КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.685
УДК 342.738:004.056.5:004.738.5

Ткаченко Олександр Сергійович
асистент кафедри кібербезпеки та програмного забезпечення
Центрально український національний технічний університет,
Кропивницький, Україна
аспірант кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0009-0008-1721-3455
alexsunnik@gmail.com

Ільєнко Анна Вадимівна
кандидат технічних наук, доцент, завідувач кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0001-8565-1117
anna.ilienko@npp.nau.edu.ua

Улічев Олександр Сергійович
к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0003-3736-9613
askin79@gmail.com

Мелешко Єлизавета Владиславівна
д.т.н., професор, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-8791-0063
elismeleshko@gmail.com

Смірнов Олексій Анатолійович
д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

ПРАВОВІ ЗАСАДИ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація. У даній роботі досліджуються правові аспекти регулювання інформаційних впливів у соціальних мережах, що набувають особливого значення в умовах сучасних цифрових викликів. Автори розглядають міжнародне та національне законодавство, зокрема нормативні акти Європейського Союзу, США, Китаю та Австралії, аналізуючи підходи різних країн до контролю інформаційних потоків, забезпечення свободи слова, захисту даних користувачів та відповідальності онлайн-платформ. Стаття підкреслює важливість збалансованої правової системи, яка сприяла б збереженню демократичних свобод і водночас забезпечувала інформаційну безпеку, захищаючи вразливі групи населення, зокрема дітей. Ідеальна правова система повинна включати заходи з контролю дезінформації, забезпечення прозорості політичної реклами, захисту персональних даних та відповідальності соціальних платформ. Особлива увага має бути зосереджена на захисті вразливих груп, таких як діти, та на боротьбі з мовою ненависті. Комплексний підхід, що передбачає поєднання законодавчих змін, просвітницьких заходів та співпраці з технологічними компаніями, є необхідним для створення безпечного онлайн-середовища. Висновки авторів підтверджують необхідність постійної адаптації законодавства до швидко змінюваних умов інформаційного середовища. Рекомендується впроваджувати ефективні правові заходи для протидії інформаційним загрозам

© О.С. Ткаченко, А.В. Ільєнко, О.С. Улічев, Є.В. Мелешко, О.А. Смірнов, 2024

і дезінформації, а також забезпечувати міжнародну співпрацю для узгодження правових стандартів. Перспективним є вивчення методів підвищення прозорості алгоритмів, що формують інформаційний простір користувачів, задля зменшення їхнього впливу на сприйняття інформації та поведінку. Подальші дослідження мають на меті оцінку ефективності існуючих правових норм та розробку стратегій їх адаптації у різних соціокультурних контекстах.

Ключові слова: соціальні мережі; інформаційний вплив; правове регулювання; дезінформація; кібербезпека; захист даних; свобода слова; відповідальність платформ; міжнародні стандарти; інформаційна безпека.

ВСТУП

Постановка завдання дослідження

Поширення інформаційних впливів у соціальних мережах є важливим і складним процесом, який підлягає різнобічному регулюванню. На сьогодні соціальні мережі виступають як унікальний засіб масової комунікації, що суттєво впливає на формування суспільної думки, політичні процеси, економічні тенденції та багато інших аспектів життя. В умовах стрімкого розвитку технологій та значного зростання активності користувачів у мережах виникає необхідність формування правових засад для контролю та регулювання поширення інформаційних впливів. Це дослідження покликане розглянути правові основи, які регулюють порядок і обмеження щодо інформації, що циркулює в соціальних мережах, враховуючи особливості правових систем різних країн та сучасні тенденції розвитку права в цьому напрямку.

Інформаційний вплив може набувати різних форм, включаючи політичну пропаганду, дезінформацію, маніпулювання суспільною думкою, тощо. Відтак, дослідження розпочинається із визначення основних понять і класифікації інформаційних впливів, що дозволяє встановити загальні правові принципи та механізми регулювання, які вже існують або які необхідно розробити для ефективного контролю. Одним із ключових завдань є аналіз правових актів на міжнародному та національному рівнях, які стосуються питання поширення інформації в цифровому просторі, включаючи, але не обмежуючись, питанням авторського права, прав людини, приватності, свободою вираження та обмеженням на поширення фейкових новин.

На міжнародному рівні організації, такі як Європейський Союз, ООН та Рада Європи, намагаються створити єдині стандарти щодо інформаційної безпеки та захисту прав користувачів у мережі, але водночас визнано різноманітність підходів у різних країнах. Це ускладнює створення глобального законодавства, однак підштовхує окремі країни до розробки власних регуляцій, аби запобігти негативним наслідкам інформаційного впливу.

В Україні регулювання інформаційного простору також набуває актуальності, зокрема в контексті запобігання поширенню дезінформації, забезпечення національної безпеки та захисту інтересів громадян. Важливим аспектом цього є вдосконалення законодавства, яке дозволить більш ефективно регулювати діяльність соціальних мереж.

Постановка проблеми. З огляду на складність, а також на постійну мінливість інформаційного простору, актуальним є розгляд ролі держави в цьому процесі. Як поєднати забезпечення свободи слова з необхідністю контролю та обмеженням на поширення шкідливих інформаційних впливів. Особливу увагу заслуговують питання меж державного втручання у функціонування соціальних мереж, оскільки надмірне регулювання може порушувати права користувачів та обмежувати свободу слова, а

недостатнє — створювати ризики для громадської безпеки. Дослідження включає аналіз правових норм, що регулюють дані питання, та порівняння їх ефективності в різних юрисдикціях.

Аналіз останніх досліджень і публікацій. Дослідження існуючих публікацій згідно теми, виявив що це досить важливе питання, яким дійсно цікавляться науковці. От, наприклад, О.Г. Радзієвська у 2017 році досліджувала правові засади та механізми протидії негативним інформаційним впливам, зокрема на дітей. Вона акцентує увагу на регулюванні інформаційного середовища та необхідності розробки правових механізмів для захисту дитячої свідомості від інформаційної агресії в соціальних мережах [18]. А В. Я. Новицький у 2022 році у роботі «Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах» розглядає технології впливу на користувачів соціальних мереж та відповідні правові заходи для реагування на гібридні загрози. Дослідник пропонує розробку нових нормативно-правових актів для забезпечення національної інформаційної безпеки [19]. А. Правдюк у статті 2023 року «Астротурфінг в соціальних мережах як загроза демократичному державотворенню» аналізує механізми маніпулятивного впливу та правові аспекти, пов’язані із захистом суспільства від інформаційних війн, що є особливо актуальним в умовах активного використання соціальних мереж [20]. Р. Черниш у 2019 році розглядав досвід країн Європейського Союзу у боротьбі з поширенням фейкової інформації, акцентуючи увагу на законодавчих та нормативних аспектах, спрямованих на запобігання дезінформації в соціальних мережах. Важливою частиною дослідження є аналіз правових інструментів протидії [21].

Мета статті. Розробити набір рекомендацій для удосконалення правового регулювання щодо законодавчих змін для національного регулювання, який забезпечить баланс між свободою слова та захистом громадської безпеки і національних інтересів з урахуванням як національних особливостей, так і міжнародних стандартів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У сучасному суспільстві, яке Д. Белл, Е. Тоффлер, Г. Кан, А. Турен та інші філософи називають «інформаційним» або «постіндустріальним», все більше ваги отримує такий ресурс, як інформація [1]. Інформація стає глобальною, отримує самоцінність та стає індикатором економічного, соціального та технологічного рівня розвитку суспільства. Всі звичні речі, такі як спілкування, обмін новинами, навчання і навіть воєнні дії дедалі більше перетікають в інформаційно-кібернетичний простір. Інформація стає зброєю, інструментом, за допомогою якого можна впливати на думки спільнот та спонукати людей, які є ціллю інформаційного впливу, до потрібних дій. Проте всі інформаційні впливи мають регулюватися: не можна так просто знехтувати використанням найціннішого ресурсу сьогодення. Тож розглянемо правові засади та аспекти застосування інформаційних впливів.

