ПРАВОВЕ РЕГУЛЮВАННЯ DEEPFAKES І СИНТЕТИЧНОГО КОНТЕНТУ: ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ ЄС ТА УКРАЇНИ

БІСЮК Олена Сергіївна - кандидат юридичних наук, доцент, професор кафедри публічного та європейського права, директор Навчально-наукового інституту міжнародних відносин та права ПЗВО «Київський міжнародний університет», м. Київ

https://orcid.org/0000-0002-1570-2721

УДК 347.78:004.5(4-6ЄС:477)

DOI: https://doi.org/10.71404/NP.2025.4.76

У статті досліджено правове регулювання deepfakes і синтетичного контенту як нового виду цифрової загрози, що набуває особливої актуальності в умовах збройного конфлікту та інформаційного протиборства. Метою дослідження є порівняльний аналіз регуляторних підходів Європейського Союзу та України до синтетичних медіа, виявлення прогалин національного законодавства та формулювання пропозицій щодо його вдосконалення. Встановлено, що ЄС сформував комплексну нормативну архітектуру, що охоплює Регламент (ЄС) 2024/1689 (AI Act), Регламент (ЄС) 2022/2065 (Digital Services Act) та Посилений кодекс практики щодо дезінформації (2022). Ключовим досягненням є закріплення легальної дефініції deepfakes у ст. 3(60) AI Act, класифікація синтетичних систем як систем обмеженого ризику та запровадження обов'язків щодо маркування контенту. Водночас критично оцінено недостатність прозорісних зобов'язань як єдиного механізму захисту. Щодо України, проаналізовано чинну нормативну базу — Закон «Про медіа» (2022), Закон «Про авторське право і суміжні права» (2022), Закон «Про цифровий контент та цифрові послуги» (2023), Кримінальний кодекс України, а також стратегічні документи — Дорожню карту з регулювання ШІ (2023) та Білу книгу (2024). Виявлено системні прогалини: відсутність легальної дефініції deepfakes, недостатність кримінально-правових норм, брак механізмів ідентифікації та маркування синтетичного контенту. У порівняльному аналізі констатовано суттєве відставання України від євростандартів. Сформульовано пропозиції de lege ferenda: закріплення дефініції синтетичного контенту в окремому законодавчому акті, доповнення Кримінального кодексу спеціальними складами, запровадження обов'язкового маркування AI-генерованого контенту, прискорення гармонізації з AI Act ЄС.

Ключові слова: deepfakes, синтетичний контент, штучний інтелект, правове регулювання, AI Act, Digital Services Act, інформаційна безпека, дезінформація, Європейський Союз, міжнародно-правове регулювання, законодавство, воєнний стан, міжнародна безпека, міжнародне гуманітарне право, захист прав.

Постановка проблеми

У сучасних умовах стрімкого розвитку технологій генеративного штучного інтелекту проблема правового регулювання синтетичного контенту набуває особливої гостроти. Deepfakes — штучно створені або маніпульовані аудіо-, відео- чи фотоматеріали, що виглядають як справжні, — перетворились із інструменту розваг на зброю інформаційного протиборства, когнітивного впливу та дискредитації публічних осіб. Практичним підтвердженням цього є резонансний інцидент березня 2022 року, коли в інформаційний простір було запущено deepfake-відео із зображенням Президента України Володимира Зеленського, що нібито закликає військових здатися — приклад, який наочно продемонстрував деструктив-

ний потенціал синтетичних медіа у збройному конфлікті [1, с. 19].

Актуальність дослідження зумовлена щонайменше трьома чинниками. По-перше, технологічним: за даними аналітичних центрів, кількість deepfakes в інформаційному просторі зросла у десятки разів упродовж 2022–2024 років, тоді як методи їх виявлення не встигають за темпами технологічного вдосконалення [2]. По-друге, правовим: ані у вітчизняному, ані у більшості зарубіжних правопорядків досі відсутнє комплексне законодавче регулювання відповідних відносин. По-третє, безпековим: в умовах гібридної агресії проти України deepfakes стали елементом стратегії психологічного та інформаційного тиску, що безпосередньо загрожує національній безпеці й суспільній довірі до інформації.

Зв'язок із практичними завданнями виявляється у необхідності гармонізації українського законодавства з регуляторними стандартами ЄС у контексті євроінтеграційного курсу України, зокрема в частині імплементації положень AI Act Regulation (EU) 2024/1689 щодо синтетичного контенту.

