Цифрова трансформація

УДК 34:004 + 342.9.

ДУБНЯК М.В., *кандидат юридичних наук,* завідувач наукової лабораторії правового забезпечення цифрової трансформації, Наукового центру цифрової трансформації і права ДНУ "ІІБП" НАПрН України.
ORCID: https://orcid.org/0000-0001-7281-6568.

ПРАВОВІ ПІДХОДИ В ЗАКОНІ ЄС ПРО ШТУЧНИЙ ІНТЕЛЕКТ: ДОСВІД ДЛЯ УКРАЇНИ

DOI…

Анотація. *Ця стаття звертає увагу на ключові особливості гармонізованих правил щодо ШІ в ЄС (англ. – Artificial Intelligence Act, AIA). Аналізується поняття "систем штучного інтелекту" та підхід до визначення ризикових сфер застосування ШІ та інші особливості ШІ. Формуються перспективні напрямки для удосконалення законодавства України про штучний інтелект, зокрема в частині екосистеми даних та їх законного використання у системах ШІ (англ. – Artificial Intelligence, AI).*

Ключові слова: *штучний інтелект, правові підходи, AIA, Artificial intelligence Act, Цілі сталого розвитку, інформаційні технології, правова етика, екосистема даних, інформаційне право, правовий режим інформації, прогнозні висновки, база даних, основоположні права.*

Summary*. This article draws attention to the key features of the Laying down harmonised rules on Artificial Intelligence in the EU (Artificial Intelligence Act, AIA). The author analyzes the concept of "Artificial Intelligence Systems" and the approach to determining the risky areas of AI application and other features of the AIA. Promising directions for improving the Ukrainian legislation on artificial intelligence are being formed, in particular, in terms of the data ecosystem and their legal use in artificial intelligence systems.*

Keywords*: artificial intelligence, legal approaches, AIA, Artificial Intelligence Act, Sustainable Development Goals, information technology, legal ethics, data ecosystem, information law, legal regime of information, predictive conclusions, database, fundamental rights.*

Постановка проблеми. Технології штучного інтелекту (далі – ШІ) здатні покращувати прогнозування, оптимізувати операції і розподіл ресурсів. Це особливо важливо для компаній, які працюють в таких конкурентних секторах як: навколишнє середовище, зміна клімату, охорона здоров'я, наука, освіта та навчання, юстиція та правоохоронна діяльність, державний сектор, управління інфраструктурою, енергетика, транспорт, логістика, фінанси, сільське господарство. Однак ті самі елементи та методи, які забезпечують соціально-економічні переваги ШІ, також можуть спричинити нові ризики або негативні наслідки для окремих людей чи суспільства [3]. Останні роки ми спостерігаємо стрімкий приріст документів для регулювання ШІ. Вони охоплюють як технічні регламенти, так і стратегії, концепції впровадження ШІ, а також кодекси етичних практик розробки технологій.

У гострому питанні про правове регулювання ШІ кожна країна намагається зайняти першість. При цьому будь-які незбалансовані кроки у цьому напрямку можуть призвести до фрагментарного і обтяжливого регулювання, що обмежить галузь.

Технології ШІ використовують різні набори даних, застосовуються у різних сферах, можуть бути програмним забезпеченням чи вбудовуватись в окремі пристрої. Тому для окремих країн важко ефективно та самостійно впоратись із цим завданням. Фрагментовані національні нормативні акти неминуче призведуть до перешкод у безперебійній циркуляції товарів і послуг з ШІ.

Для повоєнної відбудови України корисно створити привабливе правове поле, що дозволить впровадити інноваційні рішення для відбудови інфраструктури та економіки України. Саме тому, аналіз правових підходів, запропонованих в гармонізованих правилах щодо ШІ в ЄС (англ. – Artificial intelligence Act, AIA) та Рамковій Конвенції Ради Європи, є актуальним дослідженням.

Результати аналізу наукових публікацій. Науковим підґрунтям для аналізу дефініції "штучний інтелект" були праці Баранова О.А. [1], Бєлякова К.І. [2]. Від часу публікації гармонізованих правил щодо ШІ в ЄС [3] з'явилось безліч аналітичних та наукових статей з детальним аналізом нових положень, це зокрема праці: Ebers, M., Hoch, V.R., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. [5] Bu Q. [7], Svantesson D.J. [11]. Наукові праці цих вчених дозволили нам дослідити проблему формування дефініції з урахуванням усіх складних, але істотних ознак технічного терміну "штучний інтелект". Раніше не вирішеною проблемою є питання правового регулювання даних, запропонованих у AIA у процесі розробки ШІ, тому фокус цієї роботи присвячений саме такому аналізу.

Метою статті є виявлення підходів правового регулювання даних для розробки ШІ та особливості захисту прав людини і формування законодавчих ініціатив щодо регулювання ШІ в Україні.

Завдання роботи: 1. Проаналізувати поняття "системи штучного інтелекту" в контексті їх нормативного закріплення та інші особливості AIA; 2. Виявити юрисдикційні підходи в AIA, порівняти їх з GDPR та описати можливі проблеми; 3. Проаналізувати ризики для основоположних прав людини та Цілей сталого розвитку у зв'язку із запропонованими підходами регулювання ШІ; 4. Сформувати законодавчі ініціативи для України з питань правового регулювання ШІ.

