## Перспективи правового регулювання використання ШІ:

# Практичні орієнтири для науковців України

Провідна професіоналка з інтелектуальної власності УКРНОІВІ

**Юліана Зух-Кіпріянова**

IP OFFICE
Ukrainian National Office for Intellectual Property and Innovations

# Регулювання використання ШІ.

01.

**Яка ситуація в Україні?**

02.

**Яка ситуація в ЄС?**

03.

**Які переспективи для України?**

# В Україні

Наразі спеціальне регулювання використання ШІ в науці відсутнє?

## Концепція розвитку штучного інтелекту в Україні

одне із завдань: “сприяння застосуванню технологій штучного інтелекту за напрямами науки, а також міждисциплінарні дослідження на перетині галузі штучного інтелекту та інших галузей науки”.

## План заходів на 2025–2026 роки

передбачає “розроблення і подання Кабінетові Міністрів законопроєкту щодо правового врегулювання у сфері розвитку ШІ у IV кварталі 2026 року”.

## Біла книга і Дорожня карта

описують поетапний підхід до майбутнього регулювання, орієнтований на підготовку до закону аналога AI Act, добровільні кодекси поведінки, рекомендації та інші підготовчі інструменти.

## ЗУ «Про авторське право і суміжні права»

встановлює право sui generis на неоригінальні об’єкти, згенеровані комп’ютерною програмою, строком на 25 років. (ст.33)

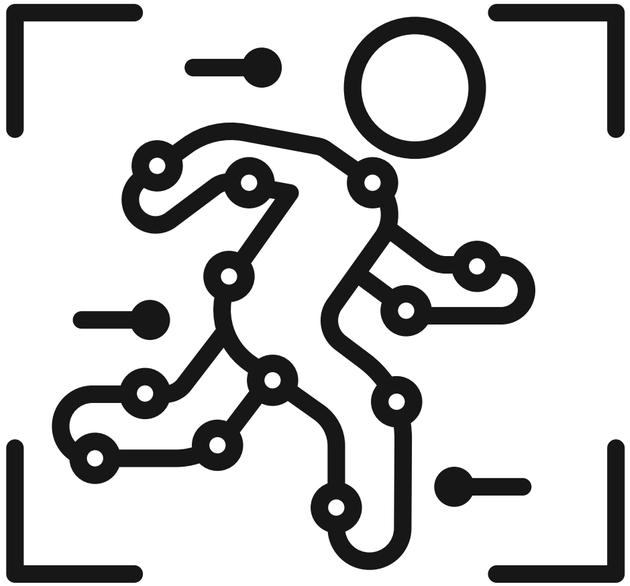
# Законодавча база: Мінцифри розробляється національний закон про ШІ