Аналіз останніх досліджень і публікацій

Аналіз наукових джерел свідчить про те, що проблематика deepfakes та синтетичного контенту перебуває у фокусі уваги переважно зарубіжних дослідників. Серед найвагоміших публікацій слід виокремити праці М. Лабуза (M. Łabuz), який здійснив системний аналіз положень AI Act щодо deepfakes і дійшов висновку про недостатність прозорісних зобов'язань як захисного механізму [3, с. 1–5]. Дослідник також розкрив телеологічні проблеми дефініції, пов'язані з використанням терміна «existing» у ст. 3(60) AI Act, що може обмежувати сферу її застосування [4, с. 1–3].

М. Павелець (M. Pawelec) дослідила вплив синтетичних медіа на демократичні інституції, систематизувавши типи шкідливого використання deepfakes за критеріями впливу на колективне формування волі та підотчетність публічної влади [1, с. 19]. Ф. Ромеро Морено (F. Romero Moreno) здійснив аналіз відповідності регулятивних механізмів AI Act положенням ст. 8 та 10 Конвенції про захист прав людини та основоположних свобод, піддавши критиці ризик порушення права на приватність та свободу вираження поглядів [5, с. 1–7].

Дж. Лакс, С. Вахтер та Б. Мітельштадт поставили під сумнів концепцію «надійного» ШІ в контексті AI Act, зазначивши, що ризик-орієнтований підхід може не враховувати глибинних суспільних загроз [6, с. 3–8]. М. Гусовець проаналізував правові обмеження Цифрового акта про послуги у сфері протидії дезінформації, зокрема щодо deepfake-контенту [7].

В українській науці означена проблематика перебуває на початковому етапі осмислення. Є. В. Дуліба дослідив загальні засади AI Act у контексті балансу між інноваціями та ризиками [8]. В. В. Бойко та М. В. Серебро зосередились на порівняльно-правовому аналізі зарубіжних підходів до регулювання ШІ [9, с. 23–24] [10, с. 1–3].

Разом з тим у вітчизняній юридичній науці досі відсутні комплексні дослідження, присвячені порівняльному аналізу регуляторних підходів ЄС та України до deepfakes і синтетичного контенту. Не розроблено концепції легальної дефініції для потреб національного законодавства, не сформульовано системних пропозицій щодо кримінально-правового та інформаційно-правового регулювання. Саме заповненню цих прогалин присвячена означена стаття.

Мета статті

Метою статті є здійснення порівняльного аналізу регуляторних підходів Європейського Союзу та України до правового регулювання deepfakes і синтетичного контенту, виявлення системних прогалин вітчизняного законодавства та формулювання науково обґрунтованих пропозицій щодо його вдосконалення.

Для досягнення зазначеної мети поставлено такі завдання: розкрити поняття та правову природу deepfakes як об'єкта правового регулювання; проаналізувати регуляторну архітектуру ЄС щодо синтетичного контенту; охарактеризувати стан правового регулювання в Україні; здійснити порівняльний аналіз обох підходів; сформулювати пропозиції de lege ferenda.

Виклад основного матеріалу дослідження

Термін «deepfake» виник у 2017 році як похідне від «deep learning» (глибинне навчання) та «fake» (підробка) і первісно використовувався для позначення синтетичних відео, створених за допомогою генеративно-змагальних мереж (GAN) [11]. Нині поняття набуло ширшого значення та охоплює будь-який аудіо-, відео- або фотоматеріал, що є повністю або частково штучно згенерованим чи маніпульованим з використанням технологій глибинного навчання.

Легальне визначення deepfakes на рівні ЄС закріплено у ст. 3(60) Регламенту (ЄС) 2024/1689 (AI Act): це «штучно згенерований або маніпульований контент у форматі зображення, аудіо або відео, що нагадує існуючих осіб, об'єкти, місця, суб'єктів або події та для пересічної особи виглядатиме як справжній або правдивий» [11]. Дискусійним у науковій літературі залишається питання щодо терміна «існуючих» (existing): М. Лабуз застерігає, що буквальне тлумачення може виключити з-під дії норми синтетичних персонажів, не прив'язаних до реальних прототипів, звужуючи захисний потенціал дефініції [4, с. 3–5].

З точки зору правової природи синтетичний контент може одночасно торкатися декількох сфер правового регулювання: права інтелектуальної власності (несанкціоноване використання зображення, голосу особи), захисту персональних даних (обробка біометричної інформації без згоди), інформаційного права (поширення дезінформації), кримінального права (наклеп, шахрайство, підбурювання до насильства). Ця міжгалузевість суттєво ускладнює вироблення єдиної регуляторної відповіді.

