ПУБЛІЧНО-ПРАВОВІ ТА ПРИВАТНО-ПРАВОВІ ЗАСАДИ ПРАВОЗАСТОСУВАННЯ В СУЧАСНИХ УМОВАХ

УДК 347.5
DOI: 10.32782/2078-3566/2025-5-9

Дмитро ЛЕЩЕНКО©
кандидат юридичних наук, доцент
(Дніпровський державний університет внутрішніх справ, м. Дніпро, Україна)

ОСОБЛИВОСТІ ВІДПОВІДАЛЬНОСТІ ЗА ШКОДУ, ЗАПОДІЯНУ ІЗ ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

У статті розглядається питання відповідальності за шкоду, заподіяну із використанням штучного інтелекту. Охарактеризовано процес врегулювання штучного інтелекту у ЄС та наведено основні риси спеціального нормативного акта – EU AI Act – прийнятого у 2024 році та присвяченого гармонізованим правилам використання штучного інтелекту. Зазначено, що в Україні у 2020 році була прийнята Концепція розвитку штучного інтелекту, яка подальшого розвитку не отримала і не трансформувалась у спеціальний закон чи підзаконні акти, що б врегульовували використання ШІ в Україні. У дослідженні наведено основні види відповідальності за шкоду, заподіяну із використанням штучного інтелекту. Наголошується на особливостях встановлення факту вини розробників, операторів та користувачів штучного інтелекту. Звертається увага на окремі моменти, яким варто приділяти увагу при притягненні винних осіб до відповідальності, а також на необхідності розробки перспективного законодавства України відповідно до існуючих міжнародних стандартів.

Ключові слова: *деліктна відповідальність; штучний інтелект; Акти та Директиви ЄС; розробники, оператори та користувачі інструментів штучного інтелекту; цифрова трансформація.*

Постановка проблеми. Впровадження штучного інтелекту (далі – ШІ) в усьому світі прискорюється неймовірними темпами, і переважна більшість людей та організацій не заперечують потенційні переваги, які пропонує ШІ для окремих осіб та суспільства загалом. В той же час ШІ несе із собою і серйозні виклики, деякі з яких вже виявлені, а інші, ймовірно, виникатимуть найближчим часом – починаючи від репутаційних ризиків і закінчуючи майновими збитками та шкодою кібербезпеці не лише окремих організацій, а й цілих країн.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Вагомий внесок у розроблення наукових положень із зазначеної тематики зробили такі науковці, як: О. О. Баранов, А. С. Довбиш, Т. В. Єрошенко, Т. Д. Лукашова, М. І. Мірошниченко, А. І. Шевченко, Cynthia Kroet, Michèle Dubrocard та інші. Нині особливої актуальності також набувають питання щодо адаптації чинного законодавства України до реалій технологічного сьогодення та актуальних міжнародних стандартів. Вирішення цих проблемних питань вимагає комплексного підходу й подальших науково-практичних

ORCID iD: https://orcid.org/0009-0000-8955-8892
dmytro.leshchenko@dduvs.edu.ua

розробок.

Метою статті є дослідження основних міжнародних нормативно-правових актів, у яких намагались врегулювати питання відповідальності за шкоду, заподіяну із використанням ШІ, та проведення порівняльного аналізу із відповідними вітчизняними нормативно-правовими актами.

Виклад основного матеріалу. Як відзначалось мною у попередніх дослідженнях, ініціатива прийняття у 2020 році Концепції розвитку штучного інтелекту [3] подальшого розвитку в Україні не отримала і не трансформувалась у спеціальний закон чи підзаконні акти, щоб врегульовували використання ШІ в Україні.

Тим часом у ЕС було розроблено та прийнято EU AI Act – Регламент № 2024/1689 Європейського Парламенту та Ради ЄС від 13 червня 2024 року (далі – EU AI Act), що встановлює гармонізовані правила щодо штучного інтелекту. Відповідно до п. 4 преамбули Регламенту під ШІ розуміється "сімейство технологій, що швидко розвивається, що сприяє отриманню широкого спектру економічних, екологічних і суспільних переваг у всьому спектрі галузей і соціальної діяльності. Шляхом покращення прогнозів, оптимізації операцій і розподілу ресурсів, а також персоналізації цифрових рішень, доступних для окремих осіб і організацій, використання штучного інтелекту може забезпечити ключові конкурентні переваги підприємствам і підтримувати соціально та екологічно вигідні результати, наприклад, у сфері охорони здоров'я, сільського господарства, безпеки харчових продуктів, освіти та навчання, ЗМІ, спорту, культури, управління інфраструктурою, енергетики, транспорту та логістики, державних послуг, безпеки, правосуддя тощо" [7].

