УДК 347:004.8

ЦИВІЛЬНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАВДАНУ ШТУЧНИМ ІНТЕЛЕКТОМ

Бондаренко І. Ю.
e-mail: ivan.bondarenko@nure.ua
Науковий керівник – канд. юр. наук, доцент Турута О. В.
Харківський національний університет радіоелектроніки, каф. СГН
м. Харків, Україна

This work identifies gaps in Ukrainian civil law regarding deepfake-related harm, analyses real cases including the Pikesville conviction in the United States, and provides a comparative overview of regulatory approaches in the EU, USA, UAE, and South Korea.

Розвиток штучного інтелекту, здатного генерувати зображення, породив технологію «Deepfake». Це синтетичний аудіовізуальний контент, що відтворює зовнішність, голос та поведінку реальної людини без її згоди. Deepfake може використовуватись для шахрайства, дискредитації та дезінформації. Ця технологія вже декілька років завдає шкоди як публічним особам, так і пересічним громадянам. Попри порушення прав фізичної або юридичної особи, Цивільний кодекс України (ЦК України) та багатьох країн не містить спеціальних норм щодо відповідальності за такі порушення. Метою роботи є виявлення прогалин у цивільно-правовому захисті фізичної особи від технології deepfake та сформулювати пропозиції для законодавців з урахування міжнародного регулювання та завершених судових справ.Звернемось до показових випадків. 16 березня 2022 року в ефірі телеканалу «Україна 24» з'явилося deepfake-відео, де Президент В. Зеленський нібито закликає бійців скласти зброю. Відео було швидко розповсюджене в соціальних мережах, однак незабаром спростоване [1]. Цей інцидент проілюстрував здатність deepfake дестабілізувати суспільство в умовах війни. У 2024 році в мережі поширилися явно сексуальні deepfake-зображення Тейлор Свіфт. Також прем'єр-міністерка Італії Дж. Мелоні подала до суду на авторів аналогічного відео зі своїм зображенням, встановивши прецедент для правових позовів проти deepfake-зловживань [2].

В Україні deepfake як правове явище не визначено жодним актом. Захист може здійснюватися лише за загальними нормами ЦК України, а саме: ст. 296, що передбачає право на використання імені: ім'я фізичної особи може використовуватися іншою особою лише у випадках і порядку, встановлених законом; ст. 297, що передбачає право на повагу гідності та честі; ст. 308, ч. 1: фотографія, інші художні твори, на яких зображено фізичну особу, можуть бути публічно показані, відтворені, розповсюджені лише за її згодою; ст. 1166: майнова шкода, завдана неправомірними діями, відшкодовується в повному обсязі особою, яка її завдала.

Ключова прогалина полягає в тому, що ст. 308 ЦК України захищає оригінальні фотографії та художні твори, але не їх синтетичну ШІ-імітацію. Deepfake – це не відтворення наявного зображення, а генерація нового, а в такому випадку закон його не охоплює. Крім того, ШІ не є суб'єктом цивільного права – ні фізичною особою, ні юридичною. Застосування цивільно-правової відповідальності за завдання майнової шкоди згідно зі ст. 1166 ЦК України передбачає встановлення винної особи, а у deepfake-інциденті відповідач «розмитий» між розробником ШІ, безпосереднім порушником та платформою – і кожен з них ухиляється від відповідальності.

Аналіз законодавства країн світу свідчить про спільну тенденцію руху від загальних норм до спеціального регулювання deepfake, однак жодна з існуючих моделей не забезпечує повноцінного цивільно-правового захисту потерпілого [3]. Так, наприклад ст. 3 Акту про штучний інтелект Європейського союзу (AI Act) визначає deepfake «зображення, аудіо або відеоконтент, створений або маніпульований ШІ, що нагадує реальних осіб і сприймається як автентичний». Провайдери зобов'язані маркувати такий контент у машино-читабельному форматі, а розповсюджувачі – вказувати штучне походження. Це превентивний підхід, однак питання цивільної відповідальності за шкоду Регламент не врегульовує. У США регулювання існує як на федеральному рівні, так і на рівні окремих штатів. Наприклад, у Каліфорнії ухвалили закон AB-730, а в Техасі SB-751. Вони забороняють deepfake кандидатів у виборчий період. Закон «No Fakes Act (2023)» забороняє ШІ-репліки без згоди особи з винятками для новин і пародій. Спеціального закону про цивільну відповідальність немає. В ОАЕ федеральний закон № 45 від 2021 про захист персональних даних забороняє обробку персональних даних без згоди. Кіберзлочинне законодавство карає поширення інформації з метою наклепу, а deepfake охоплюється цими нормами лише опосередковано. У Південній Кореї після понад 800 зафіксованих злочинів із deepfake сексуального характеру та розслідування Telegram-ботів посилено покарання: зберігання і перегляд такого контенту – до 7 років ув'язнення (раніше до 5) [3].