**Що може змінити майбутній закон:**

**1. Класифікація систем:** розподіл ШІ на рівні ризику (неприйнятний, високий, обмежений).

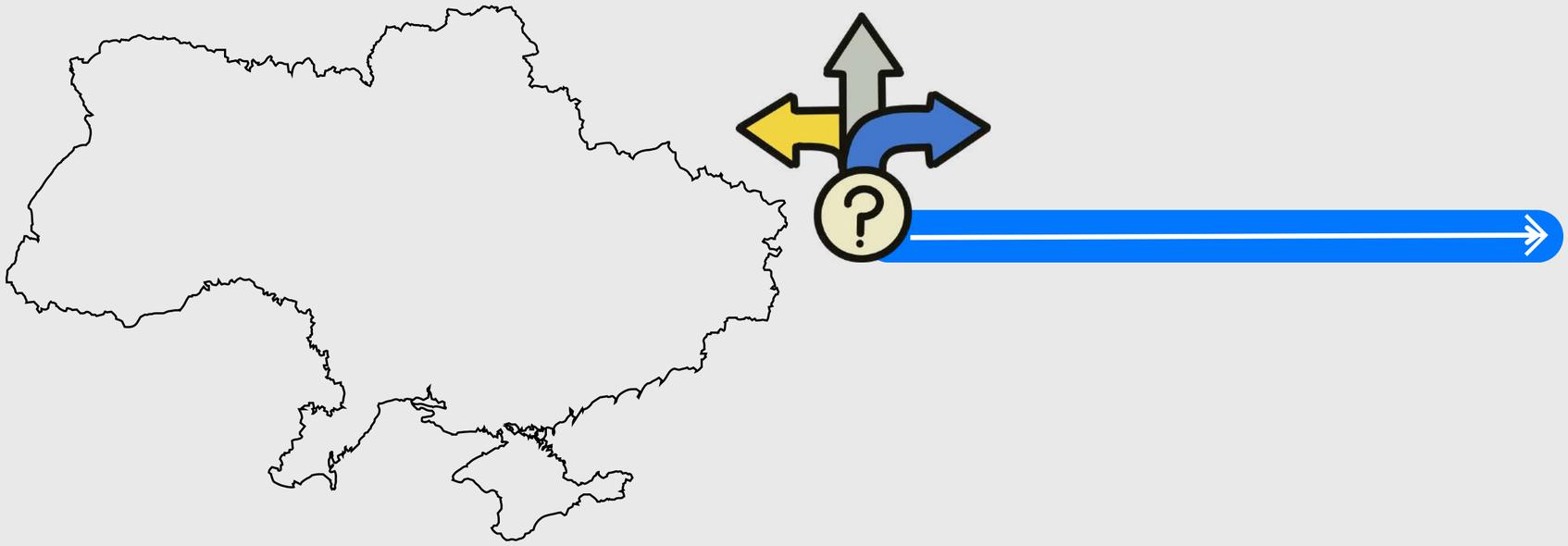
**2. Заборони:** повна заборона систем соціального скорингу та розпізнавання емоцій на робочих місцях (згідно з нормами ЄС, що почали діяти в лютому 2025 року).

**3. Нагляд:** створення або визначення органу, який буде виконувати функції національного AI Office для ринкового нагляду.



# AI Act (Регламент 2024/1689)

Регулювання рухається до більшої формалізації, більшої підзвітності, більшої вимоги до документування, оцінки ризиків, прозорості й контролю.



# Act AI (Регламент ЄС 2024/1689)

**Відповідно до статті 2(6), його дія не поширюється на системи та моделі штучного інтелекту, включно з їхніми результатами, якщо вони спеціально створені й введені в експлуатацію виключно для цілей наукових досліджень і розробок.**

**Стаття 2(8) додатково передбачає, що Регламент не застосовується до діяльності з дослідження, тестування або розроблення систем і моделей ШІ до моменту їх виведення на ринок або введення в експлуатацію.**

Отже, правовий простір для наукових досліджень зберігається насамперед на **докомерційному етапі,** у межах внутрішньої дослідницької роботи, проте звужується в тих випадках, коли дослідження переходить у фазу реального тестування, практичного застосування або наближається до ринкового впровадження.

| | **Provider** | **Deployer** |
|---|---|---|
| Хто це | Особа, орган, установа або інший суб’єкт, який **розробляє** систему ШІ чи модель загального призначення, або **замовляє її розроблення**, і **виводить її на ринок** або **вводить в експлуатацію** під власним ім’ям чи торговельною маркою. | Особа, орган, установа або інший суб’єкт, який **використовує** систему ШІ під своєю владою. |
| Діяльність | Створення, замовлення створення, виведення на ринок, введення в експлуатацію під власним ім’ям. | Використання системи у власній діяльності або в межах власної організаційної відповідальності. |
| На що дивиться Регламент | На те, **хто контролює появу системи як продукту або інструменту**, що виходить за межі внутрішньої розробки. | На те, **хто реально застосовує систему** і під чиєю владою відбувається її використання. |
| Приклад | Лабораторія розробила модель для оцінювання, університет запускає її під власною назвою у внутрішньому або зовнішньому середовищі. У такому разі саме ця установа виступає provider. Це випливає з того, що вона розробила або замовила систему і ввела її в експлуатацію під власним ім’ям. | Університет або дослідницький центр бере вже створену систему і застосовує її, наприклад, для відбору, оцінювання, аналізу даних чи іншого дослідницького процесу. У такому разі він є deployer. |
| Практичний наслідок | Саме для provider далі стають критичними питання відповідності, класифікації системи, документації, управління ризиками та інших обов’язків залежно від категорії системи. | Для deployer ключовими стають правила належного використання системи, дотримання вимог до застосування і, залежно від типу системи, окремі спеціальні обов’язки. |