ШІ активно використовується для захисту інформаційних систем: виявлення вірусів, фішингових атак, аналіз поведінки користувачів, автоматизована реакція на загрози. Проте зростає кількість інцидентів, коли ШІ стає інструментом кіберзлочинців (автоматизація фішингу, генерація deepfake, атаки на системи тощо). В якості прикладу можна навести генеративний ШІ, зокрема ChatGPT, який став доступнішим, що робить фішингові атаки через нього ефективнішими. Зокрема, непоодинокими були випадки, коли ChatGPT генерував текст фішингових листів та автоматично створював шахрайські вебсайти, які імітували справжні інтернет-ресурси (виглядають абсолютно ідентично до оригінальних) і налаштовувались так, щоб на них користувачі вводили свої дані.

Отже, можна констатувати, що ШІ може бути як корисним помічником, так й інструментом злочинців, насамперед тих, хто порушує кібербезпеку як окремих організацій, так і цілих країн, при цьому завдаючи шкоди необмеженому колу осіб.

Зазвичай у будь-яких правовідносинах мало хто заздалегідь думає про відповідальність. Однак, як сказав Томас Карлейль: «Неможливо ступити ні кроку по цій землі без того, щоб не стикнутися з відповідальністю та обов'язком, який необхідно виконати». Дійсно, використання штучного інтелекту також тягне за собою права, обов'язки та відповідальність.

Але де проходить межа між відповідальністю розробника програми зі штучним інтелектом та користувача такої програми? Як влучно зазначила Клян А., поки Ілон Маск та Марк Цукерберг сперечаються про небезпеку штучного інтелекту для людства, юристи сперечаються про те, хто несе відповідальність за наслідки роботи штучного інтелекту [1].

Відповідальність, пов'язана з використанням штучного інтелекту, станом на сьогодні нормативно не закріплена, навіть у ЄС, де по суті був прийнятий спеціальний нормативний документ, що встановлював стандарти для ШІ.

У зв'язку з цим у ЄС, починаючи з 2022 року, неодноразово порушувалося питання притягнення до відповідальності за шкоду, заподіяну із використанням ШІ. Так, 28 вересня 2022 року Європейська Комісія опублікувала свою Пропозицію щодо Директиви про адаптацію правил недоговірної (деліктної) цивільної відповідальності до штучного інтелекту (Директива про відповідальність за штучний інтелект – AILD), що викликало багато надій серед усіх, хто був стурбований потенційно шкідливими наслідками використання систем ШІ [5].

Але вона не отримала підтримки і AI Liability Directive (AILD) було вилучено з робочої програми Комісії на 2025 рік через відсутність прогресу в переговорах та «жодної передбачуваної згоди» щодо цієї пропозиції. Основна проблема полягала у неможливості співіснування в ЄС 27 різних режимів відповідальності за шкоду, заподіяну ШІ, що призводить до різних рівнів захисту та спотвореної конкуренції між підприємствами з різних держав-членів» [6]. Хоча Комісія зазначила, що справа може залишитися на столі,

якщо парламент і Рада ЄС зобов'яжуться провести над нею масштабну роботу протягом наступного року.

На сьогодні за неправомірне використання ШІ для кібератак у світі передбачені наступні види відповідальності:

1) кримінальна відповідальність за кібератаки, зокрема за несанкціонований доступ до комп'ютерних систем, розповсюдження шкідливого програмного забезпечення, фішинг, маніпуляції з даними, в тому числі із використанням ШІ. В США такі дії регулюються, зокрема, Computer Fraud and Abuse Act (CFAA), законами про посилення кібербезпеки та про кіберзлочинність і підробку, а в інших країнах існують аналогічні закони. Санкцій передбачають: - позбавлення волі від кількох місяців до довічного ув'язнення, особливо за кібертероризм, шпигунство, шахрайство з використанням ШІ; - штрафи від 1000 до 250000 доларів; - конфіскація майна; - заборона в'їзду для іноземців; – умовне покарання, пробація тощо;

2) адміністративні штрафи та санкції за порушення законів про кібербезпеку, захист персональних даних (зокрема, EU AI Act 2024, GDPR 2016 у ЄС, Закон України «Про захист персональних даних»), особливо якщо атаки призвели до витоку або неправомірного використання персональних даних. Наприклад, за порушення EU AI Act передбачені штрафи до €15 млн або 3% світового обороту компанії;