Міжнародна нормативно-правова база

Правові засади поширення інформаційних впливів у соціальних мережах наразі формуються на перетині міжнародного права, національних законів і стандартів, що регулюють свободу слова, інформаційну безпеку, приватність та боротьбу з дезінформацією. Кожна країна підходить до цього питання по-різному, проте існує кілька спільних доктрин та міжнародних стандартів, які створюють основу для

регулювання соціальних медіа. Розглянемо їх докладніше. По-перше це «Загальна Декларація прав людини», що прийнята і проголошена резолюцією 217 А (ІІІ) Генеральної Асамблеї ООН від 10 грудня 1948 року [2]. У статті 19 цієї Декларації вказано, що кожна людина має право на свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів. Це створює певний правовий базис свободи слова при користуванні соціальними мережами. Проте ця сама свобода може бути обмежена для захисту національної безпеки, суспільного порядку та інших інтересів що в свою чергу суперечить статті 30 Загальної Декларація прав людини, у якій зазначено що ніщо у Декларації не може бути витлумачено як надання будь-якій державі, групі осіб або окремим особам права займатися будь-якою діяльністю або вчиняти дії, спрямовані на знищення прав і свобод, викладених у цій Декларації, тому що в такому разі порушується право людини на свободу шукати, одержувати і поширювати інформацію зі статті 19.

Іншим, але не менш важливим, документом є «Міжнародний пакт про громадянські і політичні права» ратифікований 19 жовтня 1973 року [3]. У пункті 2 статті 19 цього пакту вказано, що «Кожна людина має право на вільне вираження свого погляду; це право включає свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір.» Цей пункт в основних тезисах перегукується із статтею 19 Загальної Декларації прав людини, яку було розглянуто вище. Але в Міжнародному пакті про громадянські і політичні права є ще пункт 3 статті 19, в якому зазначено, що «Користування передбаченими в пункті 2 цієї статті правами накладає особливі обов'язки і особливу відповідальність. Воно може бути, отже, пов'язане з певними обмеженнями, які, однак, мають встановлюватися законом і бути необхідними: a) для поважання прав і репутації інших осіб; b) для охорони державної безпеки, громадського порядку, здоров'я чи моральності населення». З цього пункту видно, що за 25 років, що минули з прийняття у 1948 році Загальної Декларація прав людини, змінилося і ставлення до поширювання інформації. На розповсюджувачів інформації окрім прав накладаються ще й зобов'язання та додаткова відповідальність. Інформація почала сприйматись як загроза правам та/або репутації інших осіб, та, що ще важливіше, як загроза державної безпеки, громадському порядку, здоров'ю чи моральності населення. Всі ці важливі доповнення, порівняно зі статтею 19 Загальної Декларації прав людини, вже надають підґрунтя для діяльності органів безпеки, та інших установ, що займаються безпекою інформаційно-кібернетичного простору. Під діяльністю може бути обмеження як доступу осіб до певної інформації так і самої інформації, що загрожує безпеці держави.

Ще одним міжнародним документом є Резолюція A/HRC/RES/49/21 «Роль держав у боротьбі з негативним впливом дезінформації на здійснення та реалізацію прав людини», ухвалена Радою з прав людини 1 квітня 2022 року [4]. Ця резолюція визнає, що дезінформація може негативно впливати на права людини, і підкреслює ключову роль держав у боротьбі з нею. Держави повинні забезпечити, щоб їхні заходи протидії дезінформації відповідали міжнародним нормам із прав людини, сприяли свободі вираження та праву на доступ до інформації. Державам рекомендується впроваджувати багатосторонні стратегії, співпрацюючи з міжнародними організаціями, медіа, приватним сектором та іншими зацікавленими сторонами. Особлива увага приділяється заохоченню компаній, зокрема соціальних мереж, до боротьби з дезінформацією, забезпечуючи прозорість та відповідність алгоритмів при збереженні поваги до прав людини. Держави також повинні утримуватися від організації або спонсорування

кампаній дезінформації та засуджувати подібні дії. Важливим є підтримання міжнародного співробітництва для боротьби з дезінформацією, включаючи організацію дискусій на високому рівні, щоб обговорити негативний вплив дезінформації та заходи протидії.

Регіональна нормативно-правова база

Із загальносвітових міжнародних стандартів перейдемо до більш локальних — розглянемо «Загальний регламент про захист даних (GDPR)» який діє по зоні Євросоюзу та набрав чинності 25 травня 2018 року [5]. Цей регламент, як і розглянуті вище нормативні документи, забезпечує по-перше — це прозорість інформації, та вільність її розповсюдження. І по-друге це захист даних при використанні соціальних мереж. Він регулює збір, обробку та поширення персональної інформації в цифровому просторі, включаючи соціальні мережі. Цей Регламент не застосовують до опрацювання персональних даних фізичною особою у ході суто особистої або побутової діяльності, а, отже, жодним чином не пов'язаної з професійною або комерційною діяльністю. Особисту або побутову діяльність може становити ведення кореспонденції та зберігання адрес, або ведення соціальних мереж і онлайн-діяльності, розпочатої у контексті такої діяльності. Проте цей Регламент застосовують до контролерів і операторів, які надають засоби для опрацювання персональних даних для такої особистої або побутової діяльності. За порушення передбачено значні штрафи, що стимулює платформи захищати приватність користувачів.

Ще одним нормативно-правовим документом є «Кодекс практики ЄС щодо дезінформації» [6]. Цей кодекс вперше був прийнятий у 2018, після декількох років обговорень та пропозицій, адже до цього проблема цифрової дезінформації не стояла так гостро. Проте науково-технічний прогрес не стоїть на місці, і з'являються нові способи поширення дезінформації. І таким чином, вже у 2022 році, тобто через 4 роки після першого прийняття, вийшла посилена редакція, у якій кодекс був значно оновлений. Учасниками кодексу є відомі компанії, технологічні платформи та соцмережі: Adobe, Google, Meta (Facebook, Instagram, Threads), Microsoft, TikTok, Twitch, Twitter, які зобов'язуються підвищувати прозорість реклами, зменшувати вплив фейкових акаунтів та ботів.

Із положень варто відзначити повну демонетизацію поширення дезінформації, тобто постачальники дезінформації не отримують фінансової вигоди з доходів від реклами. Також посилений Кодекс зобов'язує сторони, які його підписали, ввести більш суворі заходи прозорості, і в першу чергу прозорості політичної реклами. Це і більш ефективне маркування, щоб користувач одразу бачив, що перед ним рекламний пост, і зобов'язання розкривати спонсора, який замов рекламу та витрати на цю рекламу, а також період показу цієї реклами. Всі ці пункти дозволяють користувачам легко розпізнавати наприклад політичну рекламу. Крім того, ті, хто підписали, зобов'язуються створити ефективні бібліотеки оголошень з можливістю пошуку для політичної реклами. Користувачі будуть краще захищені від дезінформації завдяки вдосконаленим інструментам для розпізнавання, розуміння та маркування дезінформації, доступу до авторитетних джерел та ініціатив щодо підвищення медіаграмотності [7]. Також цим кодексом гарантується посилення співпраці з фактчекерами, надання дослідникам кращого доступу до даних та більш кращі системи моніторингу. Що зумовлює більш точну перевірку фактів на їх достовірність, а відповідно і отримання користувачами більш вірогідно правдивої інформації.

