Д. Волошин, мол. наук. співроб. НЮБ НБУВ

Законодавче регулювання ШІ в ЄС: аналіз AI Act та практика державного контролю

Стрімкий розвиток технологій штучного інтелекту (далі – ШІ) супроводжується не лише розширенням їх практичного застосування, але й зростанням ризиків для прав людини, безпеки та демократичних процесів. Відсутність чітких правових рамок на початкових етапах розвитку цих технологій зумовила необхідність формування комплексного підходу до їх регулювання. Активне формування підходів до правового регулювання ШІ в Європі розпочалося ще у 2018 р. Одними з ключових результатів цього процесу та важливими кроками у вирішенні окреслених проблем стали ухвалення Конвенції зі штучного інтелекту, прав людини, демократії та верховенства права (далі – Конвенція) та Artificial Intelligence Act, тобто Закон про ШІ (далі – AI Act).

Протягом останніх років у європейських державах з'являлося дедалі більше документів, що частково регулювали порядок функціонування ШІ. Проте актуальним лишалось питання розробки єдиного акту, який встановив би загальний стандарт для ШІ систем. Для того, щоб розпочати процес його розробки, в Раді Європи сформували Комітет зі штучного інтелекту (далі – Комітет), який з 2021 р. працював над Конвенцією. І 17 травня 2024 р. Комітет Міністрів Ради Європи ухвалив Конвенцію зі штучного інтелекту, прав людини, демократії та верховенства права. Вона стала першим договором у сфері штучного інтелекту, відкритим для всіх держав світу[25]. Прийняття цього документа обумовило перехід від рекомендаційних та етичних підходів («м'якого права») до формування імперативних норм, у межах яких розвиток і застосування ШІ підпорядковуються міжнародно-правовим нормам[26].

Положення цієї Конвенції спрямовані на забезпечення того, щоб діяльність протягом життєвого циклу систем штучного інтелекту повністю відповідала правам людини, демократії та верховенству права. Крім того, Конвенція має на меті захищати права людини, демократію та верховенство права, а також сприяти підвищенню довіри до систем штучного інтелекту. Для досягнення цієї мети Конвенція визначає такі основні завдання та напрямки дій: створення глобальної правової бази; управління ризиками та вирішення проблем; впровадження національних заходів; захист від дискримінації та збереження приватності; забезпечення прозорості та нагляду; стимулювання безпечних інновацій; підвищення цифрової грамотності; міжнародне співробітництво[27]. Тобто головна ціль Конвенції це прагнення до збалансування технологічного прогресу із захистом фундаментальних прав людини та демократичних інститутів.

Згідно зі ст. 3, сфера застосування Конвенції охоплює діяльність протягом усього життєвого циклу систем штучного інтелекту і поширюється на: державні органи; приватні організації чи осіб, якщо вони виконують завдання або діють від імені державних органів; інших приватних суб'єктів. Водночас Конвенція встановлює чіткі винятки і не поширюється на: діяльність, яка здійснюється в інтересах національної безпеки (за умови, що

[25] Петрів О. Від гучних заяв до практики: реалії регулювання штучного інтелекту. Центр демократії та верховенства права. URL: https://cedem.org.ua/analytics/regulyuvannya-shtuchnogo-intelektu/

[26] Берназюк І. М. Рамкова Конвенція Ради Європи про штучний інтелект у контексті захисту прав людини: виклики та значення для України. Науковий вісник Ужгородського національного університету. Серія: Право 3.93 (2026): С. 18-30. С. 19

[27] Рамкова конвенція Ради Європи зі штучного інтелекту, прав людини, демократії та верховенства права. (Страсбург, 17 травня 2024 року). URL: https://vkksu.gov.ua/sites/default/files/rye_ramkova_konvenciya_zi_shtuchnogo_intelektu_prav_lyudyny_demokratiyi_ta_verh._prava.pdf

вона відповідає міжнародному праву та поважає демократичні інститути); будь-які питання, що стосуються національної оборони; досліджень і розробок, що стосуються систем штучного інтелекту, які ще не стали доступними для використання, якщо тільки випробування або подібна діяльність не здійснюються таким чином, що вони можуть завдати шкоди правам людини, демократії і верховенству права[28].

Для того, щоб у приватній та державній сфері на ринку ЄС розроблялись та застосовувались надійні та безпечні системи ШІ 13 березня 2024 р. у Європарламенті в Страсбурзі проголосували за AI Act, що має регулювати використання систем штучного інтелекту, які функціонують в Європейському Союзі. AI Act регулює системи ШІ залежно від їхнього рівня ризику та впливу[29].