3) цивільна відповідальність за завдану шкоду третім особам, включно з відшкодуванням збитків, якщо кібератака була здійснена з використанням ШІ-компонентів, наприклад, генеративних моделей, що створюють фішингові листи або шкідливий код. Наприклад, компанія Microsoft повідомила про подання позову проти 10 неназваних відповідачів, звинувачених у використанні її сервісу Azure OpenAI. Згідно з позовом, поданим у грудні 2024 року до Окружного суду США Східного округу Вірджинії, відповідачі нібито використовували викрадені облікові дані клієнтів та спеціальне програмне забезпечення для обходу заходів безпеки, створюючи шкідливий контент через платформу. Розмір майнової та моральної шкоди встановлює та підтверджує суд у кожному конкретному випадку;

4) санкції проти кіберзлочинців. Зокрема, США, Велика Британія та Австралія запровадили санкції проти російського кіберугруповання Evil Corp, включно з арештом активів і забороною діяльності;

5) втрата ліцензій і дозволів на ведення діяльності, що пов'язана з інформаційними технологіями або обробкою даних, у разі систематичних порушень кібербезпеки;

6) репутаційні втрати, які можуть призвести до значних фінансових збитків і втрати довіри клієнтів та партнерів.

В Україні згідно із Законом «Про основні засади забезпечення кібербезпеки України» 2017 року: "особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом" [2].

Кримінальний кодекс України містить ряд статей (ст. ст. 361, 361-1, 361-2, 362, 363, 363-1 ККУ) за різні злочини, зокрема за несанкціоноване втручання в роботу інформаційних систем, а також за перешкоджання роботі комп'ютерних мереж шляхом масового розповсюдження повідомлень (це можуть бути DDos-атаки, спам) тощо. За такі правопорушення передбачено різні санкції: – штраф від 1000 до 4000 НМДГ; – пробаційний нагляд на строк до 3 років; – обмеженням волі на 3 роки; - виправні роботи на строк до 2 років; – позбавлення волі на строк до 3 років.

Для відшкодування шкоди, завданої кіберзлочинами чи шкоди, спричиненою ШІ, можуть застосовуватись і загальні норми Цивільного кодексу України, що регулюють деліктну відповідальність, а саме: – відшкодування майнової шкоди (ст. 1166 ЦКУ); – відшкодування моральної шкоди (ст. 1167 ЦКУ).

В той же час ані міжнародне законодавство, ані законодавство України станом на червень 2025 року не містять "прямих" кримінальних чи цивільних норм, що передбачають відповідальність саме за шкоду, завдану із використанням ШІ, але застосовуються норми існуючих Актів, Кодексів та законів про кіберзлочини.

Оскільки нормативно-правове регулювання відповідальності за шкоду, заподіяну із використанням штучного інтелекту, відсутнє як у ЄС, так і в Україні, то для визначення

відповідальної особи у кожному окремому випадку важливим є встановлення причинно-наслідкового зв'язку та встановлення моменту, дії, обставини тощо, внаслідок якої виникла некоректна робота ШІ.

Деякі автори в якості прикладу наводять ситуацію, коли внаслідок використання автопілоту, згенерованого із використанням ШІ, сталася ДТП. З метою визначення відповідальної особи необхідно буде встановлювати, чия саме відповідальність настає (розробника, оператора чи користувача технології ШІ) та що стало причиною аварії:

а) недоліки самої програми, що матиме наслідком відповідальність творця такої програми чи її обслуговуючої компанії (розробника чи оператора ШІ);

б) некоректне використання автопілоту водієм, що потягне відповідальність останнього (користувача ШІ);

в) втручання третіх осіб, які, наприклад, зламали та пошкодили програму або внесли в неї певні зміни та, відповідно, вина таких осіб [1].

Як бачимо, через відсутність врегулювання, багато питань стосовно притягнення до відповідальності за шкоду, заподіяну із використанням ШІ, залишаються без відповідей та вирішуються юристами за аналогією з іншими подібними правовідносинами, а сам вид відповідальності остаточно буде встановлювати та призначати суд у кожному конкретному випадку.

Враховуючи викладене вище, кримінальна та цивільна відповідальність за шкоду від використання ШІ – це реальність частково сучасного, але у більшій мірі перспективного міжнародного законодавства, з тенденцією до посилення захисту потерпілих через спрощення доказування, обов'язкове страхування та підвищені вимоги до прозорості й управління ризиками для розробників, операторів і користувачів ШІ.