Варто згадати директиву ЄС про електронну комерцію, прийняту 08 червня 2000 [8], проте в майже в усіх пунктах досі не втратила своєї актуальності. Ця директива регулює діяльність інтернет-платформ, включно із соціальними мережами, та здебільшого стосується комерційної діяльності, проте вона містить також статті та положення про інформацію та її передачу через мережу Інтернет. Директива про електронну комерцію закликає відповідні платформи до певної відповідальності за контент, який вони розміщують або модерацію якого здійснюють.

Це основні нормативно-правові акти, що стосуються поширення інформаційних впливів та діяльності соціальних мереж в зоні Євросоюзу.

Локальна нормативно-правова база

Далі починають діяти вже регіональні постанови та закони. Застосування інформаційних впливів у соціальних мережах в Україні регулюється комплексом законів, спрямованих на баланс між свободою слова, захистом національної безпеки та правами громадян. Одним із ключових документів є Конституція України [9], яка гарантує свободу вираження думки, проте встановлює можливі обмеження для захисту інтересів суспільства, зокрема національної безпеки, громадського порядку та прав інших осіб. Це створює правове підґрунтя для втручання держави в інформаційну сферу, включно із соціальними мережами, у разі загрози важливим суспільним та державним інтересам.

Наступним йде Закон України «Про інформацію» [10]. Він надає додаткову регуляцію діяльності у сфері поширення інформації. Він забезпечує свободу інформаційної діяльності, але також запроваджує відповідальність за дезінформацію та неправдиві повідомлення, які можуть завдати шкоди державі або громадськості. Цей закон стає особливо важливим у контексті боротьби з маніпуляціями та інформаційними атаками в соціальних мережах, де швидкість поширення контенту останнім часом значно випереджає можливості перевірки цього контенту.

Закон України «Про захист персональних даних» [11] стосується безпеки особистої інформації, що є особливо актуальним в умовах цифрової комунікації. Соціальні мережі накопичують величезні обсяги персональних даних, і цей закон гарантує, що такі дані обробляються відповідно до законодавства, а також передбачає санкції за порушення конфіденційності.

Важливу роль у захисті національної безпеки в умовах інформаційних впливів відіграє Закон України «Про основи національної безпеки України» [12], який визначає інформаційну безпеку як одну з ключових складових національної безпеки. Це дозволяє державі втручатися в діяльність, пов’язану з дестабілізацією суспільства через соціальні мережі, зокрема під час гібридних загроз і війни.

Закон України «Про медіа» [13] надає певні розуміння стосовно сектору медіа та діяльності окремих його суб’єктів. Він забезпечує реалізацію права на свободу вираження поглядів та права на отримання правдивої та актуальної інформації, забезпечує плюралізм думок і вільне поширення інформації. А також, що важливо, гарантує захист національних інтересів України та прав користувачів медіа-сервісів. Це все ґрунтується на принципах прозорості, справедливості та неупередженості, стимулює конкурентне середовище, рівноправність і незалежність медіа.

Далі розглянемо Закон України «Про основні засади забезпечення кібербезпеки України» [14]. Він описує регуляторні механізми, що стосуються онлайн-платформ. Зокрема, ці механізми передбачають відповідальність за поширення фейкових новин, пропаганди та закликів до насильства, що є прямими загрозами в соціальних мережах.

Це відображає світову тенденцію до більш жорсткого контролю інформаційних потоків у цифровому середовищі.

На додаток до цього, положення Кримінального кодексу України [15] передбачають кримінальну відповідальність за діяльність, яка може порушувати інформаційну безпеку держави або підривати суспільний лад, а також стосується передачі та розповсюдження конфіденційної або незаконної інформації через інформаційно-телекомунікаційні системи, Інтернет та зокрема через соціальні мережі.

Аналізуючи законодавчу базу, можна зробити висновок, що Україна намагається створити збалансовану систему регуляції інформаційного простору, що враховує як потреби безпеки держави, так і права громадян на свободу слова. В умовах сучасних гібридних загроз, соціальні мережі стають важливим інструментом як для дестабілізації, так і для захисту, що вимагає постійного вдосконалення законодавства та посилення контролю за інформаційними потоками. Однак, важливо, щоб ці заходи не порушували основоположних прав і свобод громадян, що потребує збалансованого підходу між забезпеченням безпеки та захистом демократичних цінностей.

Цифрові та технічні засоби

Тепер перейдемо від правових документів до цифрових і технічних засобів які вже реалізовані згідно цим документам.

Першою можна зазначити сумісну ініціативу ЄС та України «Нації проти дезінформації» [16]. Ця ініціатива навіть вводить нове поняття — інфодемія, утворене від слів інформаційна пандемія, і означає загрозу дезінформацією, яка може мати наслідки на кшталт епідемії, масової хвороби через неправдиву інформацію, яка впливає на підсвідомість та змінює поведінку та лояльність людей. «Нації проти дезінформації» — це міжнародний рух, який об’єднує країни та людей у боротьбі з цією самою інфодемією. Для боротьби з цією загрозою пропонується використовувати такі «ліки», як сервіси-фактчекінги (Detector Media, STOPFAKE), сервіси-правдомовці (We Are Ukraine, UkraineWorld) та ресурси протидії дезінформації (SPRAVDI, PutinLies, PROPASTOP).

Із дещо локального цифрового засобу перейдемо до більш глобальних. Так, інтеренет-платформи, такі як Facebook, Google та Twitter, співпрацюють із міжнародними організаціями для розробки стандартів і методів боротьби з дезінформацією. Як один із результатів цієї співпраці можна зазначити створення у 2015 році ініціативи перевірки фактів International Fact-Checking Network (IFCN) — Міжнародну Мережу Перевірки Фактів. Ця мережа створена для того, щоб об’єднати зростаючу спільноту перевіряючих фактів у всьому світі. Мережа виступає за цілісність інформації в глобальній боротьбі з дезінформацією та підтримує тих, хто перевіряє факти, через створення мереж, розбудову потенціалу та співпрацю, допомагає створювати інструменти та стандарти для перевірки фактів на міжнародному рівні [17].

Також, варто згадати Global Network Initiative (GNI) [18] — Глобальну Ініціативу Інтернету, неурядову організацію, що захищає свободу вираження та приватність в Інтернеті, протидіючи цензурі з боку авторитарних урядів. Заснована 29 жовтня 2008 року, вона об’єднує корпорації, некомерційні організації та академічні інститути. GNI базується на міжнародних правах людини та співпрацює з учасниками для забезпечення дотримання цих принципів. Учасники, зокрема Meta, Google, Microsoft і Yahoo, зобов’язані захищати права користувачів, дотримуючись міжнародних стандартів. Організація також отримує фінансування від урядів і приватних фондів.

Правове регулювання в окремих країнах

Розглянемо стандарти деяких країн, які можуть бути джерелами для актуальних рішень у сфері інформаційних впливів в соціальних мережах.

Однією з перших країн у контексті правового регулювання інформації в соціальних мережах є США, де Перша поправка до Конституції [23] гарантує свободу слова і свободу преси. Ці принципи значно впливають на законодавчі основи функціонування соціальних медіа, забезпечуючи право громадян висловлюватися без надмірного втручання. Водночас у США існують закони, які встановлюють певні обмеження. Наприклад, закон 18 U.S.C. § 875(c) [28] обмежує поширення мови ненависті в мережі, тоді як 18 U.S.C. § 373 [29] і рішення у справі *Brandenburg v. Ohio* [30] дозволяють заборонити висловлювання, що закликають до неминучого насильства. Закони про захист дітей в Інтернеті, зокрема Communications Decency Act (CDA) [31] і Children's Online Privacy Protection Act (COPPA) [32], також відіграють важливу роль у регулюванні шкідливого контенту для дітей, дозволяючи платформам видаляти небезпечні матеріали й захищати особисті дані неповнолітніх.