А вже 2 серпня 2025 р., набули чинності вимоги до прозорості для універсальних моделей штучного інтелекту (ШІ). Зокрема згідно з новими правилами, постачальники таких додатків, як ChatGPT та Gemini, повинні розкривати, як працюють їхні системи та на яких даних вони навчалися. Серед іншого, нові правила ЄС мають на меті посилити захист авторських прав[30]. Також Закон має суттєвий вплив на американських технологічних гігантів, зокрема Microsoft, Google, Amazon, Apple та Meta. Дія Закону поширюється за межі ЄС, впливаючи на будь-яку організацію, що здійснює діяльність або має вплив на території ЄС[31].

Дослідники з галузі права зазначають, що AI Act є першою в світі спробою створення всеохоплюючої регуляторної рамки для ШІ-систем. Особливістю європейського підходу є його превентивний характер та чітка орієнтація на захист фундаментальних прав громадян[32].

На сьогодні ЄС виступає глобальним лідером у сфері цифрового регулювання, прикладом чого є прийняття у 2016 році та набуття чинності 25 травня 2018 р. Загального регламенту про захист даних (General Data Protection Regulation, далі – GDPR), який спрямований на захист фізичних осіб стосовно обробки їх персональних даних та вільний рух таких даних[33]. Він встановлює принципи роботи з даними; особливості згоди користувачів на таку обробку; права користувачів щодо їх персональних даних; деталізує порядок збору, обробки та зберігання таких даних для контролюючих організацій та ін.

Окремої уваги заслуговує відповідальність за порушення GDPR, адже санкції досить суворі. До прикладу, покарання за порушення встановлених вимог може бути у вигляді штрафу до 4 % світового річного обороту компанії або ж до 20 млн євро. GDPR застосовується до компаній та організацій, що, в процесі їх функціонування, здійснюють збір, обробку та зберігання персональних даних громадян ЄС, а також у випадках, коли така компанія чи організація знаходиться в межах

[28] Рамкова конвенція Ради Європи зі штучного інтелекту, прав людини, демократії та верховенства права. (Страсбург, 17 травня 2024 року). URL: https://vkksu.gov.ua/sites/default/files/rye_ramkova_konvenciya_zi_shtuchnogo_intelektu_prav_lyudyny_demokratiyi_ta_verh._prava.pdf

[29] Європарламент ухвалив перший у світі Закон про штучний інтелект. Центр демократії та верховенства права. URL: https://cedem.org.ua/news/eu-zakon-pro-shtuchnyi-intelekt/

[30] Худякова О. У ЄС почали діяти вимоги до прозорості штучного інтелекту. Deutsche Welle. URL: https://www.dw.com/uk/u-es-nabuli-cinnosti-vimogi-do-prozorosti-stucnogo-intelektu/a-73509162

[31] Закон про штучний інтелект в ЄС набув чинності: за порушення на компанії чекатимуть штрафи до 7 % річного доходу. Fintech Snsider. URL: https://fintechinsider.com.ua/zakon-pro-shtuchnyj-intelekt-v-yes-nabuv-chynnosti-za-porushennya-na-kompaniyi-chekatymut-shtrafy-do-7-richnogo-dohodu/

[32] Гаркуша А. О. Міжнародно-правові тенденції регулювання штучного інтелекту: комплексний аналіз та практика застосування. Полтавський правовий часопис 1 (2024): 142-158. С. 147.

[33] Петрів О. Спесивцева О. Міжнародні підходи до розвитку ШІ та принципів відповідальності за використання: висновки для України. Центр демократії та верховенства. URL: https://analytics.intsecurity.org/mizhnarodni-pidhody-rozvytku-shi/

ЄС, незалежно від того, чи опрацювання персональних даних здійснюється в межах ЄС чи поза межами ЄС, а також незалежно від суб'єктів, персональні дані яких обробляються. Перевагою провадження правил GDPR є формування ділової репутації компанії як такої, що цінує персональні дані своїх клієнтів. Окрім цього, забезпечення безпеки даних надасть можливість уникнути фінансових та економічних втрат у майбутньому[34].