Виклад основного матеріалу. У Білій книзі ЄС про ШІ визначено європейські підходи для формування довіри до нього. Правове регулювання має заохочувати бізнес до розробки ШІ, а користувачі бути впевненими у достовірності висновків та рішень ШІ.

Правова основа ЄС щодо регулювання ШІ повинна бути: 1. орієнтована на людину; 2. забезпечувати безпечність розробки технології, що відповідає закону; 3.враховувати та формувати повагу до основних прав.

У процесі розробки AIA, первісно, пропонувалось декілька правових підходів:

1. добровільна схема маркування;
2. галузевий підхід – "ad-hoc" (з лат. – конкретне вирішення проблеми, а не широке застосування);
3. оцінка ризику;
4. оцінка ризику + кодекси поведінки для систем AI без високого ризику (отримав найбільше схвальних відгуків та пропозицій – *Авт.);*
5. обов'язкові вимоги для всіх систем ШІ, незалежно від ризику, який вони становлять (п.п. 3.3. AIA) [3];

У процесі громадського обговорення AIA було отримано понад 1200 пропозицій від: бізнес-компаній, фізичних осіб, академічних і дослідницьких установ, державних органів, громадянського суспільства, організацій захисту прав споживачів (п. 3.1 AIA

[3]). Нормативне регулювання не може описувати всі випадки для застосування усіх систем ШІ. Це особливо складно для динамічних, конкурентних і швидко масштабованих сфер, куди відносяться розробка і застосування ШІ.

Враховуючи попередньо сформовані Комісією етичні принципи розробки, розгортання та використання ШІ [4] і пов'язаних технологій, правовий підхід ЄС ґрунтується саме на оцінці ризиків.

Аналіз поняття "система штучного інтелекту" і його значення для правового регулювання.

AIA не містить визначення "штучний інтелект", у Преамбулі акту є загальне описання ШІ як *"сімейства технологій, що швидко розвивається, і може сприяти отриманню широкого спектру економічних і суспільних переваг у всіх галузях промисловості та соціальної діяльності"*.

Описано сфери покращення всіх видів управлінської діяльності "ш*ляхом 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 для компаній і підтримувати соціальні та екологічні результати"* (п. 3 AIA).

У статті 3 (1) AIA є технологічно нейтральне визначення ***"система штучного інтелекту***" – означає програмне забезпечення, яке розроблено з використанням однієї або кількох технік і підходів, перелічених у Додатку I, зокрема:

(a) підходи до машинного навчання: контрольоване, неконтрольоване та навчання з підкріпленням, з використанням різноманітних методів, у тому числі глибокого навчання;

(b) підходи, що ґрунтуються на логіці та знаннях, включаючи представлення знань, індуктивне (логічне) програмування, бази знань, механізми логічного висновку та дедуктивні механізми, (символічні) міркування та експертні системи.

(c) статистичні підходи, байєсівське оцінювання, пошук і методи оптимізації (Додаток I, AIA – *Авт*.); і може, для заданого набору визначених людиною цілей, генерувати результати, такі як вміст, прогнози, рекомендації або рішення, що впливають на середовища, з якими вони взаємодіють [3].

Хоча це визначення "систем штучного інтелекту" можна вважати широким, його практична доречність сумнівна. Ключовою особливістю AIA є його визначення ризиків застосування ШІ у високоризикових сферах та визначення категорії трьох ризиків: неприйнятний ризик; високий ризик; низький або мінімальний ризик.

Отже, визначення "системи штучного інтелекту" ґрунтується на:

1. ключових функціональних характеристиках програмного забезпечення, зокрема, на здатності, для заданого набору визначених людиною цілей, генерувати результати, такі як вміст, прогнози, рекомендації або рішення, які впливають на середовище, з яким система взаємодіє, будь то у фізичному чи цифровому вимірі;

2. системи ШІ можуть бути розроблені з різними рівнями автономії;

3. системи ШІ можуть бути вбудовані (фізично інтегровані) та не вбудовані в продукт (обслуговує функціональні можливості).

4. визначення пов'язано із конкретним переліком методів та підходів розробки ШІ, які описані в окремому Додатку I.

Багато хто асоціює термін "штучний інтелект" з методом "машинного навчання", а не з простими процесами автоматизації, у яких виконуються заздалегідь запрограмовані правила відповідно до логічних міркувань. Визначення ШІ в "широкому значенні"

актуальне для охоплення заборонених практик і охорони основних прав і свобод (див. Табл. 1). Однак це визначення, як і Регламент в цілому, не встановлює цивільної відповідальності для постраждалих громадян від таких заборонених практик (підсвідомі маніпуляції, експлуатація вразливості, соціальна оцінка або віддалена біометрична ідентифікація).

Обов'язкові вимоги до розробки високоризикового ШІ (Розділ ІІІ, Глава 2, AIA [3]) засновані на спостереженні, що на фундаментальні права негативно впливають, особливі характеристики машинного навчання. Наприклад, такі як непрозорість, складність, залежність від даних, автономна поведінка. В заснованих на логіці алгоритмах ці характеристики або відсутні, або частково присутні. Тому широке визначення ШІ потенційно призводить до надмірного регулювання [5, с. 590].