Одним із важливих законопроєктів у США є Закон про чесність реклами в Інтернеті (Honest Ads Act) [24]. Цей документ зобов'язує соціальні медіа компанії розкривати інформацію про рекламодавців політичної реклами, що спрямоване на протидію втручанню у вибори та забезпечення прозорості інформаційних кампаній. Важливе місце в регулюванні соціальних мереж посідає також розділ 230 Закону про захист комунікацій (Section 230 of the Communications Decency Act) [25], який надає платформам захист від відповідальності за контент, що створюють користувачі. Він дозволяє соціальним медіа здійснювати модерацію, але залишається предметом активних дискусій через його можливий вплив на свободу слова та обов'язки платформ.

Наступною державою розглянемо Китай та саме закон про кібербезпеку [26]. Це один із найсуворіших у світі законів про кібербезпеку, який значною мірою впливає на регулювання соціальних мереж. Прийнятий у 2017 році, Закон про кібербезпеку зобов'язує всі компанії зберігати дані користувачів на серверах, розташованих в Китаї, що дозволяє уряду мати безпосередній доступ до інформації та контролювати діяльність соціальних медіа. Основна мета цього закону полягає у забезпеченні інформаційної безпеки та захисті державної стабільності, що досягається через суворе регулювання та моніторинг контенту. Китайський уряд активно бореться з будь-якою інформацією, яку вважає загрозливою для національної безпеки чи соціального порядку, зокрема, це стосується закликів до протестів, поширення «чуток» і політично чутливого контенту. Законодавство надає уряду широкі повноваження для втручання в діяльність платформ, зобов'язуючи їх посилено контролювати публікації та швидко реагувати на виявлення забороненого контенту. У випадку порушення цього закону на компанії можуть бути накладені значні штрафи, їх діяльність може бути призупинено, а для осіб, відповідальних за регулювання інформаційного середовища, передбачена кримінальна відповідальність. Таким чином, закон створює основу для безпрецедентного контролю над інформаційним середовищем, спрямованого на підтримку стабільності та безпеки держави.

В Австралії також діє суворе законодавство щодо регулювання контенту в Інтернеті. Закон про онлайн-безпеку (Online Safety Act) [25], ухвалений у 2021 році, зобов'язує соціальні медіа компанії оперативно видаляти шкідливий контент, включаючи мову ненависті, погрози, а також порнографічні матеріали. На вимогу австралійської влади компанії мають 24 години для видалення такого контенту, інакше на них можуть бути накладені великі штрафи. Цей закон є частиною політики уряду,

спрямованої на забезпечення безпечного онлайн-середовища для громадян, зокрема дітей та вразливих груп населення. Законодавчі заходи підтримуються спеціальною службою, призначеною для відстеження порушень і виявлення контенту, що становить загрозу для безпеки та благополуччя користувачів. Закон про онлайн-безпеку є важливим кроком у запобіганні поширенню шкідливих матеріалів і зміцненні захисту користувачів від негативного інформаційного впливу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На основі отриманої інформації створимо порівняльну таблицю, що аналізує чинні законодавства у сфері інформаційних впливів у соціальних мережах для Євросоюзу, України, США, Китаю та Австралії за десятьма критеріями. Оцінимо кожний критерій від 1 до 5, де 1 — найнижча оцінка, тобто невідповідність обраному критерію, а 5 — найвища, повна відповідність обраному критерію.

Розглянемо кожний критерій окремо з поясненнями. Першим критерієм розглянемо захист свободи слова. США (5 балів) залишаються лідером у питанні захисту свободи слова завдяки Першій поправці до Конституції, яка гарантує право на вільне висловлювання та обмежує втручання держави, зокрема в діяльність соцмереж (5 балів). В Україні (4 бали) та Євросоюзі (4 бали) свобода слова також захищена законодавчо, але в обох випадках можуть застосовуватися обмеження для захисту громадської безпеки та запобігання поширенню шкідливої інформації. Австралія (4 бали) підтримує свободу слова, але законодавчі заходи там є більш жорсткими порівняно з США. У Китаї (1 бал) свобода слова суттєво обмежена — уряд контролює поширення інформації та забороняє будь-який контент, який може загрожувати суспільній стабільності чи критикувати владу.

Наступним буде контроль за дезінформацією. Китай (5 балів) має потужний контроль над дезінформацією, активно регулюючи всі інформаційні потоки та застосовуючи цензуру для припинення поширення неправдивих даних. Євросоюз (4 бали) також має високий рівень контролю над дезінформацією, розробляючи єдину стратегію протидії фейкам і створюючи механізми перевірки фактів. Австралія (4 бали) також активно діє у цьому напрямі, зобов’язуючи платформи швидко реагувати на дезінформацію. В Україні (3 бали) прийняті закони для боротьби з дезінформацією, але їхня ефективність обмежена. У США (3 бали) обмежений контроль з боку уряду, соцмережі регулюють дезінформацію самостійно, використовуючи надані державою платформи для боротьби з дезінформацією, зберігаючи основи свободи слова.

Потім розглянемо вимоги до видалення шкідливого контенту. У США (4 бали) CDA Section 230 захищає соцмережі від відповідальності за контент, але вони мають право видаляти шкідливий контент. У Китаї (5 балів) суворі вимоги до видалення контенту, що суперечить офіційним позиціям уряду. В Австралії (5 балів) закон про онлайн-безпеку зобов’язує видаляти шкідливий контент за 24 години. В іншому випадку передбачені значні штрафи для соціальних мереж, які не видаляють шкідливий контент вчасно. В Україні (4 бали) вимоги до видалення є, однак законодавчо вони ще не повністю сформовані й можуть бути менш жорсткими адже механізми їх виконання не завжди чіткі. У Євросоюзі (5 балів) регламент зобов’язує швидке видалення нелегального та шкідливого контенту.

Після цього розглянемо прозорість політичної реклами. У США (4 бали) закон про чесність реклами вимагає розкриття інформації про політичних рекламодавців. У Китаї

(1 бал) політична реклама контролюється державою, прозорість не забезпечується. В Австралії (5 балів) суворі вимоги щодо прозорості політичної реклами в соцмережах. В Україні (3 бали) законодавство з прозорості політичної реклами ще розвивається. У Євросоюзі (4 бали) директиви ЄС вимагають прозорості для політичної реклами.

Наступним розглянемо захист даних користувачів. У Євросоюзі (5 балів) GDPR є найсуворішим регламентом захисту даних для компаній у світі. У Китаї (5 балів) суворі вимоги до захисту даних, особливо через закон про кібербезпеку. В Австралії (4 бали) діють закони, схожі на GDPR, але на менш жорсткому рівні порівняно з Євросоюзом, є зобов'язання повідомляти про витоки. В Україні (3 бали) та США (3 бали) діють загальні закони про захист даних, але вони менш детальні та регулювання менш суворе, ніж у ЄС.

Відповідальність платформ іде наступною. У всіх п'яти країнах платформи несуть певну відповідальність за контент. У США (3 бали) CDA Section 230 забезпечує соцмережам частковий захист, але вони відповідають за модерацію. У Китаї (4 бали) платформи несуть відповідальність за контент, що суперечить політиці уряду. В Австралії (4 бали) платформи зобов'язані видаляти шкідливий контент. В Україні (3 бали) відповідальність платформ не чітко визначена, що дає платформам певну свободу дій. У Євросоюзі (4 бали) директиви встановлюють відповідальність за невчасне видалення нелегального контенту.

Далі розглянемо вимоги до зберігання даних. Китай (5 балів) запровадив суворі вимоги щодо зберігання даних, зобов'язуючи компанії зберігати дані на локальних серверах. У США (2 бали) законодавство не зобов'язує зберігати дані в країні, але деякі правила існують. В Австралії (3 бали) вимоги є, але вони менш суворі, ніж у Китаї чи ЄС. В Україні (2 бали) зберігання даних регулюється, але немає суворих вимог до розміщення. Євросоюз (4 бали) має структуроване регулювання через GDPR, яке вимагає забезпечення високого рівня безпеки даних користувачів.