У той же час, Європейський Союз сформував багаторівневу нормативну архітектуру, що включає три ключових інструменти.

Першим і центральним є Регламент (ЄС) 2024/1689 (AI Act), що набрав чинності 1 серпня 2024 року [11]. AI Act застосовує ризик-орієнтований підхід, класифікуючи системи ШІ за чотирма рівнями: неприйнятний, високий, обмежений та мінімальний ризик. Deepfakes класифіковано у категорію «обмеженого ризику», наслідком чого є покладання виключно прозорісних зобов'язань без суворих ex ante вимог. Стаття 50 AI Act встановлює такі обов'язки: провайдери систем ШІ, що генерують синтетичний контент, зобов'язані забезпечити його машинозчитуване маркування, що дозволяє ідентифікацію штучного походження (ст. 50(2)); деплоєри систем, що генерують або маніпулюють зображеннями, аудіо чи відео у форматі deepfake, зобов'язані чітко і розпізнавано розкрити штучну природу такого контенту (ст. 50(4)).

Санкційний режим AI Act є значним: порушення заборонених практик ШІ тягне штраф до 35 млн євро або 7% глобального річного обороту, інші суттєві порушення — до 15 млн євро або 3% [11]. Водночас у доктрині відзначено суттєві недоліки обраного підходу. По-перше, прозорісні зобов'язання є неефективними щодо зловмисних акторів, які апріорі не будуть їх дотримуватись. По-друге, AI Act не передбачає механізмів захисту та компенсації для жертв deepfakes. По-третє, норми містять широкі винятки для сатиричного та художнього контенту, що відкриває можливості для зловживань [5, с. 10–15] [3, с. 20–25].

Другим рівнем регулювання є Регламент (ЄС) 2022/2065 про єдиний ринок цифрових послуг (Digital Services Act, DSA), що набрав повного застосування у лютому 2024 року [11]. DSA формує правову основу для відповідальності платформ за поширення шкідливого контенту, зокрема deepfakes. Дуже великі онлайн-платформи (VLOP) та пошукові системи (VLOSE) зобов'язані здійснювати оцінку системних ризиків та вживати заходів їх мінімізації, включаючи ризики, пов'язані з дезінформацією, де синтетичний контент відіграє дедалі більшу роль. Взаємозв'язок AI Act і DSA закріплено у Recital 118 AI Act, відповідно до якого виконання вимог щодо управління ризиками за DSA вважається достатнім для потреб AI Act у частині, що перетинається.

Третім рівнем є Посилений кодекс практики щодо дезінформації (2022), що з 1 липня 2025 року набув статусу кодексу поведінки відповідно до механізмів DSA [11]. Кодекс містить зобов'язання платформ щодо ідентифікації та маркування маніпульова-

ного контенту, співпраці з перевірниками фактів, надання доступу дослідникам. Слід зауважити, що М. Гусовець обґрунтовано вказує на внутрішнє протиріччя у системі: DSA сам по собі не забороняє дезінформацію, а Кодекс як інструмент м'якого права зберігає залишкову добровільність, що послаблює ефективність регулювання [7].

Таким чином, регуляторна архітектура ЄС характеризується системністю, горизонтальною узгодженістю та багаторівневим характером, поєднуючи «тверде» право (AI Act, DSA) з м'яким (Кодекс). Разом з тим доктрина одностайно вказує на ключову прогалину: система захищає від шкоди, що виникає внаслідок ненаправленого обігу deepfakes, але є недостатньою щодо цілеспрямованих кампаній дезінформації із залученням державних акторів [2].

На відміну від ЄС, в Україні відсутнє спеціальне законодавство щодо deepfakes і синтетичного контенту. Правове регулювання здійснюється фрагментарно через низку галузевих актів, жоден з яких не містить відповідної легальної дефініції.

У сфері авторського права Закон України «Про авторське право і суміжні права» від 01.12.2022 № 2811-IX у ст. 33 встановлює право sui generis на контент, згенерований ШІ, закріплюючи його за особами, яким належать майнові права на систему ШІ або які мають ліцензійні повноваження, за відсутності договірного регулювання [11]. Водночас цей Закон не врегульовує питання несанкціонованого використання біометричних даних, голосу чи зображення особи для створення deepfakes — ситуації, коли об'єктом маніпуляції є реальна людина.