Технологічна нейтральність визначення "систем штучного інтелекту", простежується у підході, за яким, методи розробки ШІ винесені в окремий Додаток І, а не перераховані в самій дефініції в статті 3(1) AIA. Це додає варіативності правовому регулюванню, адже Додаток І, може бути доповнений новими підходами і техніками.

Заборонені практики застосування штучного інтелекту.

У статті 5 AIA визначає чотири різні типи заборонених практик ШІ, оскільки вони суперечать цінностям ЄС або порушують основні права:

1. (a) системи штучного інтелекту, які використовують підсвідомі методи впливу на людину, щоб суттєво спотворити поведінку людини таким чином, що спричиняє або може спричинити фізичну чи психологічну шкоду цій особі чи іншій особі;

(b) системи штучного інтелекту, які використовують будь-яку вразливість певної групи осіб через їхній вік, фізичні чи розумові вади, щоб суттєво спотворити поведінку особи, що належить до цієї групи, таким чином, завдає або може завдати цій особі чи іншій особі фізичної чи психологічної шкоди.

(c) заборона на загальну соціальну оцінку системами AI державними органами.

(d) використання систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних місцях пов'язаних з діяльністю правоохоронних органів, крім таких:

(i) пошук потенційних жертв злочинів, у тому числі зниклих дітей;

(ii) запобігання безпосередній загрозі життю, безпеці фізичних осіб, терористичного акту;

(iii) виявлення, локалізація, ідентифікація або судове переслідування злочинця або підозрюваних у вчиненні кримінальних правопорушень, які караються вироком у вигляді позбавлення волі або ордером на затримання не менше трьох років [3].

Застосування ШІ на підставі п. (d) дозволяється за умови врахування характеру ситуації, наслідків використання систем з ШІ для громадян, обмеження в застосуванні систем ШІ у часі та просторі, з урахуванням доказів та загроз, отримання судового дозволу або відповідного адміністративного органу, крім випадків термінових дій (п.п 21, 22 Преамбули AIA [3]).

У контексті заборони "біометричної ідентифікації у реальному часі", п. (d), варто відзначити низку прогалин. Саме по собі очікування "бути ідентифікованим у публічному місці" можуть спричинити жахливі наслідки для здійснення основних прав і свобод [7, с. 125-126]. Європейський інспектор із захисту даних зазначає, що "необхідний більш суворий підхід, враховуючи, що віддалена біометрична ідентифікація представляє надзвичайно високі ризики глибокого та недемократичного втручання в приватне життя людей" [8].

В АІА є заборона практик “соціальної оцінки” державними органами, однак немає заборони використання таких же систем приватними організаціями. Розвиток та розгортання систем цифрових технологій здебільшого здійснюється приватним сектором. Тому ризик використання практик “соціальної оцінки” у приватних компаній вищий, ніж у державних органів. Тому заборона повинна застосовуватися до всіх випадків використання біометричних систем ШІ – як державних, так і приватних і така заборона має поширюватися на всі подібні системи ШІ [5, с. 592].

Системи штучного інтелекту високого ризику.

Щоб класифікувати систему ШІ як високоризикову, необхідно визначити (1) її цільове призначення, (2) тяжкість можливої шкоди та (3) ймовірність заподіяння шкоди. АІА стосується двох категорій ШІ високого ризику: систем ШІ, як компонентів безпеки продуктів; та систем ШІ, що мають наслідки для основних прав, і використовуються у сферах, перерахованих у Додатку ІІІ (Табл. 1).

Таблиця 1.
Високоризикові сфери застосування систем ШІ
(Сформовано Авт. з урахуванням п. 32-40, додатку ІІІ АІА, Хартії ЄС про основоположні права [6]*).*

Сфера	**Призначення систем та опис ризику**	**Які основні права порушує**
Дистанційна біометрична ідентифікація фізичних осіб в “реальному часі”	Необ’єктивні результати встановлення особи, можлива дискримінація, безпідставне використання чутливих персональних даних.	Ст. 7. Повага до приватного та сімейного життя. Ст. 8. Захист персональних даних.
Управління, експлуатація критичної інфраструктури.	Несправність систем ШІ у сферах: управління та експлуатації дорожнього руху, постачання води, газу, опалення та електроенергії, може завдати шкоди у великих масштабах.	Ст. 6. Право на безпеку. Ст. 37. Охорона навколишнього середовища Ст. 38. Захист споживачів.
Освіта та професійне навчання.	Можуть вплинути на професійний хід життя людини та здатність забезпечувати засоби до існування. Системи ШІ можуть підтримувати історичні моделі дискримінації.	Ст. 14. Право на освіту, професійну підготовку та підвищення кваліфікації. Ст. 21. Недопущення дискримінації.
Працевлаштування, управління працівниками, доступ до зайнятості.	Найм, підбір працівника, прийняття рішень щодо просування по службі чи звільнення, розподіл завдань, моніторинг чи оцінка особи у трудових відносинах впливає на кар’єрні перспективи. Можливі історичні моделі дискримінації, наприклад щодо жінок, вікових груп, осіб з обмеженими можливостями, осіб певного расового чи етнічного походження або сексуальної орієнтації.	Ст. 15. Свобода вибору професії та право на працю. Ст. 21. Недопущення дискримінації. Ст. 27. Право робітників на інформацію та консультації в межах підприємства. Ст. 30. Захист у разі невиправданого звільнення.