На відміну від підходів, закладених у GDPR, сфера застосування AI Act має більш диференційований характер і не охоплює всі системи штучного інтелекту. Зокрема, він поширюється не на всі системи ШІ. Системи, які випускаються на ринок, вводяться в експлуатацію або використовуються для військових, оборонних або національних цілей безпеки, виключені зі сфери його застосування незалежно від того, який тип суб'єкта здійснює таку діяльність (державний чи приватний суб'єкт). Національна безпека залишається виключною відповідальністю держав-членів відповідно до ст. 4 (2) Договору про ЄС. Проте якщо така система ШІ (що розроблена та використовується для військових, оборонних або національних цілей безпеки) використовується одночасно і поза цими цілями (наприклад, для цивільних або гуманітарних цілей, цілей правоохоронної діяльності або громадської безпеки), така система підпадає під дію AI Act. У такому випадку, суб'єкт, який використовує систему ШІ для інших цілей, ніж військові, оборонні або національної безпеки, повинен забезпечити відповідність систем ШІ вимогам AI Act[35].

Документ має чітку ієрархічну структуру і складається із трьох основних блоків: вступної частини, основних нормативних розділів та додатків. Зокрема, основна нормативна частина складається з 13 розділів та охоплює ключові аспекти правового регулювання ШІ, зокрема від загальних положень та заборонених практик до правил класифікації високоризикових систем та встановлення вимог регулювання до них; встановлює вимоги щодо прозорості та регулювання класифікації великих ШІ моделей; визначає обов'язки їх провайдерів та застосування відповідних кодексів практик[36].

Зокрема, основні положення цього законодавчого акту передбачають:

1. Визначення рівнів ризику систем ШІ.
2. Введення обов'язкової сертифікації для певних систем ШІ. До таких систем належать, наприклад, системи біометричної ідентифікації, критичної інфраструктури, освітні або професійні оцінювальні системи.
3. Встановлення вимог для певних систем ШІ щодо необхідності інформування користувачів про те, що вони взаємодіють з системою ШІ, а не людиною.
4. Встановлення правил прозорості для систем ШІ, призначених для взаємодії з фізичними особами, систем розпізнавання емоцій, а також систем ШІ, які використовуються для створення або оброблення зображень, аудіо – або відеоконтенту.
5. Створення єдиного європейського ринку ШІ. Це передбачає введення єдиних правил для роботи з технологіями ШІ на території ЄС, що сприятиме вільному руху систем ШІ та послуг на європейському ринку.
6. Заборону на використання певних методів штучного інтелекту[37].

[34] Бирлад Ю. Що таке GDPR та чи варто його виконувати поза межами ЄС. Адвокатське об'єднання Бачинський та партнери. URL: https://legalaid.ua/ua/shho-take-gdpr/

[35] Петрів О. Спесивцева О. Міжнародні підходи до розвитку ШІ та принципів відповідальності за використання: висновки для України. Центр демократії та верховенства. URL: https://analytics.intsecurity.org/mizhnarodni-pidhody-rozvytku-shi/

[36] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series. 2024/1689, 12 July 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

[37] Петрів О. Штучний інтелект та Artificial Intelligence Act: час для юридичних рамок. Центр демократії та верховенства. URL: https://cedem.org.ua/analytics/artificial-intelligence-act/

Зокрема, положення AI Act поширюються на розробників і постачальників систем та моделей штучного інтелекту, продукція яких виводиться на ринок Європейського Союзу або використовується в його межах, незалежно від їхнього фактичного місцезнаходження.

Щодо суб'єктів, до яких він застосовується, то їхнє коло визначено в ч. 1 ст. 2 Регламенту, а саме:

– постачальники, що розміщують на ринку або вводять в експлуатацію системи штучного інтелекту, або розміщують на ринку моделі штучного інтелекту загального призначення в Союзі, незалежно від того, чи ці постачальники зареєстровані або розташовані в Союзі, чи в третій країні;

– розгортачі систем штучного інтелекту, які мають місцезнаходження або розташовані в Союзі;

– постачальники та розгортачі систем штучного інтелекту, які мають місцезнаходження або розташовані в третій країні, де результат, вироблений системою штучного інтелекту, використовується в Союзі;

– імпортери та дистриб'ютори систем штучного інтелекту;

– виробники продукції, що розміщують на ринку або вводять в експлуатацію систему штучного інтелекту разом зі своїм продуктом та під своїм ім'ям або торговою маркою;

– уповноважені представники постачальників, які не зареєстровані в Союзі;

– зацікавлені особи, які розташовані в Союзі[38].