Закон України «Про медіа» від 13.12.2022 № 2849-IX містить загальні положення щодо захисту від дезінформації, зобов'язуючи медіасуб'єктів дотримуватись стандартів достовірності інформації [11]. Проте цей закон не поширюється на широке коло платформ та не містить спеціальних механізмів протидії синтетичному контенту. Закон України «Про цифровий контент та цифрові послуги» від 10.08.2023 № 3321-IX, що набрав чинності 02.03.2024, спрямований насамперед на регулювання договірних відносин між постачальниками та споживачами цифрових послуг і також не стосується проблеми deepfakes безпосередньо [11].

У кримінально-правовому вимірі діяльність із створення та поширення deepfakes може кваліфікуватись за загальними нормами: ст. 182 КК (порушення недоторканності приватного життя), ст. 171 (перешкоджання законній діяльності журналістів), ст. 190 (шахрайство), ст. 255-1 (пропаганда), ст. 436-2 (виправдання збройної агресії). Водночас ці норми є загальними і не охоплюють специфіку технологічного способу вчинення правопорушення, що ускладнює доказування та правову кваліфікацію.

На стратегічному рівні Міністерство цифрової трансформації України у жовтні 2023 року представило Дорожню карту з регулювання ШІ, а у червні 2024 року — Білу книгу [11]. Ці документи передбачають двоетапну модель переходу від добровільної до обов'язкової регуляції: перший етап (2024–2025) — формування культури самоврядування та добровільні кодекси поведінки; другий (з 2026) — запровадження обов'язкових правил, гармонізованих з AI Act ЄС із досягненням 20% конвергенції до 2026 року та 50% — до 2027 року [11]. У травні 2025 року Україна підписала Конвенцію Ради Європи про ШІ, права людини, демократію та верховенство права, взявши на себе зобов'язання щодо забезпечення поваги до основоположних прав при застосуванні систем ШІ [11].

Таким чином, можна констатувати, що система правового регулювання deepfakes в Україні перебуває на початковому етапі формування. Наявні норми є фрагментарними, не утворюють цілісного регуляторного режиму та не відповідають масштабу загроз, що генеруються синтетичним контентом в умовах тривалого збройного конфлікту.

Водночас слід взяти до уваги, що між регуляторними підходами ЄС та України існує суттєва асиметрія за декількома ключовими параметрами.

Щодо нормативної архітектури: ЄС має тришарову конструкцію (AI Act — DSA — Кодекс), тоді як Україна характеризується фрагментарним і дисперсним регулюванням через галузеві закони без координаційного центру. Щодо дефінітивного апарату: ЄС

має легальну дефініцію deepfakes у ст. 3(60) AI Act [11]; в Україні відповідне поняття в жодному нормативному акті не визначено, що є фундаментальним недоліком правової системи. Щодо превентивних механізмів: AI Act запроваджує обов'язок маркування та ідентифікації штучного походження синтетичного контенту; в Україні такі механізми відсутні. Щодо відповідальності: AI Act передбачає значні штрафи на рівні ЄС [11]; в Україні відповідальність може наставати виключно за загальними нормами КК, що є недостатнім. Щодо захисту жертв: ні ЄС, ні Україна наразі не мають спеціальних компенсаційних механізмів для потерпілих від deepfakes, що є спільною прогалиною обох систем [5, с. 25–28].

Дискусійним залишається питання про те, чи є ризик-орієнтований підхід, обраний ЄС, оптимальним для умов тривалого збройного конфлікту. З одного боку, класифікація deepfakes як «обмеженого ризику» відповідає мирним умовам, де основна загроза — дезінформація та порнографічний контент без згоди. З іншого боку, в умовах гібридної агресії синтетичні медіа стають інструментом прямих інформаційних атак на воєнну та цивільну інфраструктуру, що вимагає якісно іншого рівня регуляторної відповіді [11]. Ми поділяємо позицію дослідників, які вказують, що Україна, на відміну від ЄС, може і повинна встановити більш жорсткі регуляторні вимоги для воєнного та кризового контексту, зберігаючи при цьому загальну сумісність із acquis ЄС [11].

Висновки

На підставі проведеного дослідження сформульовано такі висновки. По-перше, deepfakes і синтетичний контент є самостійним об'єктом правового регулювання, що має комплексну правову природу, охоплюючи одночасно елементи інформаційного, авторського, кримінального права та законодавства про захист персональних даних. Відсутність легальної дефініції є принциповою прогалиною як для правозастосовної, так і для нормотворчої практики.