		Ст. 31. Справедливі умови праці.
Приватні та державні послуги.	Системи ШІ можуть застосовуватись для визначення питань про надання, відмову, зменшення чи скасування послуги. Це призводить до обмеження повноцінної участі в житті суспільства або підвищення рівня життя, і користування наданими правами та гарантіями.	Ст. 1. Людська гідність. Ст. 34. Соціальне забезпечення та допомога. Ст. 36. Доступ до послуг загального економічного значення. Ст. 41. Право на якісне управління. Ст. 47. Право на ефективний засіб правового захисту та на справедливий судовий розгляд.
Диспетчеризація та встановлення пріоритету служб першого реагування.	Системи ШІ, які застосовуються для реагування на надзвичайні ситуації, стихійні лиха, катастрофи можуть прийняти невірне рішення у дуже критичній ситуації для життя,здоров'я людей та їх майна.	Ст. 6. Право на безпеку. Ст. 17. Право власності. Ст. 37. Охорона навколишнього середовища.
Кредитування	Системи ШІ, які застосовуються для оцінки кредитного рейтингу або кредитоспроможності фізичних осіб, можуть призвести до необ'єктивного оцінювання, позбавлення ресурсів та дискримінації за майновою чи іншою ознакою.	Ст. 21. Недопущення дискримінації.
Дії правоохоронних органів	Дисбаланс у застосуванні може призвести до стеження, арешту або позбавлення волі фізичної особи.	Ст. 47. Право на ефективний засіб правового захисту та на справедливий судовий розгляд. Ст. 49. Принципи законності та пропорційності кримінальних правопорушень та покарань
Податкові та митні органи	Використовуються з метою запобігання, виявлення, розслідування та переслідування кримінальних правопорушень.	
Управління міграцією, надання притулку, прикордонний контроль.	Використовуються у системах для виявлення емоційного стану фізичної особи; для оцінки ризиків, пов'язаних з фізичними особами, які в'їжджають на територію держави-члена або звертаються за візою чи притулком; для перевірки достовірності документів; при розгляді заяв про надання притулку, візи та дозволів на проживання та пов'язаних із ними скарг з метою встановлення відповідності фізичних осіб, які звертаються за відповідним статусом.	Ст. 7. Повага до приватного та сімейного життя. Ст. 8 Захист персональних даних. Ст. 45. Свобода пересування та проживання. Ст. 46. Дипломатичний та консульський захист. Ст. 47. Право на ефективний засіб правового захисту та на справедливий судовий розгляд.

Правосуддя та демократичні процеси	Застосовується у системах для усунення ризиків потенційних упереджень, помилок і непрозорості, призначені для допомоги судовим органам у дослідженні та тлумаченні фактів і закону, а також у застосуванні закону до конкретної сукупності фактів.	Значний вплив на демократію, верховенство права, особисті свободи, а також ст. 47. Право на ефективний засіб правового захисту та на справедливий судовий розгляд.

Захист основоположних прав та вплив на досягнення Цілей сталого розвитку.

Застосування технологій ШІ має специфічні прояви та впливає на права людей. Наприклад, непрозорість, складність, залежність від даних – призводить до порушення законодавства про захист даних та права на приватність.

Вирішуючи цю проблему в AIA передбачено набір вимог щодо надійного ШІ та пропорційних зобов'язань для всіх учасників ланцюга створення вартості.

Крім захисту та реалізації прав передбачених Хартією ЄС про основоположні права [6] ми бачимо взаємозв'язок із Цілями сталого розвитку (далі – ЦСР) [9], зокрема:

- віднесення до високоризикових сфер застосування технологій ШІ в освіті, професійному навчанні буде сприяти забезпеченню ЦСР 4 (якісна освіта), для сфери працевлаштування і управління кадрами, доступ до зайнятості – ЦСР 8 (гідна праця та економічне зростання);
- вимоги до наборів навчальних даних, та процедури їх розкриття спрямовані на недопущення дискримінації та ЦСР 5 (гендерну рівність);
- врахування високих ризиків застосування ШІ при визначенні пріоритету служб першого реагування та управлінні критичною інфраструктурою багато в чому буде заохочувати до належних практик та досягнення ЦСР 9 (інновації та інфраструктура) та ЦСР 11 (сталий розвиток міст та спільнот).

Правовий підхід в регулюванні ШІ – це не лише права людини та етичні цінності, це більше глобальні цілі, такі як, зміна клімату та сталість. Серед основних зобов'язань можемо відзначити статтю про обов'язок постачальника повідомляти про будь-який серйозний інцидент або будь-який збій у роботі цих систем (ст. 62 AIA).

Сфера дії та юрисдикційні особливості AIA.

Аналізуючи правові підходи, описані в AIA, ми помітили суттєву схожість з Загальним регламентом про захист даних (GDPR) [10]. Обидва акти підтверджують позицію ЄС на лідерство в регулюванні інноваційних сфер.

Спільні риси:

1. Потенціал стати інструментом, який встановлює міжнародні стандарти регулювання ШІ.

Після прийняття GDPR декілька країн повністю оновили усю систему захисту персональних даних. Багато бізнесів змінили внутрішні процедури обробки даних, щоб відповідати вимогам і стандартам GDPR. Враховуючи, що AIA є одним із перших, що встановлює правила доступу систем ШІ до ринку ЄС, його будуть наслідувати багато країн та компаній.

