

УДК / UDC: 34:004.8:316.4

DOI: [https://doi.org/10.37750/2616-6798.2026.1\(56\).357246](https://doi.org/10.37750/2616-6798.2026.1(56).357246)**Олександр Дмитрович Довгань**

Державна наукова установа “Інститут інформації, безпеки і права Національної академії правових наук України”.

Київ, Україна

ORCID: <https://orcid.org/0000-0002-3453-4938>**Тарас Юрійович Ткачук**

Український науково-дослідний інститут спеціальної техніки та судових експертиз СБУ.

Київ, Україна

ORCID: <https://orcid.org/0000-0002-4620-3300>

ARTIFICIAL GENERAL INTELLIGENCE: НОВИЙ ЕТАП ГЛОБАЛЬНОЇ ПРАВОВОЇ ДИСКУСІЇ

***Анотація.** Стаття присвячена комплексному дослідженню правових та соціально-цивілізаційних наслідків можливого створення штучного загального інтелекту (Artificial General Intelligence, AGI) системи, здатної здійснювати когнітивну діяльність загального характеру на рівні людини або перевершуючи її в необмеженому колі предметних областей. Обґрунтовується теза про те, що перехід від вузького ШІ до AGI є не лише технологічним, а фундаментальним цивілізаційним зрушенням, яке ставить під сумнів ефективність правових режимів, розроблених для попередніх поколінь ШІ-систем.*

У статті проаналізовано технологічні передумови розвитку AGI, масштабування моделей, мультимодальність та автономні агентні архітектури і систематизовано сучасні прогнози щодо часових горизонтів його появи. Досліджено потенційні соціально-економічні наслідки AGI у сферах наукового прогресу, трансформації ринку праці та державного управління. Виявлено ключові ризики для фундаментальних прав людини: право на приватність, принцип недискримінації, свободу вираження поглядів та цілісність демократичних процесів.

Окрему увагу приділено аналізу еволюції корпоративних стандартів безпеки ШІ від екзистенційного горизонту 2015 року до редукованого управління юридичними ризиками у 2025 році, що свідчить про системну неспроможність саморегулювання індустрії як достатнього механізму управління ризиками рівня AGI. Проаналізовано чинні міжнародно-правові інструменти: AI Act ЄС, Рамкову конвенцію Ради Європи про ШІ, принципи ОЕСР та Рекомендацію ЮНЕСКО з етики ШІ, а також наслідки відкликання Директиви ЄС про відповідальність за ШІ.

Сформульовано висновок про необхідність якісного переходу від фрагментарного регулювання окремих застосувань вузького ШІ до системного правового режиму управління frontier-технологіями, що передбачає обов'язкові оцінки впливу на права людини, незалежний аудит, механізми звітування про інциденти та дозвільні процедури для моделей із системним ризиком. Обґрунтовано гібридну модель юридичної відповідальності розробників і операторів AGI-систем, а правосуб'єктність AGI визначено як передчасний і небезпечний крок, натомість запропоновано концепцію “AGI як об'єкта підвищеної правової уваги”.

***Ключові слова:** штучний загальний інтелект, AGI, правове регулювання штучного інтелекту, frontier-моделі, безпека штучного інтелекту, права людини, алгоритмічна відповідальність, AI Act, правосуб'єктність ШІ, технологічна сингулярність, автономні агентні системи, глобальне управління ШІ.*

Oleksandr D. Dovhan

State Scientific Institution "Institute of Information, Security and Law
of the National Academy of Legal Sciences of Ukraine"

Kyiv, Ukraine

ORCID: <https://orcid.org/0000-0002-3453-4938>

Taras Yu. Tkachuk

Ukrainian Research Institute of Special Equipment and Forensic
Expertise of Security Service of Ukraine

Kyiv, Ukraine

ORCID: <https://orcid.org/0000-0002-4620-3300>

ARTIFICIAL GENERAL INTELLIGENCE: A NEW CHAPTER IN THE GLOBAL LEGAL DISCOURSE

***Summary.** This article offers a comprehensive analysis of the legal and socio-civilisational implications associated with the potential emergence of Artificial General Intelligence (AGI) a system capable of performing general cognitive functions at or beyond the level of human intelligence across an unrestricted range of domains. It argues that the transition from narrow AI to AGI represents not merely a technological milestone but a profound civilisational shift, one that fundamentally challenges the adequacy of existing legal frameworks designed for earlier generations of AI systems.*