Після цього розглянемо запобігання мові ненависті. У США (4 бали) закони забороняють мову ненависті, але з великим акцентом на свободу слова. У Китаї (2 бали) відсутні практики боротьби з мовою ненависті, оскільки основна увага приділяється контролю за загрозами державній стабільності, що проводиться під контролем держави. В Австралії (4 бали) чіткі вимоги щодо видалення мови ненависті. В Україні (3 бали) існують закони для боротьби з мовою ненависті, але вони менш суворі. У Євросоюзі (4 бали) країни ЄС активно борються з мовою ненависті відповідно до директив.

Вплив на дітей є теж важливим аспектом, тому розглянемо і цей критерій.

Австралія (5 балів) є лідером за заходами для захисту дітей від шкідливого контенту в соцмережах, зобов'язуючи платформи швидко видаляти небезпечний матеріал. У США (3 бали) COPPA захищає дітей, але є певні обмеження. У Китаї (2 бали) вимоги до захисту дітей менш жорсткі, певний контроль існує, однак фокус зміщено на збереження стабільності. В Україні (3 бали) є закони, але захист менш структурований. У Євросоюзі (4 бали) GDPR і директиви зобов'язують платформи захищати дітей.

І останнім критерієм розглянемо гнучкість у застосуванні законів.

У США (4 бали) підхід залишається гнучким, зокрема для приватного регулювання платформ. У Китаї (1 бал) закони застосовуються строго, з мінімальною гнучкістю. В Австралії (4 бали) закони передбачають гнучкість, але контроль залишається високим. В Україні (3 бали) гнучкість залежить від ситуації, зокрема національної безпеки. У Євросоюзі (4 бали) ЄС залишає гнучкість країнам-членам, але основні директиви жорстко застосовуються.

Зібрані оцінки розмістимо в табл. 1.

ISSN 2663 - 4023

Таблиця 1

Порівняння законодавств різних країн у сфері інформаційного впливу в соціальних мережах

Критерії	Євросоюз	Україна	США	Китай	Австралія
1. Захист свободи слова	4	4	5	1	4
2. Контроль за дезінформацією	4	3	3	5	4
3. Вимоги до видалення шкідливого контенту	5	4	4	5	5
4. Прозорість політичної реклами	4	3	4	1	5
5. Захист даних користувачів	5	3	3	5	4
6. Відповідальність платформ	4	3	3	4	4
7. Вимоги до зберігання даних	4	2	2	5	3
8. Запобігання мові ненависті	4	3	4	2	4
9. Вплив на дітей	4	3	3	2	5
10. Гнучкість у застосуванні законів	4	3	4	1	4

На основі табл. 1 намалюємо пелюсткову діаграму (рис. 1).

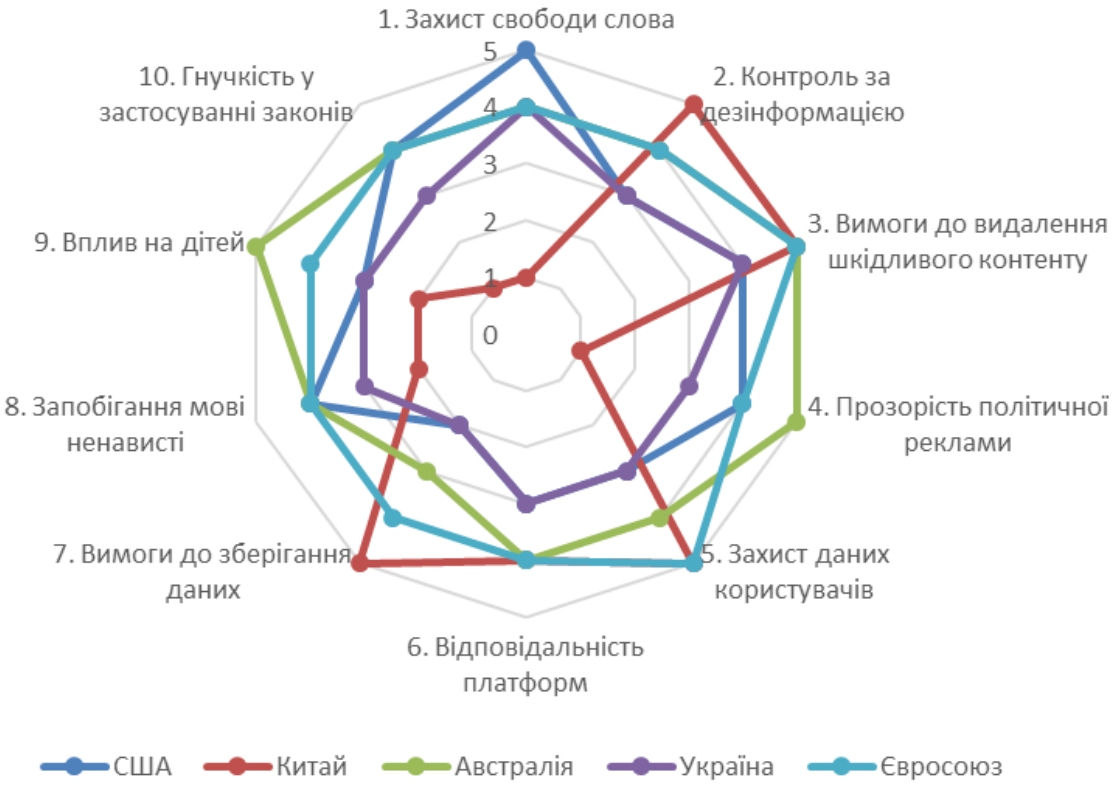

Рис. 1. Діаграма порівняння законодавств різних країн у сфері інформаційного впливу в соціальних мережах

З отриманої діаграми чітко видно сильне відхилення від норми (тобто п'ятибального, майже кола) у Китаю. Середньозважені позиції України, які ближчі за формою до кола, але не максимально можливого. І майже ідеальні «кола» у США, Євросоюзу та Австралії законодавство яких, у деяких аспектах, виявляється ідеальним.

У табл. 2 відобразимо розроблені рекомендації для законодавства у сфері регулювання інформаційних впливів у соціальних мережах за 10 критеріями, де кожен параметр оцінено на максимально можливий рівень (тобто на 5). Таке законодавство надає оптимальний баланс між захистом свободи слова, безпекою користувачів, відповідальністю платформ і захистом даних, одночасно забезпечуючи гнучкість у застосуванні законів.

