

## **ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОМЕРЦІЙНИХ ОНЛАЙН ПЛАТФОРМАХ: ЄВРОПЕЙСЬКИЙ, АМЕРИКАНСЬКИЙ ТА КИТАЙСЬКИЙ ПІДХОДИ**

**Щербак Геннадій Ростиславович**

*аспірант кафедри міжнародного, цивільного та комерційного права  
Державного торговельно-економічного університету  
м. Київ, Україна*

Кожного року все більше комерційних онлайн платформ починають використовувати технологію штучного інтелекту (далі – ШІ), оскільки це допомагає краще та ефективніше враховувати побажання своїх користувачів та залучати нових клієнтів, а також забезпечувати вищий рівень обслуговування [1].

Використання ШІ надає комерційним онлайн платформам та їх користувачам різноманітні переваги: створення персоналізованого досвіду для користувачів, платформ, оптимізація менеджменту товарно-матеріальними запасами, автоматизація обслуговування споживачів, аналіз та фільтрування відгуків користувачів, виявлення та запобігання шахрайству тощо [2]. Однак в той же час використання ШІ в системах онлайн платформ може призвести до ряду негативних наслідків: порушення безпеки особистих даних користувачів, відсутність прозорості діяльності ШІ, а також упередженість та несправедливість ШІ.

Порушення безпеки особистих даних користувачів становить загрозу, оскільки алгоритми ШІ покладаються на дані споживачів при створенні персоналізованих рекомендацій та прогнозів. Як наслідок керовані ШІ онлайн платформи, управляють величезними обсягами даних, що може загрожувати витоком даних і поставити під загрозу особисту інформацію клієнтів.

Друга проблема у сфері використання штучного інтелекту в онлайн платформах – відсутність прозорості та зрозумілості, яка існує в багатьох алгоритмах машинного навчання. Іноді буває дуже важко або навіть неможливо зрозуміти, як певний алгоритм прийшов до свого рішення чи рекомендації.

Під проблемою упередженості та несправедливості розуміється те, що алгоритми машинного навчання покладаються на відповідні дані, які є необхідними для навчання, і якщо ці дані містять будь-які упередження, алгоритм може в кінцевому підсумку посилити або навіть збільшити ці

упередження. Цілком можливо, що система може несвідомо дискримінувати певні групи на основі таких факторів, як раса, стать або економічне становище [3].

Вище зазначені проблеми вимагають належного правового регулювання. Частково діяльність ШІ є врегульованою за допомогою законодавства про захист персональних даних. Наприклад, в ЄС у травні 2018 року набрав чинності Загальний регламент про захист персональних даних (далі – GDPR). GDPR встановлює правила для збирання, оброблення та зберігання персональних даних у Європейському Союзі, а також передбачає стандарти захисту приватності, зокрема, і при використанні штучного інтелекту. Наприклад, компанія Clearview AI, яка є розробником програмного забезпечення для розпізнавання обличчя з використанням штучного інтелекту, отримала декілька штрафів за незаконне використання персональних даних осіб у декількох державах-членах ЄС [4]. Що ж стосується закону, який би безпосередньо регулював питання, пов'язані з ШІ, то в ЄС планується прийняття комплексного акту з регулювання створення та використання ШІ. Проект акту містить класифікацію моделей штучного інтелекту в залежності від ступеня ризику, пов'язаного з використанням відповідної моделі. До переліку входять наступні види: моделі неприйнятної ризику, моделі високого ризику, моделі обмеженого ризику та моделі мінімального ризику. Моделі з першої категорії будуть повністю заборонені (приклади: ШІ, який використовується для віддаленої біометричної ідентифікації в режимі реального часу в громадських місцях або керовані ШІ системи оцінювання соціальних балів, а також моделі ШІ, які можуть використовувати підсвідомі методи впливу). Моделі високого ризику дозволені, але вони повинні будуть відповідати багатьом вимогам і пройти оцінку відповідності. Цю оцінку потрібно завершити до виходу моделі на ринок. Ці моделі також мають бути зареєстровані в створеній для них базі даних ЄС (приклади: моделі ШІ, пов'язані з функціонуванням критичної інфраструктури; системи, що використовуються в процесах найму чи рейтингу працівників, системи оцінки кредитоспроможності тощо). Решта моделей мають обмежений або мінімальний ризик. Від них вимагається дотримання прозорості, тобто користувач має бути проінформований, що те, з чим він взаємодіє, створене ШІ. Ці категорії включають в себе чат-ботів або системи штучного інтелекту, які створюють або обробляють зображення, аудіо чи відеовміст [5].