По-друге, Європейський Союз сформував системну нормативну архітектуру для регулювання синтетичного контенту на основі ризик-орієнтованого підходу, де AI Act визначає горизонтальні стандарти, DSA забезпечує відповідальність платформ, а Кодекс практики задає орієнтири саморегулювання. Разом з тим встановлено, що прозорісні зобов'язання як основний захисний механізм є недостатніми для протидії цілеспрямованим інформаційним операціям із застосуванням deepfakes.

По-третє, вітчизняна правова система характеризується системними прогалинами у сфері регулювання deepfakes: відсутністю легальної дефініції синтетичного контенту, недостатністю спеціальних кримінально-правових норм, браком механізмів обов'язкового маркування AI-генерованого контенту та компенсаційних механізмів для жертв. Порівняльний аналіз засвідчує суттєве відставання України від євростандартів.

По-четверте, формулюються такі пропозиції de lege ferenda: закріплення легальної дефініції синтетичного контенту (deepfake) у спеціальному законодавчому акті із визначенням кваліфікуючих ознак; доповнення Кримінального кодексу України спеціальними складами правопорушень, що враховують технологічний спосіб вчинення діяння; запровадження обов'язкового маркування AI-генерованого контенту, аналогічного вимогам ст. 50 AI Act; прискорення гармонізації вітчизняного законодавства з положеннями Regulation (EU) 2024/1689 та Regulation (EU) 2022/2065; розроблення спеціальних регуляторних стандартів для умов воєнного стану, що враховують підвищений рівень загрози від синтетичного контенту в контексті збройного конфлікту.

Література

1. Pawelec M. Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. *Digital Society*. 2022. Vol. 1. № 2. Art. 19. DOI: https://doi.org/10.1007/s44206-022-00010-6 (дата звернення: 25.09.2025 р.)

2. Center for News, Technology & Innovation. *Synthetic Media & Deepfakes*. 2025. URL: https://cnti.org/issue-primers/synthetic-media-deepfakes/ (дата звернення: 25.09.2025 р.)

3. Łabuz M. Regulating Deep Fakes in the Artificial Intelligence Act. *Applied Cybersecurity & Internet Governance*. 2023. Vol. 2. № 1. P. 1–42. DOI: https://doi.org/10.60097/ACIG/162856 (дата звернення: 25.09.2025 р.)

4. Łabuz M. A Teleological Interpretation of the Definition of DeepFakes in the EU Artificial Intelligence Act — A Purpose-Based Approach to Potential Problems With the Word «Existing». *Policy & Internet*. 2025. Vol. 17. e435. DOI: https://doi.org/10.1002/poi3.435 (дата звернення: 25.09.2025 р.)

5. Romero Moreno F. Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content. *International Review of Law, Computers & Technology*. 2024. Vol. 38. Iss. 3. P. 1–30. DOI: https://doi.org/10.1080/13600869.2024.2324540 (дата звернення: 25.09.2025 р.)

6. Laux J., Wachter S., Mittelstadt B. Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk. *Regulation & Governance*. 2024. Vol. 18. № 1. P. 3–32. DOI: https://doi.org/10.1111/rego.12512 (дата звернення: 25.09.2025 р.)

7. Husovec M. The Digital Services Act's Red Line: What the Commission Can and Cannot Do About Disinformation. *Journal of Media Law*. 2024. DOI: https://doi.org/10.1080/17577632.2024.2362483 (дата звернення: 25.09.2025 р.)

8. Дуліба Є. В. Закон про штучний інтелект ЄС: у пошуках балансу між просуванням інновацій та визнанням ризиків. International Scientific Journal «Internauka». *Series: Juridical Sciences*. 2024. № 7. DOI: https://doi.org/10.25313/2520-2308-2024-7 (дата звернення: 25.09.2025 р.)

9. Бойко В. В. Правове регулювання штучного інтелекту: міжнародний досвід. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. Т. 35 (74). Вип. 2. С. 23–29. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.2/05 (дата звернення: 25.09.2025 р.)

10. Серебро М. В. Адміністративно-правове регулювання використання технологій штучного інтелекту: національний та зарубіжний досвід. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2024. № 70. DOI: https://doi.org/10.32782/2307-1745.2024.70.8 (дата звернення: 25.09.2025 р.)

11. RAND Corporation. Artificial Intelligence, Deepfakes, and Disinformation: A Primer. Santa Monica, 2022. URL: https://www.rand.org/pubs/perspectives/PEA1482-1.html (дата звернення: 25.09.2025 р.)