Таблиця 2

Набір рекомендацій для законодавства у сфері інформаційних впливів в соцмережах

Критерії	Ідеальна структура
1. Захист свободи слова	5 (Свобода слова захищена на найвищому рівні, обмеження застосовуються лише у випадках мови ненависті, закликів до насильства та інших шкідливих проявів, що становлять загрозу громадській безпеці [21], [38])
2. Контроль за дезінформацією	5 (Ефективна система виявлення, перевірки та протидії дезінформації, що не обмежує свободу висловлювань, але спрямована на припинення свідомо неправдивих або маніпулятивних повідомлень [39], [40])
3. Вимоги до видалення шкідливого контенту	5 (Швидка й чітка процедура видалення шкідливого контенту, яка зобов'язує платформи реагувати оперативно на порушення, особливо щодо мови ненависті та насильницького контенту [41], [42])
4. Прозорість політичної реклами	5 (Всі платформи повинні розкривати інформацію про рекламодавців і джерела фінансування політичної реклами з метою запобігання зовнішньому втручанню та прозорості виборчого процесу [43], [44])
5. Захист даних користувачів	5 (Суворий захист даних користувачів, забезпечений відповідними нормами, що вимагають надання доступу до даних лише за згодою користувача або за суворо визначених законодавчих підстав [45], [46])
6. Відповідальність платформ	5 (Платформи мають юридичну відповідальність за контент, але законодавчо підтримути модерацію контенту, що дозволяє оперативно реагувати на порушення [47], [48])
7. Вимоги до зберігання даних	5 (Дані повинні зберігатися на захищених серверах з обмеженим доступом та з урахуванням місцевого законодавства, але також передбачено інструменти для транснаціональної передачі даних при дотриманні всіх вимог захисту [49], [50])
8. Запобігання мові ненависті	5 (Ретельний контроль мови ненависті з чіткими визначеннями і вимогами, що не обмежують легітимну свободу слова, але захищають вразливі групи від образ та загроз [51], [52])
9. Вплив на дітей	5 (Суворі правила для захисту дітей від шкідливого контенту, включаючи вікові обмеження, модерацію та активне відстеження контенту, що може негативно вплинути на дітей [33] – [37])
10. Гнучкість у застосуванні законів	5 (Закони застосовуються з гнучкістю, що дозволяє адаптацію до мінливих умов, підтримуючи баланс між свободою слова та відповідальністю за шкідливий контент, особливо в кризових ситуаціях [53] – [55])

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Кількість загроз у кіберпросторі постійно зростає, і те, що сьогодні вважається захищеним та актуальним може втратити свою актуальність дуже швидко, майже за лічені хвилини. А, враховуючи те, що в сучасному світі дуже важко уявити людину без смартфону та як наслідок без соцмереж. Адже в останній час вони стали і джерелом новин (оперативних та швидких порівняно із традиційними ЗМІ), і місцем розваг та дозвілля, і, звичайно, місцем спілкування, як і замислювалися зі своєї появи.

Дивлячись на отримані результати по країнам, можна стверджувати що серед передових та високорозвинених (більшість країн середньої Африки та деякі країни південного сходу не розглядаються адже в цих країнах недостатньо розвинений кіберпростір взагалі) країн світу немає, на момент дослідження, 100% ідеальної країни в розрізі інформаційних впливів в соціальних мережах. Адже всюди є люди. Деяким потрібно щось приховати — виникає неправда або навіть дезінформація. Інші поводять себе дуже агресивно в соцмережах, ховаючись за екраном, і не бояться того що їх співрозмовник «фізично» відповість на агресію. А те, що діти зі смартфоном майже з дитинства, проте не завжди є якийсь контроль над тим, який контент вони споживають та як він вплине на їх, ще не сформовану, дитячу психіку.

Результати дослідження підкреслюють необхідність створення всеосяжної правової системи для регулювання інформаційних впливів у соціальних мережах, що дозволяє збалансувати захист свободи слова з безпекою користувачів. Ідеальна правова структура повинна включати чіткі критерії для контролю дезінформації, забезпечення прозорості політичної реклами, захист даних користувачів та відповідальність платформ. Важливими елементами для створення безпечного онлайн-середовища також є захист вразливих груп, таких як діти, та ефективна протидія мові ненависті. Важливо, щоб будь-яка правова рамка враховувала як захист користувачів від шкідливого впливу так і захист прав користувачів на свободу вираження думки, свободу слова. У цілому, для ефективного вирішення цього питання потрібен комплексний підхід, що включає законодавчі зміни, просвітницьку діяльність та співпрацю з технологічними компаніями. І в умовах мінливості інформаційного середовища, найважливіше для законодавства — це бути актуальним, відповідати поточному рівню розвитку технологій.

Подальші дослідження повинні зосередитися на вивченні адаптації таких законодавчих заходів у різних соціокультурних умовах і аналізі ефективності існуючих законів у боротьбі з інформаційними загрозами. Крім того, з огляду на швидкий розвиток технологій, важливо регулярно оцінювати відповідність законодавства новим викликам у сфері цифрової безпеки та приватності даних. Дослідження методів підвищення прозорості алгоритмів соціальних мереж, які формують інформаційний простір користувачів, є також перспективним для зменшення їхнього впливу на поведінку та сприйняття інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bell, D. (1973). *The Coming of Post-Industrial Society. A Venture in Social Forecasting*.
2. Конвенція про захист прав людини і основоположних свобод, Конвенція Ради Європи (2021). https://zakon.rada.gov.ua/laws/show/995_004#Text
3. Європейська конвенція про права людини (б. д.) https://zakon.rada.gov.ua/laws/show/995_043#Text
4. Організації Об'єднаних Націй. (2022). *Роль держав у протидії негативному впливу дезінформації на здійснення та реалізацію прав людини.* https://documents.un.org/doc/undoc/ltd/g22/296/55/pdf/g2229655.pdf?OpenElement
5. *Загальний регламент захисту даних (GDPR).* (б.д.). https://gdpr-text.com/uk/
6. *The Strengthened Code of Practice on Disinformation 2022.* (2022). https://disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Code-of-Practice-on-Disinformation-2022.pdf
7. *Оновлення Кодексу ЄС щодо боротьби з дезінформацією: основні положення.* (2022). https://jurliga.ligazakon.net/news/212519_onovlennya-kodeksu-s-shchodo-borotbi-z-deznformatsyu-osnovn-polozhennya
8. Конвенція про права дитини, Конвенція Організація Об'єднаних Націй (2023). https://zakon.rada.gov.ua/laws/show/995_021#Text

9. Конституція України, № 254к/96-ВР (2020) (Україна). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
10. Про інформацію, Закон України № 2657-XII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2657-12#Text
11. Про захист персональних даних, Закон України № 2297-VI (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2297-17#Text
12. Про свободу совісті та релігійні організації, Закон України № 987-XII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/987-12#Text
13. Про електронні комунікації, Закон України № 1089-IX (2024) (Україна). https://zakon.rada.gov.ua/laws/show/1089-20#Text
14. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text
15. Про захист суспільної моралі, Закон України № 1296-IV (2023) (Україна). https://zakon.rada.gov.ua/laws/show/1296-15#Text
16. *Nations Against Disinformation Initiative.* (б. д.). NATIONS AGAINST DISIFORMATION INITIATIVE. https://www.nationsagainstdisinformation.org/partners/
17. *International Fact-Checking Network - Poynter.* (б. д.). Poynter. https://www.poynter.org/ifcn/.
18. *Global Network Initiative.* (б. д.). https://globalnetworkinitiative.org
19. Радзієвська, О. Г. (2017). Правові засади та пріоритети розвитку протидії негативним інформаційним впливам на дітей. *Інформація і право, 2(21).* https://doi.org/10.37750/2616-6798.2017.2(21).273045
20. Новицький, В. Я. (2022). Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право, 1(40).* https://doi.org/10.37750/2616-6798.2022.1(40).254349
21. Правдюк, А. (2023). Астротурфінг в соціальних мережах як загроза демократичному державотворенню. *Наукові інновації та передові технології, 1(15),* 154–166. https://doi.org/10.52058/2786-5274-2023-1(15)-154-166
22. Черниш, Р. (2019). Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації. *Інформаційне право*, 123–128. https://doi.org/10.32849/2663-5313/2019.10.21
23. Конституція США, Перша поправка. (б. д.). https://constitution.congress.gov/constitution/amendment-1/#:~:text=Congress%20shall%20make%20no%20law,for%20a%20redress%20of%20grievances
24. The Honest Ads Act. (б. д.). U.S. Senator Mark R. Warner. https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act
25. Department of justice's review of section 230 of the communications decency act of 1996. (б. д.). Department of Justice | Homepage | United States Department of Justice. https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996
26. Про кібербезпеку, Закон (2016) (Китай). https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm
27. Про прозорість цифрових платформ, Законопроект (2021) (Австралія). https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680.
28. Розділ 875 Кодексу США, Загрози, 18 U.S.C. § 875. (б. д.). https://www.law.cornell.edu/uscode/text/18/875
29. Розділ 373 Кодексу США, Підбурювання до вчинення насильства, 18 U.S.C. § 373. (б. д.). https://www.law.cornell.edu/uscode/text/18/373
30. United States v. Reidel, рішення Верховного суду США, 395 U.S. 444 (1969). https://tile.loc.gov/storage-services/service/ll/usrep/usrep395/usrep395444/usrep395444.pdf
31. Законопроект S.314 – Communications Decency Act, 104-й Конгрес США (1995-1996). https://www.congress.gov/bill/104th-congress/senate-bill/314
32. *Children's Online Privacy Protection Rule ("COPPA").* (б. д.). Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
33. Кухарська, Н., & Кухарський, В. (2014). Загрози безпеці дітей у соціальних мережах. *Безпека інформації, 20(2),* 169–175.
34. Юрченко, О. Ю. (2013). Проблеми безпеки дітей в соціальних мережах та Інтернеті (віктимологічний аспект). *Соціально-аналітичне право: електронне фахове видання, 3,* 336–338.
35. Гоцуляк, К. (2015). Вплив соціальних мереж на розвиток особистості молодшого школяра. Гірська школа українських Карпат., 12–13, 152–154.
36. Проніна, О. В. (2023). Вплив соціальних мереж на дітей та підлітків: ризики та правила безпеки. *Освітній менеджмент: успішні практики та виклики,* 82–85.

