4. European Commission. Artificial Intelligence Act [Електронний ресурс] / European Commission, 2021. Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

5. The White House. Blueprint for an AI Bill of Rights [Електронний ресурс] / The White House, Office of Science and Technology Policy (OSTP), 2022. Режим доступу: https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

Зленко Вікторія
здобувач вищої освіти спеціальності D3 Менеджмент
Вінницького державного педагогічного університету імені Михайла Коцюбинського
Посвалюк О. А.
асистент кафедри фундаментальних і приватно-правових дисциплін
Вінницького державного педагогічного університету імені Михайла Коцюбинського

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ВІРТУАЛЬНИХ СЕРЕДОВИЩ

Захист персональних даних в умовах використання штучного інтелекту та віртуальних середовищ є актуальним правовим питанням, оскільки сучасні цифрові технології дають змогу збирати й аналізувати значно ширший обсяг інформації про людину, ніж традиційні онлайн-сервіси. VR/AR/XR-середовища, системи розпізнавання облич, eye-tracking, пупілометрія та алгоритми штучного інтелекту можуть фіксувати не лише звичайні ідентифікаційні дані, а й поведінкові, фізіологічні та емоційні реакції користувача. У поєднанні з іншими даними така інформація може використовуватися для створення детального цифрового профілю особи.

В українському законодавстві право на приватність має конституційне закріплення. Зокрема, стаття 32 Конституції України гарантує недопустимість втручання в особисте і сімейне життя особи, крім випадків, передбачених законом [1]. Закон України «Про захист персональних даних» визначає правові засади захисту персональних даних під час їх обробки [2]. Отже, обробка даних у системах ШІ та VR/AR/XR-середовищах має розглядатися з урахуванням як європейських, так і національних правових гарантій.

Відповідно до статті 4(1) GDPR, персональними даними є будь-яка інформація, що стосується ідентифікованої або такої, що може бути

ідентифікована, фізичної особи [3]. Тому поведінкові дані користувача у віртуальному середовищі можуть вважатися персональними даними, якщо вони прямо або опосередковано дозволяють встановити конкретну особу. Наприклад, траєкторія руху, напрямок погляду, тривалість фіксації уваги, реакція на цифрові об'єкти або спосіб взаємодії з платформою можуть у поєднанні з іншими ідентифікаторами мати персоналізований характер.

Особливої уваги потребує розмежування поведінкових і біометричних даних. GDPR визначає біометричні дані як персональні дані, отримані внаслідок спеціальної технічної обробки фізичних, фізіологічних або поведінкових характеристик особи, які дозволяють або підтверджують її унікальну ідентифікацію [3]. Отже, не кожна поведінкова характеристика автоматично є біометричною, однак у разі її використання для ідентифікації особи вона може набувати ознак біометричних даних.

У віртуальних середовищах такі ризики посилюються, оскільки VR/AR/XR-платформи можуть збирати дані про рухи тіла, положення рук, погляд, швидкість реакції, емоційні прояви та взаємодію з цифровими об'єктами. Технології eye-tracking і пупілометрії дозволяють визначати, на що саме користувач звертає увагу, як довго він утримує погляд і які стимули викликають у нього реакцію. У науковій літературі зазначається, що такі технології можуть застосовуватися у нейромаркетингу та створювати ризики надмірного впливу на автономію споживача [7]. Це свідчить про те, що навіть дані, які на перший погляд здаються технічними, можуть мати глибоко особистий зміст.

Проблема полягає не лише у зборі даних, а й у можливості виведення нової інформації за допомогою алгоритмів штучного інтелекту. ШІ може аналізувати поведінкові та фізіологічні дані й робити висновки про емоційний стан, інтереси, вразливості або психологічні особливості користувача. У цьому контексті важливим є підхід до ментальних даних, які можуть відображати когнітивні, емоційні та афективні процеси людини [6]. Водночас стаття 9 GDPR встановлює особливий режим лише для окремих спеціальних категорій персональних даних, зокрема біометричних даних з метою унікальної ідентифікації особи, даних про здоров'я та генетичних даних [3]. Тому виникає правова проблема: окремі поведінкові чи психоемоційні дані можуть формально не бути спеціальною категорією, але фактично дозволяти глибоке втручання у приватне життя людини.