# Стаття 5 AI Act. Що не допускається

- біометрична категоризація за чутливими ознаками
- виведення емоцій у сфері праці та освіти
- масове збирання зображень облич
- кримінальне прогнозування виключно на основі профілювання
- соціальне скорингування
- маніпуляція поведінкою людини
- використання вразливостей людини
- віддалена біометрична ідентифікація в реальному часі для правоохоронних цілей, крім вузьких винятків

**CHAPTER II**

**PROHIBITED AI PRACTICES**

*Article 5*

**Prohibited AI practices**

1. The following AI practices shall be prohibited:

(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

(c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity;

(d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

(e) the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

(g) the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

# Що це означає?

Стаття 5 забороняє системи ШІ, що застосовують підсвідомі техніки або маніпулятивні чи оманливі техніки, якщо це істотно спотворює поведінку людини і може завдати значної шкоди.

Забороняються системи, що використовують уразливості особи або групи осіб через вік, інвалідність чи конкретне соціальне або економічне становище.

Окремо заборонені соціальне скорингування, невибіркове збирання зображень облич для баз розпізнавання, виведення емоцій у сфері праці та освіти, а також окремі види біометричної категоризації.

**Експериментальний характер розробки не усуває заборонного ефекту норми, якщо дослідження потрапляє в коло прямо заборонених практик.**

# Рівні Ризиків

## Неприйнятни й ризик (Prohibited Practices)

Заборонено (Стаття 5 AI Act).

- Системи ШІ, які суперечать основоположним правам людини.
- Приклади: соціальний скоринг, маніпуляція вразливими групами, масовий збір біометрії для розпізнавання облич, біометрична класифікація за чутливими ознаками

## Високий ризик (HighRisk AI Systems)

- Суворий контроль за ШІ системами (Статті 6-7, Додатки I та III AI Act)
- Системи ШІ, від яких очікується значний вплив на безпеку чи основоположні права людей. Приклади: критична інфраструктура (енергетика, транспорт), медичні вироби, кредитний скоринг, надання державних і соціальних послуг, правосуддя.

## Обмежений ризик (AI systems with Transparency Obligations)

- Легші вимоги, що стосуються прозорості (Стаття 50 AI Act).
- Користувачів потрібно чітко інформувати, що вони взаємодіють із системою ШІ або з контентом, згенерованим/зміненим ШІ.
- Приклади: чат-боти, генеративні моделі для тексту/зображень.

## Мінімальний ризик (AI systems with minimal" or no risk)

- Спеціальні обов’язкові вимоги AI Act не застосовуються. Це більшість повсякденних застосувань ШІ, що не пов'язана із великими мовними моделями.
- Приклади: фільтри спаму, системи рекомендацій у сервісах, відеоігри з елементами ШІ, інструменти управління запасами та логістикою.

## Для високоризикових систем діють такі основні обмеження.

1. вони мають бути охоплені системою управління ризиками (risk management system) за статтею 9. Тобто розробник або інший відповідальний суб’єкт повинен виявляти, оцінювати і мінімізувати ризики протягом усього життєвого циклу системи.

2. до них висуваються вимоги щодо якості даних за статтею 10. Навчальні, валідаційні та тестові набори даних мають бути релевантними, достатньо репрезентативними, наскільки можливо безпомилковими та повними. Це означає, що високоризикову систему не можна будувати на довільних або явно неякісних даних.

3. потрібна технічна документація за статтею 11 і ведення записів за статтею 12. Тобто така система не може існувати як непрозорий інструмент без належного документального супроводу.

4. діє вимога прозорості за статтею 13. Система має бути спроєктована так, щоб користувач, який її застосовує, міг належно інтерпретувати її результати. Для високоризикових систем це суттєве обмеження на використання повністю непрозорих рішень у чутливих сферах.

## Для високоризикових систем діють такі основні обмеження.

5 обов’язковим є людський нагляд за статтею 14. Людина повинна мати можливість контролювати роботу системи, виявляти аномалії, враховувати ризик автоматизаційного викривлення і, за потреби, не використовувати, ігнорувати або зупиняти систему. Отже, високоризикову систему не можна залишити без реального людського контролю.