37. Олійник, К. С. (2018). Загальна характеристика та значення соціальних мереж у житті сучасної молоді. Педагогічні науки: збірник наукових праць, 84(2), 188–191.
38. Дашковська, О. Р. (2019). Захист свободи слова в Інтернет-просторі. *Порівняльно-аналітичне право, 5*, 16–20.
39. Кузьменкова, К. С. (2024). Стратегії боротьби з дезінформацією: Європейський досвід. *Міжнародна науково-практична конференція «Від теорії до практики в управлінні та врядуванні»,* 97–99.
40. Вовчанська, О. М., & Іванова, Л. О. (2021). Ринок соціальних медіа: нові реалії для бізнесу і споживачів. *International scientific and practical conference*, 93–99. https://doi.org/10.30525/978-9934-26-042-1-22
41. Завойовська, О. М. (2024). *Програмний модуль для виявлення образливих слів та ненависті в текстових повідомленнях: кваліфікаційна робота.*
42. Кравчук, В. О. (2024). Поняття інформаційної безпеки у мережі Інтернет. *8-а Міжнародна науково-практична конференція,* 757–763.
43. Кропивко, В. (2022). Політична реклама у публічній комунікації: між державним регулюванням та ринком. *Вісник Львівського університету, 43*, 282–288. https://doi.org/10.30970/PPS.2022.43.34
44. Радіо, М. В. (2023). Державне регулювання передвиборної кампанії у соціальних медіа (сучасна практика іноземних країн). *Політичне життя, 2*, 76–82. https://doi.org/ 10.31558/2519-2949.2023.2.9
45. Гавловський, В. Д. (2011). До питання захисту персональних даних у соціальних мережах. *Боротьба зі злочинністю і корупцією*, *24*, 252–262.
46. Прокопович, Л. В., & Лопаков, О. С. (2021). Шляхи підвищення захисту персональних даних користувачів соціальних мереж. *The Scientific Heritage, 65*, 32–37.
47. Кукіна, Н. В., Савчук, Я. О., & Ляліук, А. М. (2024). Аналіз ролі соціальних мереж у формуванні брендової лояльності. *Актуальні проблеми сучасної науки, 8(278),* 116–128.
48. Маркулинець, А. (2024). Цивільно-правове регулювання соціальної комерції: взаємодія користувачів та брендів. *Наукові інновації та передові технології, 10(38)*, 238–249.
49. Чередніченко, О. Ю., Ткаченко, В. В., & Вовк, М. А. (2018). Дослідження профілів користувачів соціальних мереж. *Збірник наукових праць ХНУ, 2(56)*, 113–119.
50. Щербаков, С., & Хрипко, С. (2024). Поняття великих даних. *Modern Trends in the Development of Scientific Space*, 60–65.
51. Колесник, Г. О. (2021). «Мова ворожнечі» як соціальний та лінгвістичний феномен. Вчені записки Таврійського національного університету, 32(71), 278–283.
52. Сахацька, О. (2023). Технологія навчання підлітків виявлення мови ненависті у медіа і запобігання її поширенню. *Наукові горизонти XXI століття,* 1210–1213.
53. Васильківський, М. В., & Будаш, М. В. (2023). Забезпечення інформаційного захисту в телекомунікаційних мережах 6G. *Науковий вісник ВНТУ.*
54. Карапетян, А. О. (2020). Гнучкість у застосуванні законів у сфері освіти. *Наукові записки ЦДПУ, 186,* 115–120. https://doi.org/10.36550/2415-7988-2020-1-186-115-120
55. Гулак, Г. М., Жильцов, О. Б., Киричок, Р. В., Коршун, Н. В., & Складанний, П. М. (2024). *Інформаційна та кібернетична безпека підприємства.* Підручник. Львів : Видавець Марченко Т. В.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Oleksandr Tkachenko
Assistant of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
PhD student at the Department of Cybersecurity
State University "Kyiv Aviation Institute", Kyiv, Ukrain
ORCID ID: 0009-0008-1721-3455
alexsunnik@gmail.com

Anna Ilyenko
Candidate of Technical Sciences, Associate Professor,
Head of the Cybersecurity Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Oleksandr Ulichev
Candidate of Technical Sciences, Senior Lecturer of
Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0003-3736-9613
askin79@gmail.com

Yelyzaveta Meleshko
Doctor of Engineering Sciences, Professor, Associate Professor of
Cybersecurity & Software Department,
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-8791-0063
elismeleshko@gmail.com

Oleksii Smirnov
Doctor of Sciences, Professor,
Head of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

LEGAL BASIS FOR THE DISSEMINATION OF INFORMATION INFLUENCES IN SOCIAL NETWORKS

Abstract. This paper examines the legal aspects of the regulation of informational influences in social networks, which are of particular importance in the conditions of modern digital challenges. The authors examine international and national legislation, in particular the regulations of the European Union, the United States, China and Australia, analyzing the approaches of different countries to the control of information flows, ensuring freedom of speech, protecting user data and the responsibility of online platforms. The article emphasizes the importance of a balanced legal system that would help preserve democratic freedoms and at the same time ensure information security, protecting vulnerable groups of the population, including children. An ideal legal system should include measures to control disinformation, ensure transparency of political advertising, protect personal data and hold social platforms accountable. Special attention should be focused on protecting vulnerable groups, such as children, and on combating hate speech. A comprehensive approach involving a combination of legislative changes, education efforts and cooperation with technology companies is necessary to create a safe online environment. The authors' conclusions confirm the need for constant adaptation of legislation to the rapidly changing conditions of the information environment. It is recommended to implement effective legal measures to counter information threats and disinformation, as well as ensure international cooperation to harmonize legal standards. It is promising to study the methods of increasing the transparency of the algorithms that form the information space of users, in order to reduce their influence on the perception of

information and behavior. Further research is aimed at evaluating the effectiveness of existing legal norms and developing strategies for their adaptation in various sociocultural contexts.