2. Екстериторіальна дія положень AIA через суб'єктність учасників.

Регламент застосовується до:

(a) постачальників, які розміщують на ринку або вводять в експлуатацію системи ШІ в Союзі, незалежно від того, чи розташовані ці постачальники в Союзі чи в третій країні;

(b) користувачі систем ШІ, розташовані в межах Союзу;

(c) постачальники та користувачі систем ШІ, які розташовані в третій країні, де результати, створені системою ШІ, використовуються в Союзі.

Згідно з визначенням у статті 3 (2) AIA, термін "постачальник" означає – *фізичну або юридичну особу, державний орган, установу чи інший орган, який розробляє (або має) систему штучного інтелекту з метою розміщення її на ринку, або введення його в експлуатацію під власним ім'ям або торговою маркою, платно чи безкоштовно*.

Стаття 3(9) AIA, визначає "розміщення на ринку" як – *перший доступ до системи ШІ на ринку Союзу* [3] .

Дефініцію "введення в експлуатацію" визначено у статті 3(11) AIA. Це стосується – *постачання системи ШІ для першого використання безпосередньо користувачеві або для власного використання на ринку Союзу за призначенням.*

З цього положення прямо не видно взаємозв'язку із попереднім терміном "введення в експлуатацію". Якщо технологія буде доступна через мережу Інтернет, як більшість користувацьких генеративних ШІ-технологій (GPT, DALLie тощо) це буде тлумачитись як "введення в експлуатацію" чи "розміщення на ринку". Припустимо, що "розміщення на ринку" має в собі економічний та комерційний критерій, а "введення в експлуатацію" – критерій "використання за призначенням". Ці два поняття не визначають чітких меж їх тлумачення. Тому будуть проблеми у правозастосовній практиці.

Стосовно статусу "постачальника" існує також вимога "локалізації представництва". Зокрема, стаття 25(1) AIA визначає – *перш ніж зробити свої системи доступними на ринку Союзу, якщо імпортера неможливо ідентифікувати, постачальники, засновані за межами Союзу, повинні за письмовим дорученням призначити уповноваженого представника, заснованого в Союзі* [3]. І на практиці це може виявитись досить проблематичним.

По-перше – "локалізація представництва" є явно обтяжливою вимогою для всіх іноземних компаній. По-друге, незрозуміло як ЄС буде контролювати цю вимогу у процесі великої масштабованості постачальників ШІ-ринку. Це призведе до порушення умов конкуренції і доступу до ринку. Будуть компанії, які можуть понести такі операційні витрати і залишитись в правовому полі, і компанії, які будуть порушувати вимоги і працювати "з тіні".

По-третє, якщо країни, що розвиваються, скопіюють в свої національні законодавства положення про "локалізацію", виникає питання: чи будуть великі компанії "локалізовувати" своїх представників у кожній країні? Звідси бачимо узаконену економічну нерівність, адже для входу на "розвинутий ринок ЄС" компанії з країни з менш розвинутою економікою одразу опиняються у нерівних і надмірно обтяжливих умовах, у порівнянні з іншими країнами [11].

"Користувач" означає – *будь-яку фізичну або юридичну особу, державний орган, агентство чи інший орган, який використовує систему ШІ під своїм керівництвом, за винятком випадків, коли система* AI *використовується під час особистої непрофесійної діяльності* [3]. Тобто правові гарантії щодо застосування систем ШІ у сфері особистої непрофесійної діяльності на користувачів не поширюються.

Найскладнішим випадком для правової інтерпретації підстав застосування AIA є фраза "результати, створені системою, використовуються в Союзі". Це положення розширює сферу дії AIA на будь-яких постачальників і користувачів систем ШІ, розташованих у третіх країнах, якщо вони виробляють будь-яку форму для застосування ШІ, яка використовується в ЄС.

Обґрунтування цього положення очевидне – воно спрямоване на уникнення ситуацій, коли організації в межах ЄС передають завдання суб'єктам за межами ЄС, щоб обійти AIA і отримати вигоду від результатів систем ШІ.

Зважаючи на цифровий характер, певні системи ШІ повинні підпадати під дію цього Регламенту, навіть якщо вони не розміщені на ринку, не введені в експлуатацію та не використовуються в Союзі. Це, наприклад, випадок оператора, заснованого в Союзі, який укладає певні послуги з оператором, заснованим за межами Союзу, щодо діяльності, яка буде виконуватися системою ШІ, яка кваліфікуватиметься як високоризикова, а наслідки її використання впливатимуть на фізичних осіб, які знаходяться в Союзі. За таких обставин система ШІ, яка використовується оператором за межами Союзу, може обробляти дані, законно зібрані в Союзі та передані з нього, і надавати оператору-підряднику в Союзі результати цієї системи ШІ, отримані в результаті такої обробки (п. 11 AIA [3]).

Незважаючи на всю логічність та виправданість цього підходу, виникає зауваження, аналогічне до екстериторіальної дії положень GDPR. У випадку з GDPR широко використовується доктрина "ефектів" – *(застосовується для охоплення іноземців за кордоном, чия поведінка відбувається за межами держави-резидента, але має наслідки для держави, що виконує рішення),* принцип пасивної правосуб'єктності – (*застосовується юрисдикція держави, де суб'єкт здійснює свою діяльність*) або навіть принцип об'єктивної територіальності – *(застосовується юрисдикція держави, в якій має місце результат діяльності*).