Визначальною особливістю AI Act є запровадження ризик-орієнтованого підходу до регулювання штучного інтелекту. У межах цього підходу всі системи штучного інтелекту класифікуються залежно від рівня ризику, який вони становлять для особи та суспільства, що, в свою чергу, визначає обсяг правових вимог та обмежень щодо їх використання. Зокрема серед них виділяють:

– Мінімальний ризик. До нього належать елементи ШІ, інтегровані в інші програмні продукти, наприклад ШІ в комп'ютерних іграх або спам-фільтри. Діяльність таких систем не регулюється Актом, але може регулюватися використання систем ШІ для особистих потреб, не пов'язаних з професійним використанням іншим законодавством ЄС. Також не регулюється використання систем ШІ для особистих потреб, не пов'язаних з професійним використанням.

– Обмежений ризик. Люди повинні бути чітко проінформовані коли вони взаємодіють із ШІ (наприклад, із чат-ботами). Системи, що генерують аудіо-, відео-, чи текстовий контент повинні маркувати результати у машинозчитувальному форматі, як штучно згенеровані[39].

– Високий ризик. Це системи біометричної ідентифікації, системи, які використовуються в критичній інфраструктурі, системи освіти, управління персоналом, державних послуг тощо[40]. Системи ШІ з високим ризиком (які можуть загрожувати безпеці чи правам людей) дозволені, але підлягають суворим вимогам контролю – виробники та користувачі таких систем мають забезпечити відповідність цілої низки критеріїв. До прикладу це стосується управління даними, їх прозорість, можливість контролю людиною, кібербезпека тощо). До високоризикових віднесено ШІ у восьми сферах, включаючи критично важливі галузі як от медицина, транспорт, зайнятість та освіта. Наприклад, системи ШІ, що використовуються для прийняття рішень щодо доступу до освіти або оцінювання здобувачів освіти/учнів, визначено як високоризикові (Додаток ІІІ до Акту ЄС про ШІ). Це означає, що якщо заклад освіти застосовує алгоритм для відбору абітурієнтів, або школа – для автоматичного виставлення оцінок, такі системи повинні пройти оцінку

[38] Забокрицький, І. І. Акт про Штучний Інтелект (Artifical Inteligence Act, AI Act) як основа правового регулювання штучного інтелекту в ЄС: огляд основних положень. Аналітично-порівняльне правознавство 3.3 (2025): 282-286.

[39] Акт Європейського Союзу про штучний інтелект. Deloitte. URL: https://www.deloitte.com/ua/uk/services/tax/perspectives/tax-and-legal-alerts-2024-08-12.html

[40] Заборона неприйнятних практик використання штучного інтелекту в ЄС. Deloitte. URL: https://www.deloitte.com/ua/uk/services/tax/perspectives/tax-and-legal-alert-2025-02-13.html

відповідності вимогам: мати якісні тренувальні дані, документацію, забезпечувати можливість перевірки результатів людиною тощо[41].

– Неприйнятний ризик (Заборонені практики ШІ). Акт забороняє такі системи (наприклад, системи соціального рейтингування, створені для маніпуляцій людьми, нецільове збирання зображень обличь)[42].

Зокрема, розділ, що регулює такі high-risk системи ШІ є одним із найбільших. У ньому визначається, що high-risk ШІ використовується в критичних сферах, таких як системи прийняття рішень у судових процесах, оцінки ризику в банківській сфері, контролю за працівниками, та біометричні системи ідентифікації. AI Act вимагає від розробників ШІ систем високого ризику дотримуватися строгих вимог щодо безпеки, прозорості та етичності.

Системи цієї категорії поділяються на вісім основних груп, які:

1. Використовують біометричну ідентифікацію.
2. Застосовуються у критичній інфраструктурі (наприклад, транспорт), що може поставити під загрозу життя і здоров'я громадян.
3. Визначають доступ до освіти або оцінюють студентів (наприклад, підрахунок балів на іспитах).
4. Використовуються під час прийому на роботу, або приймають рішення щодо просування по службі, розірвання контрактів чи розподілу завдань (наприклад, програмне забезпечення для сортування резюме для процедур найму на роботу).
5. Застосовуються під час надання приватних та державних послуг (наприклад, кредитний скоринг, який позбавляє громадян можливості отримати кредит).
6. Використовуються в правоохоронних органах, які можуть втручатися у фундаментальні права людей (наприклад, оцінка достовірності доказів).
7. Використовуються під час організації міграційних процесів, надання притулку або прикордонного контролю. Наприклад, застосування ШІ в поліграфах чи подібних інструментах для виявлення емоційного стану особи, перевірки автентичності проїзних документів.
8. Допомагають у роботі судових систем та забезпечують різні демократичні процеси. Призначені для допомоги судовим органам у дослідженні фактів та законів, а також у застосуванні Закону в різних ситуаціях.