Keywords: social media; information influence; legal regulation; disinformation; cybersecurity; data protection; freedom of speech; platform liability; international standards; information security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bell, D. (1973). *The Coming of Post-Industrial Society. A Venture in Social Forecasting.*
2. Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe Convention (2021). https://zakon.rada.gov.ua/laws/show/995_004#Text
3. European Convention on Human Rights (n. d.). https://zakon.rada.gov.ua/laws/show/995_043#Text
4. United Nations (2022). *The role of States in countering the negative impact of disinformation on the exercise and enjoyment of human rights.* https://documents.un.org/doc/undoc/ltd/g22/296/55/pdf/g2229655.pdf?
5. *General Data Protection Regulation (GDPR)*. (n. d.). https://gdpr-text.com/uk/
6. *The Strengthened Code of Practice on Disinformation 2022.* (2022). https://disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Code-of-Practice-on-Disinformation-2022.pdf
7. Update of the EU Code on Combating Disinformation: Key Provisions (2022). https://jurliga.ligazakon.net/news/212519_onovlennya-kodeksu-s-shchodo-borotbi-z-deznformatsyu-osnovn-polozhennya.
8. Convention on the Rights of the Child, United Nations Convention (2023). https://zakon.rada.gov.ua/laws/show/995_021#Text
9. Constitution of Ukraine, No. 254к/96-ВР (2020) (Ukraine). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
10. On Information, Law of Ukraine No. 2657-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2657-12#Text
11. On the Protection of Personal Data, Law of Ukraine No. 2297-VI (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2297-17#Text
12. On Freedom of Conscience and Religious Organisations, Law of Ukraine No. 987-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/987-12#Text
13. On Electronic Communications, Law of Ukraine No. 1089-IX (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/1089-20#Text
14. On the Basic Principles of Ensuring Cybersecurity of Ukraine, Law of Ukraine No. 2163-VIII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2163-19#Text
15. On the Protection of Public Morality, Law of Ukraine No. 1296-IV (2023) (Ukraine). https://zakon.rada.gov.ua/laws/show/1296-15#Text
16. *Nations Against Disinformation Initiative.* (n. d.). NATIONS AGAINST DISIFORMATION INITIATIVE. https://www.nationsagainstdisinformation.org/partners/
17. *International Fact-Checking Network - Poynter.* (n. d.). Poynter. https://www.poynter.org/ifcn/.
18. *Global Network Initiative.* (n. d.). https://globalnetworkinitiative.org
19. Radzievska, O. G. (2017). Legal basis and priorities for the development of counteracting negative information influences on children. Information and Law, 2(21). https://doi.org/10.37750/2616-6798.2017.2(21).273045
20. Novytskyi, V. Y. (2022). Strategic principles of information security in modern conditions. *Information and Law, 1(40).* https://doi.org/10.37750/2616-6798.2022.1(40).254349
21. Pravdiuk, A. (2023). Astroturfing in social networks as a threat to democratic state-building. *Scientific innovations and advanced technologies, 1(15),* 154–166. https://doi.org/10.52058/2786-5274-2023-1(15)-154-166
22. Chernysh, R. (2019). Legal experience of the European Union countries in the field of combating the spread of fake information. *Information Law,* 123–128. https://doi.org/10.32849/2663-5313/2019.10.21
23. US Constitution, First Amendment. (n. d.). https://constitution.congress.gov/constitution/amendment-1/#:~:text=Congress%20shall%20make%20no%20law,for%20a%20redress%20of%20grievances
24. The Honest Ads Act. (б. д.). U.S. Senator Mark R. Warner. https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act

25. Department of justice's review of section 230 of the communications decency act of 1996. (б. д.). Department of Justice | Homepage | United States Department of Justice. https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996
26. On Cybersecurity, Law (2016) (China). https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm
27. Transparency of Digital Platforms Bill (2021) (Australia). https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680.
28. Section 875 of the US Code, Threats, 18 U.S.C. § 875 (b. d.). https://www.law.cornell.edu/uscode/text/18/875.
29. Section 373 of the U.S. Code, Incitement to commit violence, 18 U.S.C. § 373. (b.d.). https://www.law.cornell.edu/uscode/text/18/373
30. United States v. Reidel, US Supreme Court decision, 395 U.S. 444 (1969). https://tile.loc.gov/storage-services/service/ll/usrep/usrep395/usrep395444/usrep395444.pdf
31. Bill S.314 – Communications Decency Act, 104th U.S. Congress (1995–1996). https://www.congress.gov/bill/104th-congress/senate-bill/314
32. *Children's Online Privacy Protection Rule ("COPPA*"). (n. d.). Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
33. Kukharska, N., & Kukharskyi, V. (2014). Threats to children's safety in social networks. *Security of information, 20(2),* 169–175.
34. Yurchenko, O. Y. (2013). Problems of children's safety in social networks and the Internet (victimological aspect). *Social and analytical law: electronic professional edition, 3,* 336–338.
35. Hotsulyak, K. (2015). Influence of social networks on the development of junior schoolchildren's personality. *Mountain School of the Ukrainian Carpathians, 12–13,* 152–154.
36. Pronina, O. V. (2023). The impact of social networks on children and adolescents: risks and safety rules. *Educational management: successful practices and challenges,* 82–85.
37. Oliynyk, K. S. (2018). General characteristics and importance of social networks in the life of modern youth. *Pedagogical sciences: a collection of scientific works, 84(2),* 188–191.
38. Dashkovska, O. R. (2019). Protection of freedom of speech in the Internet space. *Comparative and Analytical Law, 5,* 16–20.
39. Kuzmenkova, K. S. (2024). Strategies for combating disinformation: European experience. *International scientific and practical conference 'From theory to practice in management and governance',* 97–99.
40. Vovchanska, O. M., & Ivanova, L. O. (2021). Social media market: new realities for business and consumers. *International scientific and practical conference,* 93–99. https://doi.org/10.30525/978-9934-26-042-1-22
41. Zavoivska, O. M. (2024). *Software module for detecting offensive words and hatred in text messages: qualification work.*
42. Kravchuk, V. O. (2024). The concept of information security on the Internet. *8th International Scientific and Practical Conference,* 757–763.
43. Kropyvko, V. (2022). Political advertising in public communication: between state regulation and the market. *Lviv University Bulletin, 43,* 282–288. https://doi.org/10.30970/PPS.2022.43.34
44. Radio, M. V. (2023). State regulation of the election campaign in social media (modern practice of foreign countries). *Political life, 2,* 76–82. https://doi.org/ 10.31558/2519-2949.2023.2.9
45. Havlovskyi, V. D. (2011). On the issue of personal data protection in social networks. *The fight against crime and corruption, 24,* 252–262.
46. Prokopovych, L. V., & Lopakov, O. S. (2021). Ways to improve the protection of personal data of social network users. *The Scientific Heritage, 65,* 32–37.
47. Kukina, N. V., Savchuk, Y. O., & Lialiuk, A. M. (2024). Analysing the role of social networks in the formation of brand loyalty. *Actual problems of modern science, 8(278),* 116–128.
48. Markulynets, A. (2024). Civil law regulation of social commerce: interaction of users and brands. *Scientific innovations and advanced technologies, 10(38),* 238–249.
49. Cherednichenko, O. Y., Tkachenko, V. V., & Vovk, M. A. (2018). Research of profiles of social network users. *Collection of scientific works of KNU, 2(56),* 113–119.
50. Shcherbakov, S., & Khrypko, S. (2024). The concept of big data. *Modern Trends in the Development of Scientific Space,* 60–65.
51. Kolesnyk, H. O. (2021). 'Hate speech' as a social and linguistic phenomenon. *Scientific Notes of Taurida National University, 32(71),* 278–283.

52. Sakhatska, O. (2023). Technology for teaching adolescents to identify hate speech in the media and prevent its spread. *Scientific Horizons of the XXI century*, 1210–1213.
53. Vasylkivskyi, M. V., & Budash, M. V. (2023). Ensuring information security in 6G telecommunication networks. *Scientific Bulletin of VNTU.*
54. Karapetyan, A. O. (2020). Flexibility in the application of laws in the field of education. *Scientific Notes of the Central State Pedagogical University, 186*, 115–120. https://doi.org/10.36550/2415-7988-2020-1-186-115-120
55. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.