Справа Pikesville (США, 2024–2025) – це показовий випадок, який висвітлив прогалини наявного регулювання. У січні 2024 року директор зі спорту школи Pikesville, штат Меріленд, Дажон Дар'єн використав ШІ-інструменти для генерації аудіозапису директора Еріка Айсверта з расистськими та антисемітськими висловлюваннями. Запис поширився в соцмережах, зокрема через Instagram-акаунт із 340 000 підписників. Це спровокувало хвилю погроз і поліція була змушена охороняти будинок Айсверта [4]. Мотивом була помста за відмову поновити контракт через систематичні порушення службової дисципліни. Криміналістичний аналіз трьох незалежних експертів, включно з підрядником ФБР, підтвердив: запис містив сліди ШІ-генерації з подальшим людським редагуванням для

додання фонових шумів [4]. У квітні 2025 року суд виніс вирок: 4 місяці ув'язнення. Його засудили за єдиним пунктом обвинувачення у правопорушенні середньої тяжкості – «перешкоджання діяльності навчального закладу». Первинні обвинувачення у переслідуванні, помсті свідку та крадіжці були знято в рамках угоди [4]. Ця справа наочно демонструє центральну проблему: навіть за повної криміналістичної доказової бази та встановленого винуватця – відсутність спеціальних норм про deepfake призводить до мінімального покарання, а цивільна відповідальність за реальну шкоду честі, гідності та кар'єрі потерпілого залишається невирішеною.

Отже, deepfake є новим видом цивільного правопорушення, що завдає шкоди правам фізичної особи. З урахуванням виявлених прогалин пропонується три напрями вдосконалення законодавства України. По-перше, доповнити ст. 308 ЦК України нормою, що забороняє створення та поширення deepfake без згоди особи та гарантує право вимагати видалення контенту і відшкодування шкоди. По-друге, закріпити солідарну відповідальність розробника ШІ-системи та безпосереднього порушника у випадках, коли система не мала технічних обмежень для запобігання зловживанням. По-третє, зобов'язати платформи маркувати deepfake-контент під загрозою субсидіарної відповідальності – відповідно до вимог ст. 50(4) Регламенту 2024/1689 [3]. Запровадження запропонованих змін до ЦК України дозволить мнімізувати існуючу прогалину і забезпечити реальний захист особистих прав у цифровому середовищі.

Список використаних джерел:

1. Луценко Є. В ефірі «Україна 24» показали фейкове повідомлення Зеленського про «капітуляцію». Громадське. 16.03.2022. URL: https://hromadske.ua/posts/na-telekanali-ukrayina-24-translyuvali-fejkove-zvernennya-zelenskogo-pro-kapitulyaciyu (дата звернення: 28.02.2026).

2. Брудна боротьба: нардеп розповів, як штучний інтелект використовують для створення еротичних deep-fake відео. ТСН. 24.03.2024. URL: https://tsn.ua/svit/brudna-borotba-nardep-rozpoviv-yak-shtuchniy-intelekt-vikoristovuyut-dlya-stvorennya-erotichnih-deep-fake-video-2542531.html (дата звернення: 28.02.2026).

3. Petriv O. Artificial Intelligence and Deepfakes: How Countries Respond to Threats. Centre for Democracy and Rule of Law. 30.09.2024. URL: https://cedem.org.ua/en/analytics/artificial-intelligence-and-deepfakes-how-countries-respond-to-threats/ (дата звернення: 28.02.2026).

4. Former school athletic director gets 4 months in jail in racist AI recording case. Associated Press. 29.04.2025. URL: https://apnews.com/article/racist-ai-recording-maryland-high-school-487ea673b0449077cb23e7970546cb9f (дата звернення: 28.02.2026).