В США на федеральному рівні не існує законодавчого акту, який би комплексно регулював захист персональних даних користувачів онлайн платформ. Як виключення можна назвати Закон про захист конфіденційності дітей в Інтернеті (COPPA) 1998 року. COPPA вимагає від вебсайтів та онлайн-сервісів чіткої політики конфіденційності, що пояснює, яка інформація буде збиратися від дітей, як вони її

використовуватимуть і за яких обставин вони розкриватимуть її третім сторонам [6]. Однак ряд штатів прийняли власні закони щодо захисту персональних даних користувачів онлайн платформ на зразок європейського GDPR, а саме в Каліфорнії, Колорадо, Коннектикуті, Массачусетсі, Мериленді, Нью-Йорку та Вірджинії. Що ж стосується закону про ШІ, то в США також йде розробка комплексного закону, який би врегулював питання створення та використання штучного інтелекту. Окрім того, 30 жовтня 2023 року президент США видав Виконавчий наказ про безпечний, захищений і надійний штучний інтелект. Цей документ, зокрема, вимагає від розробників систем штучного інтелекту ділитися своїми результатами перевірок безпеки та іншою важливою інформацією з урядом США. Також цей наказ встановлює заборону використання ШІ для посилення дискримінації, упередженості та інших зловживань у сфері правосуддя, охорони здоров'я тощо [7].

У Китаї також немає жодного комплексного закону про захист даних в онлайн платформах. Натомість положення, що стосуються захисту особистої інформації та безпеки даних, є частиною складної системи та містяться в різних законах і постановах. Проте, трьома основними стовпами системи захисту персональної інформації в КНР є Закон про захист персональної інформації (PIPL), Закон про кібербезпеку (CSL) і Закон про безпеку даних (DSL) [8]. Як і в ЄС та США, в Китаї нема комплексного закону, який би врегулював питання створення та використання штучного інтелекту. Однак Китайська адміністрація з кіберпростору видала ряд законодавчих актів для регулювання окремих сфер ШІ, а саме: Положення щодо алгоритмованих рекомендацій, Положення щодо глибокого синтезу (діпфейк) та Положення щодо генеруючого ШІ [9, с. 2]. Положення встановлюють ряд вимог до онлайн платформ: реєстрація ШІ, проведення оцінювання безпеки штучного інтелекту, недопущення використання ШІ в маніпулятивних цілях та для забезпечення недобросовісної конкуренції, недопущення використання даних для навчання ШІ з незаконних джерел тощо [9, с. 5–11].

Отже, можна підсумувати, що питання правового регулювання створення та використання ШІ як загалом, так і безпосередньо в онлайн платформах в ЄС, США та Китаї частково вирішуються існуючими законами про захист особистих даних, а також вирішується створенням комплексних та окремих законів для безпосереднього регулювання створення та використання ШІ.

### **Література:**

1. 19 ways to use artificial intelligence in ecommerce. URL: <https://www.linnworks.com/blog/artificial-intelligence-in-ecommerce/>

2. Artificial Intelligence in eCommerce. URL: <https://www.altexsoft.com/ai-solutions-for-ecommerce/>.
3. Ethical Considerations in AI for Ecommerce. URL: <https://www.linkedin.com/pulse/ethical-considerations-ai-ecommerce-jheeva-subramanian>.
4. Штучний інтелект: проблеми та перспективи правового регулювання в Україні та ЄС. URL: <https://pravo.ua/shtuchnyi-intelekt-problemy-ta-perspektyvy-pravovoho-rehuliuвання-v-ukraini-ta-ies/>.
5. The EU AI Act: What it means for your business. URL: [https://www.ey.com/en\\_ch/forensic-integrity-services/the-eu-ai-act-what-it-means-for-your-business](https://www.ey.com/en_ch/forensic-integrity-services/the-eu-ai-act-what-it-means-for-your-business).
6. Children's Online Privacy Protection Rule ("COPPA"). URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>.
7. A step forward for AI regulation in the US. URL: <https://www.clydeco.com/en/insights/2023/11/a-step-forward-for-ai-regulation-in-the-us>.
8. Data protection law of China. URL: <https://www.dlapiperdataprotection.com/index.html?c=CN&t=law>.
9. China's New AI Regulations. *Latham & Watkins. Client Alert Commentary*. 2023. № 3110. P. 1-25. URL: <https://www.lw.com/admin/upload/SiteAttachments/Chinas-New-AI-Regulations.pdf>.