Встановлення цих критеріїв, допоможе отримати принаймні 3 переваги: сфера застосування акта, легітимність вимог юрисдикції, чітка міжнародна державна практика з цих питань [11].

Очікується, що використання ШІ буде супроводжуватись практиками прозорості і зобов'язанням розкривати інформацію про те, що контент створено за допомогою автоматизованих засобів, зокрема, для систем:

1. які взаємодіють з людьми;
2. використовуються для виявлення емоцій або визначення зв'язку з (соціальними) категоріями на основі біометричних даних;
3. генерують або маніпулюють вмістом ("глибокі фейки").

Таке інформування дозволить людям зробити усвідомлений вибір або відступити від певної ситуації (п. 5.2.4. AIA). Для підтвердження відповідності вимог AIA, системи ШІ високого ризику повинні мати маркування CE (п.67 AIA), та зареєструвати систему ШІ в спеціальній базі даних ЄС (п. 69 AIA) [3].

Правові підходи до формування екосистеми даних.

Системи ШІ з високим рівнем ризику, які використовують дані для навчання мовних моделей, мають бути розроблені на основі навчальних даних, які відповідають критеріям якості. Зокрема, практикам керування даними (ст. 10 AIA), обліку, документування та зберігання записів (ст. 12 AIA), прозорості та надання інформації користувачам (ст. 13 AIA), людського нагляду (ст. 14 AIA), надійності, точності та кібербезпеки (ст. 15 AIA) [3].

Практика управління даними стосується таких етапів: (a) відповідні варіанти дизайну; (b) збір даних; (c) відповідні операції обробки даних з підготовки, такі як анотація, маркування, очищення, збагачення та агрегація; (d) формулювання відповідних припущень, зокрема щодо інформації, яку дані повинні вимірювати та представляти; (e) попередня оцінка наявності, кількості та придатності необхідних

наборів даних; (f) експертиза на можливі упередження; (g) визначення будь-яких можливих прогалин або недоліків даних, а також способів усунення цих прогалин і недоліків (ст. 10(2), AIA [3]).

Проаналізуємо детальніше п. (f) – "експертиза на можливі упередження". AIA не надає дефініцію терміну "упередження", що ускладнює його розуміння. Це може спричинити конфлікти серед постачальників ШІ, оскільки вони не знатимуть які заходи застосовувати для запобігання або мінімізації упередженості чи дискримінації. Для постачальників також проблематично подати технічну документацію, у якій мають продемонструвати, критерії тестування навчальних наборів даних на "упередженість" (для виконання вимоги додатку IV AIA про технічну документацію, яка включає загальний опис системи та детальний опис процесу розробки елементів ШІ).

Стаття 10(3) AIA містить положення про те, що – *набори навчальних даних для валідації та тестування мають бути відповідними, репрезентативними, без помилок і повними. Вони повинні мати відповідні статистичні властивості, у тому числі, щодо осіб або груп осіб, щодо яких планується використовувати систему ШІ високого ризику*. Ці характеристики наборів даних можуть відповідати на рівні окремих наборів даних або їх комбінації.

Такий рівень досконалості даних технічно неможливий і також може перешкоджати інноваціям. Отже, AIA мав би вимагати від постачальників вжиття заходів для достовірності наборів даних, а не розкриття інформації про самі набори даних. Адже навчальні набори даних є комерційною цінністю компаній розробників ШІ.

AIA описує кілька методів підвищення конфіденційності таких як, псевдонімізація, шифрування, анонімізація (ст. 10(5) AIA) [3]. Це робить дані не вільними від "помилок", хоча це допомагає у захисті конфіденційних даних.

Положення AIA вимагають надавати детальний опис елементів системи ШІ та процесу її розробки:

(d) вимоги до даних у формі таблиць даних, що описують методології та методи навчання, використані набори навчальних даних, включаючи інформацію про походження цих наборів даних, їх обсяг і основні характеристики; як дані були отримані та відібрані; процедури маркування (наприклад, для контрольованого навчання), методології очищення даних.

(g) використані процедури валідації та тестування, включаючи інформацію про використані дані валідації та тестування та їхні основні характеристики; показники, які використовуються для вимірювання точності, надійності, кібербезпеки та відповідності іншим відповідним вимогам, а також потенційно дискримінаційного впливу; журнали випробувань та всі звіти про випробування, датовані та підписані відповідальними особами (вимоги до технічної документації ст. 11, та додаток 4, AIA [3].

На практиці вимога "повного розкриття даних і документації для органів ринкового нагляду" щодо навчання, перевірки і тестування наборів даних (ст. 64(1) AIA може бути декларативним і обмежуючим положенням для інноваційної діяльності. Це пояснюється тим, що деякі системи ШІ можуть бути створені з використанням наборів даних, яких не існує як навчального набору даних в розумінні AIA. Або системи ШІ, які не використовували централізовані набори даних. Наприклад, розвиток ШІ через інтегроване, спільне навчання (англ. – Federated Learning, FL) є підтипом машинного навчання (англ. – machine learning, ML), яке використовується розробниками для навчання ШІ моделей без централізованого збору даних. FL залишає дані там, де вони є, розподілені між численними пристроями та серверами [12]. Це означає, що ці системи ШІ не завжди можуть продемонструвати відповідність вимогам до набору даних згідно

зі ст. 10 AIA, генерувати централізовані журнали як вимагається в ст. 12 AIA, або надати прямий доступ до наборів даних згідно зі ст. 64 AIA [3].