12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. L 202, 12.07.2024. P. 1–144. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 25.09.2025 р.)

13. Deonarine K. Deepfakes and Human Rights: Why the EU AI Act is Becoming the Global Standard for Ethical AI Regulation. MEIG Programme. 2025. URL: https://www.meig.ch/highlight-50-2025-deepfakes-and-human-rights-why-the-eu-ai-act-is-becoming-the-global-standard-for-ethical-ai-regulation/ (дата звернення: 25.09.2025 р.)

14. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union*. L 277, 27.10.2022. P. 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (дата звернення: 25.09.2025 р.)

15. European Commission. Strengthened Code of Practice on Disinformation. Brussels, 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (дата звернення: 25.09.2025 р.)

16. Про авторське право і суміжні права : Закон України від 01 грудня 2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20 (дата звернення: 25.09.2025 р.)

17. Про медіа : Закон України від 13 грудня 2022 р. № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20 (дата звернення: 25.09.2025 р.)

18. Про цифровий контент та цифрові послуги : Закон України від 10 серпня 2023 р. № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20 (дата звернення: 25.09.2025 р.)

19. Міністерство цифрової трансформації України. Дорожня карта з регулювання штучного інтелекту в Україні: Bottom-Up підхід. Київ, 2023. URL: https://thedigital.gov.ua/news/technologies/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu (дата звернення: 25.09.2025 р.)

20. OECD.AI. Roadmap for AI Regulation in Ukraine: A Bottom-Up Approach. 2025. URL: https://oecd.ai/en/dashboards/policy-initiatives/roadmap-for-ai-regulation-in-ukraine-a-bottom-up-approach (дата звернення: 25.09.2025 р.)

21. Council of Europe. Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. Vilnius, 2024. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence (дата звернення: 25.09.2025 р.)

22. Brookings Institution. Deepfakes and International Conflict. Washington, D.C., 2023. URL: https://www.brookings.edu/articles/deepfakes-and-international-conflict/ (дата звернення: 25.09.2025 р.)

23. European Parliamentary Research Service. Tackling Deepfakes in European Policy. Brussels, 2021. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039 (дата звернення: 25.09.2025 р.)

24. Łabuz M. Deep Fakes and the Artificial Intelligence Act — An Important Signal or a Missed Opportunity? *Policy & Internet*. 2024. Vol. 16. P. 783–800. DOI: https://doi.org/10.1002/poi3.406 (дата звернення: 25.09.2025 р.)

LEGAL REGULATION OF DEEPFAKES AND SYNTHETIC CONTENT: COMPARATIVE ANALYSIS OF EU AND UKRAINIAN APPROACHES

The article examines the legal regulation of deepfakes and synthetic content as a novel category of digital threat that has become particularly relevant in the context of armed conflict and information warfare. The purpose of the study is a comparative analysis of the regulatory approaches of the European Union and Ukraine to synthetic media, the identification of gaps in national legislation, and the formulation of proposals for its improvement. It is established that the EU has formed a comprehensive normative architecture comprising Regulation (EU) 2024/1689 (AI Act), Regulation (EU) 2022/2065 (Digital Services Act), and the Strengthened Code of Practice on Disinformation (2022). A key achievement is the establishment of a legal definition of deepfakes in Article 3(60) of the AI Act, the classification of synthetic systems as limited-risk AI systems, and the introduction of content labelling obligations. At the same time, the insufficiency of transparency obligations as the sole protection mechanism is critically assessed. With regard to Ukraine, the current regulatory framework is analysed — the Law on Media (2022), the Law on Copyright and Related Rights (2022), the Law on Digital Content and Digital Services (2023), the Criminal Code of Ukraine, as well as strategic documents — the AI Regulation Roadmap (2023) and the White Paper (2024). Systemic gaps are identified: absence of a legal definition of deepfakes, inadequacy of criminal law provisions, and lack of mechanisms for identification and labelling of synthetic content. In the comparative analysis, Ukraine's significant lag behind EU standards is noted. De lege ferenda proposals are formulated: establishing the definition of synthetic content in a separate legislative act, supplementing the Criminal Code with specific offences, introducing mandatory labelling of AI-generated content, and accelerating harmonisation with the EU AI Act.

Keywords: deepfakes, synthetic content, artificial intelligence, legal regulation, AI Act, Digital Services Act, information security, disinformation, European Union, international legal regulation, legislation, martial law, international security, international humanitarian law, protection of rights.