6 стаття 15 вимагає точності, стійкості та кібербезпеки. Тобто високоризикову систему не можна впроваджувати, якщо вона не відповідає вимогам технічної надійності.

7 для таких систем діють і додаткові обов’язки для постачальника (provider) та *користувача, який застосовує систему (deployer), зокрема щодо оцінки відповідності, системи управління якістю, моніторингу роботи системи, використання належних вхідних даних і зберігання журналів подій. Це вже статті 16, 17, 26 та інші.

# Важливо

- Стаття 50 AI Act вводить вимоги прозорості для систем, що безпосередньо взаємодіють з людиною. Особа має бути поінформована, що взаємодіє саме із системою ШІ, якщо це не є очевидним.

- Стаття 4 вимагає належного рівня обізнаності у сфері ШІ для персоналу, який працює з такими системами.

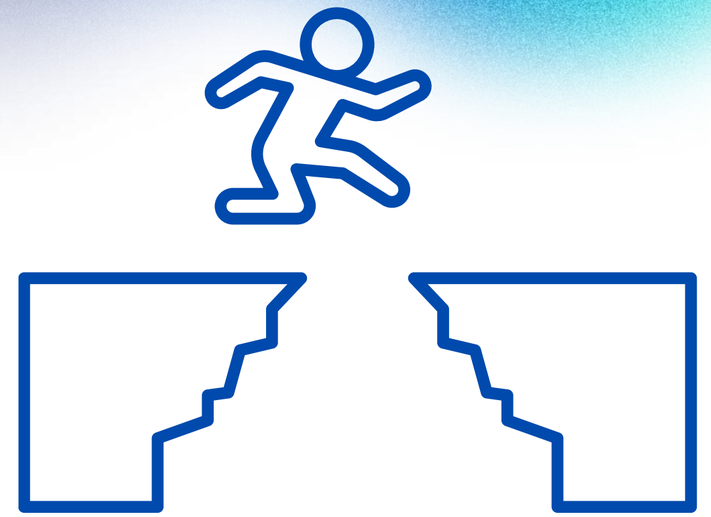
- Стаття 53 встановлює для постачальників моделей загального призначення обов’язок вести технічну документацію, запровадити політику дотримання авторського права ЄС і надавати достатньо деталізовану інформацію про дані, використані для тренування.

- Для моделей із системним ризиком вимоги ще жорсткіші. Стаття 55 охоплює оцінювання моделі, тестування на стійкість до атак, пом’якшення системних ризиків, звітування про серйозні інциденти і кібербезпеку.

- Стаття 99 передбачає значні адміністративні штрафи за порушення заборонених практик та інших вимог Регламенту.

За даними *Centre for European Policy Studies, CEPS, Clarifying the costs* for the EU's AI Act, 2021 обсяги витрат, які мають розробники ШІ в ЄС

| | |
|---|---|
| Побудова QMS (системи управління якістю) | 200–330 тис. євро |
| Щорічне підтримання QMS | близько 70 тис. євро |
| Сертифікація однієї системи | 17–23 тис. євро |
| Виведення одного високоризикового продукту МСП на ринок | до 400 тис. євро |



AI Act передбачає окремі механізми підтримки МСП, проте ключові витрати на процеси відповідності та технічну адаптацію залишаються високими.
Для українських академічних стартапів, які зазвичай мають менший фінансовий ресурс, це може стати бар'єром уже на стадії розробки продукту, особливо у високоризикових сферах, таких як медицина, освіта та інфраструктура.

Які можуть бути наслідки для проєктів, які фінансуються а проєктними коштами, донорами?

# Висновок

Для України ключовим завданням є не механічне копіювання європейських підходів, а формування такого режиму, який одночасно забезпечує захист прав людини, передбачуваність для науковця і можливість розвитку інновацій.

# ДЯКУЮ ЗА УВАГУ!

IP OFFICE
Ukrainian National Office for Intellectual Property and Innovations

# THANK YOU FOR YOUR ATTENTION!

IP OFFICE
Ukrainian National Office for Intellectual Property and Innovations