Крім того, вимога щодо надання доступу до даних має враховувати акти ЄС, такі як GDPR, які встановлюють обмеження щодо строків та обсягу зберігання даних (наприклад через принцип мінімізації (ст. 5(c) GDPR [10]).

Зобов'язання надавати вихідний код систем ШІ з високим рівнем ризику за вмотивованим запитом до органів ринкового нагляду (ст. 64(2) AIA також є проблематичним, оскільки, вихідний код може бути захищений Директивою ЄС про комерційну таємницю [13] та Директивою про комп'ютерні програми [14].

AIA не в змозі визначити критерії для вимірювання якості наборів навчальних даних наприклад, прогнозна точність, надійність, справедливість навчених моделей машинного навчання.

Очікується, що для формування високоякісних наборів даних в ЄС створено Європейські спільні простори даних для обміну даними між підприємствами та урядом. Наприклад, Європейський простір даних про охорону здоров'я сприятиме недискримінаційному доступу до даних про охорону здоров'я та навчанню алгоритмів штучного інтелекту на цих наборах даних у безпечний, своєчасний, прозорий та надійний спосіб, із збереженням конфіденційності та з відповідним інституційним управлінням.

Законодавчі ініціативи для правового регулювання ШІ в Україні.
1. В частині удосконалення дефініції "штучний інтелект"

Таблиця 2.

Порівняльно-правовий аналіз дефініцій "штучний інтелект"

Концепція розвитку штучного інтелекту в Україні № 1556-р	**AIA**
Штучний інтелект – (1) *організована сукупність інформаційних технологій*, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання (2) *системи наукових методів досліджень* і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також (3) *створювати та використовувати власні бази знань*, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань[*] [15; 16].	**Система штучного інтелекту** – означає (1) *програмне забезпечення,* яке розроблено з використанням однієї або кількох технік і підходів, (2) перелічених у Додатку I, і може, (3) *для заданого набору визначених людиною цілей*, генерувати результати, такі як вміст, прогнози, рекомендації або рішення, що впливають на середовища, з якими вони взаємодіють.
Коментар *Авт.:* 1. Сукупність інформаційних технологій – охоплює широке коло об'єктів. 2. Не визначено конкретних систем і методів наукового дослідження. 3. Фокус на автономію вирішення завдань.	Коментар *Авт.*: 1. "Програмне забезпечення" – не охоплює інших технологій. 2. Описані найпопулярніші технології і підходи для розробки технологій ШІ в окремому Додатку I. 3. Мету і цілі діяльності ШІ визначає людина.

[*] У Державній цільовій науково-технічній програмі з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року [16] використано ту саму дефініцію поняття штучний інтелект

2. В частині формування системи понятійного апарату.

У Концепції № 1556-р визначено, що *"штучний інтелект може створювати та використовувати власні бази знань"*. Дефініції і правового режиму такої "бази знань" у Концепції № 1556-р [15] не розкрито. Закон України "Про інформацію" [17], як базовний нормативний акт у сфері створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації також не містить поняття "база знань".

Закон України "Про авторське право і суміжні права" містить дефініцію "база даних" (компіляція даних) – *сукупність творів, даних або будь-якої іншої інформації у довільній формі, що розташовані у систематизованому або упорядкованому вигляді..."*. Відповідно до ст. 21 цього ж закону *"бази даних (компіляції даних) охороняються авторським правом, якщо вони за добором та/або упорядкуванням їх складових частин є результатом творчої діяльності"* [18]. Відтак бази знань створені ШІ є результатом застосування наукових методів, підходів та алгоритмів, а не результатом творчої діяльності. Тому ми говоримо про інший, самостійний об'єкт правової охорони, який заслуговує на самостійне правове закріплення, і не підпадає під правове регулювання "бази даних" (компіляції) в розумінні Закону України "Про авторське право і суміжні права".

Натомість, AIA визначає широкий спектр вимог до "навчальних наборів даних". Крім того стаття 3 AIA містить такі важливі поняття як: дані перевірки, дані тестування, вихідні дані. Також перелік дій, який формує поняття "підготовка даних" це анотація, маркування, очищення, збагачення та агрегація. Ці поняття охоплюють життєвий цикл створення технології ШІ і необхідні для здійснення різних етапів контролю. Тому їх правове закріплення є важливим елементом удосконалення законодавства.

Крім того, потребують правового визначення такі категорії даних, які формуються в результаті роботи технологій ШІ – згенеровані дані, прогнозні дані (прогнозні висновки) прогнозні рішення, рекомендаційні дані.

3. В частині системного правового регулювання.

За 2024 рік було прийнято низку нормативних документів в частині правового регулювання ШІ. Ці акти містять як інноваційні положення, так і недоліки, які будуть ускладнювати розробку інноваційних технологій. Можна точково запозичувати необхідні правові підходи та вносити зміни в численні нормативні акти, які регулюють цифрову економіку. Однак на наш погляд, з урахуванням кращих світових практик, які вже існують, і з'являться в найближчому майбутньому, доцільніше працювати над розробкою окремого Закону України "Про штучний інтелект" і паралельно удосконалювати інформаційне законодавство щодо екосистем даних.