Ці системи ШІ повинні будуть відповідати низці обов'язкових вимог та пройти процедури оцінки відповідності, перш ніж вони зможуть потрапити на ринок ЄС[43].

Також AI-акт встановлює особливі вимоги до постачальників цих систем. Як приклад, перед тим як випустити на ринок або ввести в експлуатацію систему ШІ високого ризику, необхідно скласти технічну документацію. Крім того, дана документація має постійно оновлюватись відповідно до змін, що вносяться в системі протягом її життєвого циклу.

Акт також містить обов'язки і для користувачів ШІ-систем, які використовують їх у професійній діяльності. Перед тим як використовувати високоризикову систему штучного інтелекту на робочому місці, роботодавці повинні повідомити про це працівників[44]. Користувачі повинні нести відповідальність за те, щоб

[41] Акт ЄС про штучний інтелект (EU AI Act). Курс «Застосування штучного інтелекту у сфері П(ПТ)О», модуль «Етика, регулювання та відповідальне використання ШІ». Професійна освіта онлайн. URL: https://profosvita.online/courses/course-v1:Profosvita+CM-R042-OEP+2025/courseware/cf537a87f29c45d3ba401b3e098a2e03/6729e9d50767490e8b0e5c4db02bb943/3?activate_block_id=block-v1%3AProfosvita%2BCM-R042-OEP%2B2025%2Btype%40vertical%2Bblock%40f12ab6f7bb8c4629996f08582fda5e6d

[42] Акт Європейського Союзу про штучний інтелект. Deloitte. URL: https://www.deloitte.com/ua/uk/services/tax/perspectives/tax-and-legal-alerts-2024-08-12.html

[43] Петрів О. Штучний інтелект та Artificial Intelligence Act: час для юридичних рамок. Центр демократії та верховенства. URL: https://cedem.org.ua/analytics/artificial-intelligence-act/

[44] Європарламент ухвалив перший ШІ-акт: які вимоги для бізнесу. Barbashyn law firm. URL: https://barbashyn.law/statti/yevroparlament-uhvalyv-pershyj-shi-akt-yaki-vymogy-dlya-biznesu/

система штучного інтелекту використовувалася належним чином попри те, якщо постачальник виконав свою частину роботи. Основне завдання як користувача полягає не в тому, щоб зрозуміти, як працює алгоритм, а в тому, щоб переконатися, що його використання є правильним, контрольованим і прозорим[45].

Відповідно до положень AI-акту до користувачів систем штучного інтелекту встановлюється низка обов'язкових вимог, спрямованих на забезпечення безпечного та відповідального їх застосування, зокрема серед них:

– використання відповідно до інструкцій дотримуючись вказівок виробника;

– контроль з боку людини. Особливо у системах з високим рівнем ризику завжди має бути присутня людина, здатна здійснювати контроль та втручатися;

– моніторинг продуктивності. Перевірка, чи система працює належним чином, та повідомлення постачальника про можливі відхилення від норми;

– зберігання журналів. Для систем з високим рівнем ризику зберігання журналів роботи є обов'язковим[46].

Окремим важливим елементом правового механізму, передбаченого Законом ЄС про ШІ є система санкцій. Акт встановлює трирівневу модель покарань, що диференціюється залежно від характеру та серйозності порушення. Зокрема:

– до першого рівня відноситься недотримання заборонених практик ШІ, що передбачають найсерйозніші порушення, такі як використання підсвідомих методів маніпулювання або використання вразливостей певних груп, за що передбачено штрафи до 30 млн євро або 6 % річного обороту компанії в усьому світі, залежно від того, що більше;

– другий рівень передбачає невідповідність вимогам до систем штучного інтелекту з високим ризиком, управління даними та зобов'язань щодо прозорості. Це стосується порушення вимог до систем штучного інтелекту з високим рівнем ризику, таких як нездатність запровадити систему управління ризиками, незабезпечення високоякісних навчальних даних або порушення зобов'язань щодо управління даними та прозорості за що передбачено штрафи до 20 млн євро або 4 % річного обороту компанії в усьому світі, залежно від того, що більше;

– третій рівень передбачає недотримання зобов'язань щодо прозорості, це стосується порушень інших зобов'язань і вимог, таких як нереєстрація системи штучного інтелекту в базі даних ЄС або відмова від співпраці з органами влади за що передбачено штрафи до 10 млн євро або 2 % річного обороту компанії в усьому світі, залежно від того, що більше[47].