Висновки. Таким чином, імплементація у діюче законодавство України положень EU Artificial Intelligence Act (та супровідних нормативних документів, що будуть уточнювати відповідальність винних осіб за шкоду, заподіяну із використання ШІ) або прийняття адаптованого до нього Закону про штучний інтелект, не кажучи вже про доповнення діючих Кримінального та Цивільного кодексів України нормами, що відповідатимуть міжнародним стандартам та передовим практикам, встановлюючи відповідальність за правопорушення із використанням новітніх технологій, насамперед ШІ, є нагальною потребою якщо не сьогодення (зважуючи на більш пріоритетні зовнішні фактори), то принаймні найближчих років в Україні.

Список використаних джерел

1. Клян А. Правове регулювання штучного інтелекту в Україні та світі. *GOLAW.* URL: https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

3. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

4. Шевченко А. І., Барановський С. В., Білокобильський О. В. та ін. Стратегія розвитку штучного інтелекту в Україні : монограф. ; за заг. ред. А. І. Шевченка. Київ : ІПШІ, 2023. 305 с.

5. Dubrocard M. AI liability rules: a blocked horizon? *European Area of Freedom Security & Justice.* URL: https://free-group.eu/2025/03/13/ai-liability-rules-a-blocked-horizon/.

6. Kroet C. Lawmakers reject Commission decision to scrap planned AI liability rules. *Euronews.* URL: https://www.euronews.com/next/2025/02/18/lawmakers-reject-commission-decision-to-scrap-planned-ai-liability-rules.

7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *EUR-Lex.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689.

References

1. Klian, A. Pravove rehuliuvannia shtuchnoho intelektu v Ukraini ta sviti [Legal regulation of artificial intelligence in Ukraine and the world]. *GOLAW.* URL: https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/. [in Ukr.].

2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity in Ukraine] : Zakon Ukrainy vid 05 zhovtnia 2017 r. *Vidomosti Verkhovnoi Rady Ukrainy.* 2017. № 45. Art. 403. [in Ukr.].

3. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini [On approval of the Concept of the development of artificial intelligence in Ukraine] : rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02 hrudnia 2020 r. № 1556-r. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text. [in Ukr.].

4. Shevchenko, A. I., Baranovskyi, S. V., Bilokobylskyi, O. V. ta in. Stratehiia rozvytku shtuchnoho intelektu v Ukraini [Strategy for the development of artificial intelligence in Ukraine] : monohrafiia / za zah. red. A. I. Shevchenka. Kyiv : IPShI, 2023. 305 p. [in Ukr.].

5. Dubrocard, M. AI liability rules: a blocked horizon? *European Area of Freedom Security & Justice.* URL: https://free-group.eu/2025/03/13/ai-liability-rules-a-blocked-horizon/.

6. Kroet, C. Lawmakers reject Commission decision to scrap planned AI liability rules. *Euronews.* URL: https://www.euronews.com/next/2025/02/18/lawmakers-reject-commission-decision-to-scrap-planned-ai-liability-rules.

7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689.

ABSTRACT

Dmytro Leshchenko. Peculiarities of liability for harm caused through the use of artificial intelligence. This article examines the issue of liability for harm caused through the use of artificial intelligence. The process of artificial intelligence regulation in the EU is characterized, and the main features of the special regulatory act – the EU AI Act – adopted in 2024 and dedicated to harmonized rules for the use of artificial intelligence are presented. It is noted that Ukraine adopted the Concept for the Development of Artificial Intelligence in 2020, which has not received further development and has not been transformed into a special law or secondary legislation that would regulate the use of AI. The main types of liability for harm caused through the use of artificial intelligence are outlined. Emphasis is placed on the peculiarities of establishing fault on the part of developers, operators, and users of artificial intelligence. Attention is drawn to specific aspects that should be considered when holding responsible parties accountable, as well as on the need to develop prospective Ukrainian legislation, in compliance with existing international standards.

Based on the analysis, it is emphasized that criminal and civil liability for harm from the use of AI is a reality of partly modern, but to a greater extent promising international legislation, with a tendency to strengthen the protection of victims through simplification of proof, mandatory insurance, and increased requirements for transparency and risk management for developers, operators, and users of AI.

Key words: *tort liability; artificial intelligence; EU Acts and Directives; developers, operators, and users of AI tools; digital transformation.*

Надійшла до редакції: 27.11.2025
Прийнято до друку після рецензування: 05.12.2025
Опубліковано: 31.12.2025