aus, Desinformation, Manipulationen und andere negative Phänomene im digitalen Raum zu kontrollieren. Eine der zentralen rechtlichen Grundlagen der Regulierung ist der Erste Verfassungszusatz der Vereinigten Staaten, der einen starken Schutz der Meinungsfreiheit gewährleistet. Dies bedeutet, dass staatliche Eingriffe in Inhalte, die auf Social-Media-Plattformen verbreitet werden, begrenzt sind. Der Staat kann Äußerungen nicht direkt zensieren, selbst wenn sie unpopulär oder kontrovers sind, es sei denn, die Inhalte verstoßen gegen Gesetze, etwa im Zusammenhang mit Gewalt oder der Anstiftung zu rechtswidrigen Handlungen.

Ein weiterer wichtiger Bereich der Regulierung ist die Transparenzpolitik in Bezug auf politische Werbung in sozialen Netzwerken. Nach den Präsidentschaftswahlen 2016 in den USA, bei denen groß angelegte Eingriffe in den politischen Prozess über soziale Netzwerke aufgedeckt wurden, entstand die Frage, wie gut Nutzer über die Finanzierung der politischen Werbung, die sie sehen, informiert sind. Dies führte zur Einführung neuer Regeln, die Plattformen wie Facebook und Google dazu verpflichten, Informationen darüber offenzulegen, wer politische Anzeigen finanziert und auf welche Zielgruppen diese ausgerichtet sind. Diese Maßnahmen zielen darauf ab, mehr Transparenz zu schaffen und Manipulationen durch ausländische und inländische Akteure zu verhindern.

Darüber hinaus betrifft die Regulierung sozialer Netzwerke in den USA auch den Schutz der persönlichen Daten der Nutzer. Obwohl es bisher kein landesweites Datenschutzgesetz gibt, haben einige Bundesstaaten, insbesondere Kalifornien, eigene Gesetze erlassen, die diesen Aspekt regeln. So gewährt der California Consumer Privacy Act (CCPA) den Einwohnern Kaliforniens das Recht zu erfahren, welche Daten über sie gesammelt werden, und verpflichtet Unternehmen, bei der Verarbeitung dieser Daten transparent zu sein. Obwohl dieses Gesetz nur auf Bundesstaatsebene gilt, stellt es einen wichtigen Schritt zur Stärkung des Datenschutzes in sozialen Netzwerken dar und könnte als Vorbild für die Einführung nationaler Standards dienen.

3. Die Bekämpfung manipulativer Einflüsse im modernen Internetraum ist eines der zentralen Probleme der Informationssicherheit. Soziale Netzwerke, Blogs, Nachrichtenportale und andere digitale Plattformen spielen eine wichtige Rolle bei der Bildung der öffentlichen Meinung, politischer Überzeugungen und des sozialen Verhaltens. Gleichzeitig sind diese Plattformen jedoch auch ein Raum für die Verbreitung von Desinformation, Fake News und Manipulationen geworden, was schwerwiegende Folgen für Gesellschaft und Staat hat.

Einer der Hauptansätze zur Bekämpfung von Manipulationen ist die rechtliche Regulierung der Aktivitäten digitaler Plattformen und die Einführung von Maßnahmen gegen Fake News. In vielen Ländern entwickeln Regierungen Gesetze und Vorschriften, um die Verbreitung falscher Informationen im Internet zu verhindern.

Neben legislativen Maßnahmen spielen Technologieunternehmen, die soziale Netzwerke betreiben, eine wichtige Rolle. Führende Technologiekonzerne wie Facebook, Twitter und Google sind verpflichtet, eigene Strategien zur Bekämpfung von Desinformation umzusetzen. Dabei setzen sie automatisierte Systeme ein, um Fake News, Bots und Desinformationskampagnen zu erkennen.

Ein weiterer zentraler Bestandteil der Bekämpfung von Manipulationen ist die Erhöhung der digitalen Kompetenz der Bevölkerung. Die Schulung von Nutzern, wie sie Fake News erkennen und Informationen im Internet kritisch bewerten können, ist ein wichtiger Schutzmechanismus gegen Manipulationen. Viele Länder führen Bildungsprogramme ein, die darauf abzielen, die Öffentlichkeit über Desinformation und digitale Sicherheit aufzuklären. Darüber hinaus unterstützen internationale Organisationen wie die UNO und die EU aktiv Initiativen zur Förderung der digitalen Kompetenz auf globaler Ebene.