Водночас, Закон ЄС про AI визначає загальні принципи визначення покарань, спрямовані на санкції, які є ефективними, стримуючими та пропорційними конкретним обставинам кожної справи. Приймаючи рішення про покарання, органи влади можуть враховувати різні фактори, такі як:

– особливості злочину, в тому числі характер, тяжкість і тривалість;

– чи було порушення навмисно чи через недбалість;

– заходи, вжиті правопорушником для пом'якшення негативного впливу;

– історія попередніх штрафів правопорушника;

– характеристики правопорушника, включаючи розмір, дохід і частку ринку;

– будь-які фінансові прибутки чи збитки в результаті порушення;

– якщо система штучного інтелекту використовувалася в професійних або особистих цілях.

[45] Практичний посібник з Європейського закону про штучний інтелект для малих та середніх підприємств: що зміниться для вас. ELECTE. URL: https://www.electe.net/uk/post/european-ai-act

[46] Практичний посібник з Європейського закону про штучний інтелект для малих та середніх підприємств: що зміниться для вас. ELECTE. URL: https://www.electe.net/uk/post/european-ai-act

[47] Ціна невідповідності: штрафні санкції Закону ЄС про штучний інтелект і як Shaip допомагає вам їх уникнути. Shaip by ubiquity. URL: https://uk.shaip.com/blog/the-cost-of-non-compliance-eu-ai-act-penalties/

Також Закон про ШІ використовує пропорційний підхід до малих і середніх підприємств (МСП) і стартапів, призначаючи менші штрафи залежно від їх розміру, інтересів і економічної життєздатності[48].

У контексті застосування європейського законодавства особливу увагу слід приділити практикам держав-членів ЄС щодо впровадження та нагляду за використанням ШІ. Так, наприклад, Італія випередила інших, ставши однією з перших країн, які інтегрували європейське законодавство у власне[49].

Зокрема, італійський закон встановлює конкретні правила для стратегічних секторів та вводить нові склади злочинів для боротьби з незаконним використанням штучного інтелекту. Було призначено два національні органи нагляду:

– AgID (Агентство з питань цифрової Італії): буде здійснювати загальний нагляд, проводити перевірки та застосовувати санкції;

– ACN (Агентство з національної кібербезпеки): буде контролювати питання кібербезпеки систем штучного інтелекту[50].

Прем'єр-міністр Італії Дж. Мелоні позиціонувала закон як такий, що встановлює «італійський шлях» управління штучним інтелектом, балансуючи технологічні інновації з культурною спадщиною та гуманістичними цінностями. Цей антропоцентричний підхід ставить людину в центр прийняття рішень щодо штучного інтелекту, водночас підкреслюючи етичні рамки, що зосереджені на правах та потребах людей. Законодавство інтегрується з ширшою стратегією цифрової трансформації Італії, включаючи розробку італійськомовних моделей штучного інтелекту в рамках проєкту Minerva та співпрацю з NVIDIA щодо місцевих можливостей штучного інтелекту. Під час головування Італії в G7 у 2024 р. вплив штучного інтелекту на робочі місця та нерівність став центральним питанням, що сприяло розвитку спільних рамок управління для розвитку штучного інтелекту[51].

Італійський закон запроваджує безпрецедентні кримінальні покарання за зловживання штучним інтелектом, включаючи позбавлення волі на строк від 1 до 5 років за незаконне розповсюдження шкідливого контенту, створеного штучним інтелектом, зокрема діпфейків, які завдають несправедливої шкоди. Коли ШІ сприяє традиційним злочинам, таким як шахрайство, крадіжка особистих даних або відмивання грошей, покарання збільшуються на одну третину як обтяжуюча обставина. Також Закон вимагає батьківської згоди для дітей віком до 14 років на доступ до послуг штучного інтелекту, встановлюючи посилений захист конфіденційності спеціально для неповнолітніх[52].