Важливими запобіжниками у цій сфері є принцип мінімізації даних і належна згода користувача. Відповідно до статті 5 GDPR, оброблятися мають лише ті персональні дані, які є необхідними для конкретної та законної мети [3]. Згода,

своєю чергою, має бути вільною, конкретною, поінформованою та однозначною [3]. У VR/AR/XR-середовищах це особливо важливо, оскільки користувач може не усвідомлювати, що його погляд, рухи або мікрореакції також мають значення як персональні дані.

Окремим ризиком є профілювання особи. GDPR визначає профілювання як автоматизовану обробку персональних даних для оцінювання певних особистих аспектів фізичної особи, зокрема її поведінки, інтересів, здоров'я або переміщення [3]. У дослідженнях наголошується, що багатоступеневе профілювання може створювати вибірковий вплив на різні групи осіб і породжувати проблеми у сфері автоматизованого прийняття рішень [5]. У віртуальних середовищах цей ризик посилюється, адже профіль користувача може формуватися не лише на основі кліків чи переглядів, а й на основі тілесних, емоційних і фізіологічних реакцій.

Такі дані можуть використовуватися для персоналізованої реклами, мікротаргетингу та впливу на поведінку користувача. Поведінкові й психоемоційні показники можуть допомагати визначати моменти, коли особа є найбільш вразливою до переконання або комерційного впливу. Дослідження афінного профілювання показують, що онлайн-реклама може створювати ризики дискримінації за асоціацією, коли людина зазнає певного інформаційного впливу через схожість із певною групою користувачів [8]. У VR/AR/XR-середовищах така проблема може стати ще серйознішою, оскільки система здатна враховувати реакції, які людина не завжди контролює свідомо.

Важливе значення у цьому контексті має AI Act, який встановлює правила щодо використання штучного інтелекту в Європейському Союзі [4]. Стаття 5 AI Act забороняє окремі практики застосування ШІ, зокрема використання маніпулятивних або підсвідомих технік, здатних суттєво спотворювати поведінку особи та завдавати їй фізичної або психологічної шкоди [4]. Це положення є особливо важливим для віртуальних середовищ, оскільки такі технології можуть впливати на сприйняття людини значно сильніше, ніж звичайні цифрові платформи.

Отже, захист персональних даних в умовах використання штучного інтелекту та віртуальних середовищ потребує комплексного підходу. GDPR забезпечує основні правила щодо персональних даних, спеціальних категорій, згоди, мінімізації та прозорості [3], а AI Act доповнює їх обмеженнями щодо небезпечних і маніпулятивних практик застосування ШІ [4]. Водночас розвиток VR/AR/XR-технологій, eye-tracking, пупілометрії та поведінкового профілювання потребує подальшого уточнення правових підходів, особливо

щодо даних, які формально не є спеціальними категоріями, але фактично дозволяють робити глибокі висновки про емоції, психічний стан, інтереси та вразливості людини. Основним завданням правового регулювання має бути збереження балансу між розвитком інновацій і реальним захистом приватності, автономії та гідності людини.

Список використаних джерел:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 13.06.2026).

2. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 13.06.2026).

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal of the European Union. 2016. L 119. P. 1–88. URL: http://data.europa.eu/eli/reg/2016/679/oj (дата звернення: 13.06.2026).

4. 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 and Directives (Artificial Intelligence Act). Official Journal of the European Union. 2024. L, 2024/1689. URL: http://data.europa.eu/eli/reg/2024/1689/oj (дата звернення: 13.06.2026).

5. Binns R., Veale M. Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR. International Data Privacy Law. 2021. Vol. 11, № 4. P. 319–332. URL: https://academic.oup.com/idpl/article/11/4/319/6403925?login=false (дата звернення: 13.06.2026).

6. Ienca M., Malgieri G. Mental data protection and the GDPR. Journal of Law and the Biosciences. 2022. Vol. 9, № 1. Article lsac006. DOI: https://doi.org/10.1093/jlb/lsac006.

7. Sposini L. Neuromarketing and Eye-Tracking Technologies Under the European Framework: Towards the GDPR and Beyond. Journal of Consumer Policy. 2024. Vol. 47, № 3. P. 321–344. DOI: https://doi.org/10.1007/s10603-023-09559-2.

8. Wachter S. Affinity profiling and discrimination by association in online behavioral advertising. Berkeley Technology Law Journal. 2020. Vol. 35, № 2. P. 367. DOI: https://doi.org/10.15779/Z38JS9H82M.