Висновки.

1. AIA декларує технологічно нейтральне визначення "систем штучного інтелекту", однак не надає дефініції "штучний інтелект". В національному законодавстві дефініція "штучний інтелект" охоплює сукупність інформаційних технологій, орієнтована на автономію роботи ШІ, проте не містить переліку методів та підходів розробки. "Система штучного інтелекту" в розумінні AIA призначена для виконання цілей та функцій, які задає людина.

2. Юрисдикційні підходи в AIA, так само як і в GDPR, описано дуже широко. В AIA сфера дії акту пов'язана із суб'єктним складом і місцем діяльності "постачальника", "користувача", та використання результатів роботи ШІ в Союзі. Останній критерій застосування AIA є найважчим для практичного розуміння, оскільки,

AIA не описує, яким саме чином відстежити факт “використанні результатів роботи ШІ” в Союзі. Вимога до “локалізації представництва” формує ризик економічної нерівності. Адже виконання цієї умови, надмірно обтяжлива для країн, з менш розвинутою економікою, малих бізнесів, та стартапів.

3. Визначення високоризикових сфер застосування ШІ, таких як освіта, працевлаштування, недопущення дискримінації, управління критичною інфраструктурою сприятиме досягненню ЦСР 4 (якісна освіта), ЦСР 8 (гідна праця та економічне зростання), ЦСР 5 (гендерну рівність), ЦСР 9 (інновації та інфраструктура) та ЦСР 11 (сталий розвиток міст та спільнот). Загалом однією із цілей AIA є повага до законодавства про основні права та цінності Союзу.

4. Законодавчі ініціативи для України згруповані у три напрямки – удосконалення дефініції “штучний інтелект” (1); формування понятійного апарату у сфері даних – “дані перевірки”, “дані тестування”, “вихідні дані”. Поняття та операції у сфері “підготовки даних” це “анотація”, “маркування”, “очищення”, “збагачення”, “агрегація”. Поняття даних, які формуються в результаті роботи технологій ШІ – “згенеровані дані”, “прогнозні дані” (прогнозні висновки) “прогнозні рішення”, “рекомендаційні дані” (2); формувати законодавство на базі системного підходу — шляхом прийняття окремого Закону України “Про штучний інтелект” (3).

Використана література

1. Баранов О.А. Інтелект штучний. *Енциклопедія соціогумагітарної інформології* / корд. проекту та заг. ред. проф. К.І. Бєляков. Київ: Видавничий дім “Гельветика”, 2021. Т. 2. С. 114-121.

2. Oleksandr Kostenko, Konstantin Bieliakov, Oleksandr Tykhomyrov, Irina Aristova “Legal personality” of artificial intelligence: methodological problems of scientific reasoning by Ukrainian and EU experts. *AI & SOCIET*. DOI: https://doi.org/10.1007/s00146-023-01641-0.

3. Regulation of the European Parliament and of the Council Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. Com(2021) 206 final 2021/0106(COD). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206#footnoteref45

4. Ethics guidelines for trustworthy AI (2019) URL: https://web.archive.org/web/20200226023934/https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

5. Ebers M., Hoch V.R., Rosenkranz F., Ruschemeier H., Steinrötter B. (2021).The European Commission’s Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). 4(4), 589-603. URL: https://doi.org/10.3390/j4040043

6. The Charter of Fundamental Rights of the European Union № 2016/C 202/02. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016P/TXT

7. Bu Q. (2021) The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *Int. Cybersecur. Law Rev*, 2, 113-145.

8. Закон про штучний інтелект: позитивна ініціатива, але заборона віддаленої біометричної ідентифікації в публічному просторі необхідна. – (Прес-реліз, 23 квітня 2021 р.) URL: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

9. Sustainable Development Goals. URL: https://www.undp.org/ukraine/sustainable-development-goals

10. Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation). URL:https://eur-lex.europa.eu/eli/reg/2016/679/oj

11. Svantesson D.J. (2021). The European Union Artificial Intelligence Act: Potential implications for Australia. *Alternative Law Journal*, 47, 4-9.

12. Kairouz Peter; McMahan H. Brendan; Avent Brendan and others (2021). "Advances and Open Problems in Federated Learning". *Foundations and Trends in Machine Learning.* 14 (1–2): 1–210. arXiv:1912.04977. DOI:10.1561/2200000083. ISSN 1935-8237.

13. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) URL:https://eur-lex.europa.eu/eli/dir/2016/943/oj

14. Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31991L0250

15. Концепція розвитку ШІ в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

16. Концепція Державної цільової науково-технічної програми з використання технологій ШІ в пріоритетних галузях економіки на період до 2026 року: Розпорядження Кабінету Міністрів України від 13.04.24 р. № 320-р. URL: https://www.kmu.gov.ua/npas/pro-skhvalennia-kontseptsii-derzhavnoi-tsilovoi-naukovo-tekhnichnoi-prohramy-z-vykorystannia-s320130424

17. Про інформацію: Закон України від 27.07.23 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#n18

18. Про авторське право і суміжні права: Закон України від 15.04.23 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~