Щодо державного регулювання використання ШІ, то Іспанія стала однією з перших країн ЄС, яка запровадила правила блоку, які вважаються більш всеосяжними. Як наголосив міністр, будь-хто може стати жертвою дипфейку –відео чи фото, спотворених за допомогою алгоритмів ШІ та представлених як справжні. Іспанський законопроєкт, який має бути схвалений нижньою палатою, класифікує недотримання належного маркування контенту, створеного штучним інтелектом, як «серйозне правопорушення». Це передбачає штраф до 38,2 млн дол. або 7 % глобального річного обороту компанії. Законопроєкт також забороняє використання підсвідомих технік – звуків і зображень, які є

[48] Ціна невідповідності: штрафні санкції Закону ЄС про штучний інтелект і як Shaip допомагає вам їх уникнути. Shaip by ubiquity. URL: https://uk.shaip.com/blog/the-cost-of-non-compliance-eu-ai-act-penalties/

[49] Italy pioneers Europe's first national AI law amid regulatory tensions. European AI and Cloud Summit. URL: https://cloudsummit.eu/blog/italy-pioneers-europe-first-national-ai-law

[50] Практичний посібник з Європейського закону про штучний інтелект для малих та середніх підприємств: що зміниться для вас. ELECTE. URL: https://www.electe.net/uk/post/european-ai-act

[51] Italy pioneers Europe's first national AI law amid regulatory tensions. European AI and Cloud Summit. URL: https://cloudsummit.eu/blog/italy-pioneers-europe-first-national-ai-law

[52] Italy pioneers Europe's first national AI law amid regulatory tensions. European AI and Cloud Summit. URL: https://cloudsummit.eu/blog/italy-pioneers-europe-first-national-ai-law

непомітними, – для маніпулювання вразливими групами людей. Контроль за дотриманням нових правил входитиме до компетенції новоствореного агентства з нагляду за штучним інтелектом AESIA[53].

Німеччина офіційно запроваджує обов'язкову сертифікацію всіх систем штучного інтелекту, що використовуються у державному секторі, щоб підвищити безпеку, прозорість і відповідність етичним стандартам. Нові правила передбачають оцінку алгоритмічної безпеки, прозорості рішень та відповідності GDPR, а також перевірку на запобігання дискримінаційним та упередженим результатам. Сертифікація охоплює адміністративні послуги, соціальні системи, правоохоронні органи та інші державні структури, де застосовуються AI-технології. Влада Німеччини підкреслила, що це зробить країну однією з перших у ЄС, яка формально регулює ШІ у державному секторі. Експерти прогнозують, що сертифікація може стати моделлю для приватного сектору та інших країн Європи, встановлюючи новий стандарт безпечного та етичного використання AI[54].

Франція позиціонує себе як ключовий гравець у галузі ШІ та нових технологій. Завдяки високому рівню академічної та наукової традиції, вона змогла розвинути динамічну та інноваційну екосистему, яка підтримується державними та приватними ініціативами. Національна стратегія з розвитку штучного інтелекту (SNIA), започаткована у 2018 р. та посилена планом France 2030, ілюструє прагнення країни стати європейським та світовим лідером у цій галузі[55]. Франція обрала децентралізовану організацію ринкового нагляду, що базується на органах, вже визначених операторами, з координацією під керівництвом Міністерства економіки та централізованим забезпеченням технічної експертизи, необхідної для завдань з оцінки відповідності, що виконуються органами з контролю за ринком (MSA). Однак незважаючи на публікацію проєкту призначення органів управління наглядом за дотриманням нормативних актів (MSA), прогрес у впровадженні Закону ЄС про ШІ у Франції залишається неясним і особливо затримується. Франція все ще є однією з держав, які ще не призначили свої національні компетентні органи більш ніж через п'ять місяців після закінчення терміну, встановленого Законом ЄС про ШІ[56].

Польща перебуває в процесі прийняття національного закону на доповнення до Закону ЄС про ШІ («Проєкт закону про системи штучного інтелекту»). Найновіший проєкт від 18 листопада 2025 р., але він навіть не перебуває на законодавчому етапі парламенту. Наразі в Польщі немає спеціально створеного місцевого органу влади чи регулятора, відповідального за нагляд за ШІ, окрім органів/регуляторів ЄС. Однак Польща перебуває в процесі створення спеціалізованого органу під назвою Комісія з питань розвитку та безпеки штучного інтелекту (Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji – KRiBSI). Ключові завдання, покладені на Комісію, включатимуть:

– проведення ринкового нагляду за системами штучного інтелекту;

– бути центральним контактним пунктом, призначеним Законом ЄС про ШІ;

– надання окремих думок, пояснень та тлумачень;

– обробка звітів та скарг про інциденти;

– проведення перевірок та забезпечення дотримання правил ЄС щодо штучного інтелекту;

[53] Тарасова Д. Іспанія запроваджує штрафи до $38 млн за відсутність маркування контенту, створеного ШІ. Еспресо. URL: https://espreso.tv/tekhnologiyi-ispaniya-zaprovadzhue-shtrafi-do-38-mln-za-vidsutnist-markuvannya-kontentu-stvorenogo-shi

[54] Щукіна А. Німеччина ввела обов'язкову сертифікацію AI-систем у державному секторі. New Format. RL: https://newformat.info/socium/nimechchyna-vvela-obov-iazkovu-sertyfikatsiiu-ai-system-u-derzhavnomu-sektori/

[55] Загальний огляд Франції в галузі штучного інтелекту та нових технологій. Actualités IA récentes. URL: https://www.actuia.com/uk/actors/france/

[56] EU AI Act Implementation: France Still Without Designated National Competent Authorities. AI-regulation.com. URL: https://ai-regulation.com/eu-ai-act-implementation-france-still-without-designated-national-competent-authorities/

– співпраця з ключовими національними та європейськими органами тощо.

Водночас ефективність функціонування зазначеної інституційної системи значною мірою залежить від координаційної ролі центральних органів державної влади. Міністр цифровізації відіграє центральну роль у формуванні політики та регулювання штучного інтелекту в Польщі. Зокрема, йому доручено підготувати та прийняти проєкт Закону про системи штучного інтелекту. Крім того, нещодавно було опубліковано оновлену версію Політики розвитку штучного інтелекту в Польщі до 2030 р., яка визначає раціональний напрямок розвитку штучного інтелекту в Польщі на найближчі роки. Міністерство також створило консультативну групу з питань програмного забезпечення/ штучного інтелекту, що складається з польських експертів з питань штучного інтелекту[57].

Аналіз європейського регулювання ШІ, зокрема положень AI Act свідчить про формування в ЄС комплексної та системної моделі правового регулювання штучного інтелекту, заснованої на ризик-орієнтованому підході. Особливістю цього Акта є його превентивний характер, що передбачає встановлення вимог до безпечності, прозорості та підзвітності ШІ-систем ще на етапі їх розробки та впровадження. Водночас ефективність його застосування значною мірою залежить від належної імплементації на національному рівні та функціонування інституційних механізмів контролю, що підтверджується практиками держав-членів ЄС. Подальший розвиток системи регулювання штучного інтелекту в Європі потребує узгодженості дій держав та вдосконалення механізмів реалізації.

ЩОДЕННИК БЛОГЕРА[58]

Блог на сайті «Lb.ua»

Про автора: Олена Ігнащук, кандидатка медичних наук, доцентка Школи управління в охороні здоров'я Національного університету «Києво-Могилянська академія»

Медична реформа зробила ставку на первинку. Чи встигла за нею медична освіта?

Медична реформа 2018 року змінила логіку системи: у центрі опинився пацієнт, а його головним провідником став сімейний лікар. Через лікаря первинки відбувається перший контакт людини з системою охорони здоров'я, тут формується довіра, ухвалюють перші клінічні рішення і визначають подальший маршрут. Попри це, у медичній освіті сімейна медицина досі не посідає належного місця. Навчання продовжує орієнтуватися переважно на вузьку спеціалізацію, тоді як 60–80 % потреб населення має покривати саме первинна ланка. Цю невідповідність прагне подолати нова Медична школа Києво-Могилянської академії та медичної мережі «Добробут» – програма, яка готуватиме лікарів відповідно до реальної логіки й потреб системи.

На початок 2026 року понад 30 мільйонів Українців уклали декларації з сімейним лікарем. Цей лікар координує маршрут, відповідає за профілактику і перші клінічні рішення. Реформа фінансування системи охорони здоров'я змінила логіку руху грошей, щоб забезпечити універсальне покриття медичною допомогою – тобто доступ до базових послуг для кожної людини без фінансових бар'єрів. У цій моделі саме первинна ланка стає точкою входу і основою системи.

І це відповідає реальній структурі потреб. Приблизно 90% звернень за медичною допомогою, за даними ВООЗ, пов'язані з

[57] AI laws and regulation in Poland. CMS Law Tax Future. URL: https://cms.law/en/int/expert-guides/ai-regulation-scanner/poland

[58] Збережено стиль і граматику оригіналу