The article examines the technological prerequisites for AGI development, including large-scale model architectures, multimodality, and autonomous agentic systems, and systematises contemporary forecasts regarding the likely timelines of AGI's arrival. The potential socio-economic consequences of AGI are analysed across three key domains: scientific progress, labour market transformation, and public administration. Particular attention is devoted to risks for fundamental human rights, including the right to privacy, the principle of non-discrimination, freedom of expression, and the integrity of democratic processes.

A separate section traces the evolution of corporate AI safety standards from the existential-risk framing of 2015 to the narrowly legalistic liability-management approaches of 2025 demonstrating the structural insufficiency of industry self-regulation as a mechanism for governing risks of AGI magnitude. The article critically evaluates the principal international legal instruments in this field, including the EU AI Act, the Council of Europe Framework Convention on AI, the OECD AI Principles, and the UNESCO Recommendation on the Ethics of AI, and considers the implications of the European Commission's withdrawal of the proposed AI Liability Directive.

The article concludes that a qualitative regulatory shift is required: from fragmented governance of individual narrow-AI applications toward a systemic legal regime for frontier-level technologies. Such a regime must include mandatory human-rights impact assessments, independent technical audits, incident-reporting obligations, and authorisation procedures for models presenting systemic risk. A hybrid model of legal liability for AGI developers and operators is proposed, while the attribution of legal personality to AGI is characterised as premature and potentially harmful. Instead, the article advances the concept of AGI as an object of heightened legal scrutiny.

Keywords: artificial general intelligence, AGI, AI regulation, frontier models, AI safety, human rights, algorithmic accountability, EU AI Act, AI legal personality, technological singularity, autonomous agentic systems, global AI governance.

Постановка проблеми. Ми живемо в епоху цифрової трансформації, де генеративний штучний інтелект (ШІ) поширюється надзвичайно швидко. Але це не просто чергова технологічна новинка. Насправді йдеться про глибший цивілізаційний виклик, що зачіпає саму природу людського мислення та інтелектуальної діяльності.

Попередні технологічні прориви від винаходу друкарського верстата до появи Інтернету змінювали переважно те, як ми зберігаємо й поширюємо знання. Нинішня хвиля генеративного ШІ йде значно далі. Вона ставить під сумнів саму автентичність знань і здатність людини відрізнити правдиву інформацію від створеної алгоритмами.

Проблема перевірки знань завжди була центральною для епістемології, науки про те, як ми знаємо те, що знаємо. Протягом століть суспільство створило складну систему перевірки достовірності інформації, зокрема це академічне рецензування, наукові інституції, редакційні стандарти, правила цитування та вимоги відтворюваності результатів тощо. Усі ці механізми базувалися на простому припущенні, що за текстом стоїть людина, яка мислить, робить висновки і несе відповідальність за свої твердження.

Масове впровадження інструментів ШІ починає руйнувати це припущення. Коли наукові статті, аналітичні звіти, новини, навчальні матеріали і навіть системи їхньої оцінки дедалі частіше створюються або фільтруються алгоритмами, виникає нова проблема. Суспільство може зіткнутися з тим, що дослідники називають колапсом епістемічної легітимності, ситуацією, коли звичні підстави довіряти знанням просто перестають працювати.

І це вже не теоретична загроза. Дослідники помічають явище, яке називають “алгоритмічною гомогенізацією” контенту. Системи ранжування часто віддають перевагу текстам, що відповідають формальним стилістичним шаблонам, саме таким, які легко відтворює ШІ. У результаті нестандартні, але оригінальні людські дослідження можуть опинитися на периферії інформаційного простору [1].

Наслідком цього процесу є збіднення інтелектуального середовища. Простір для нетипових ідей звужується, наукові дискусії втрачають евристичну глибину, а загальний масив знань поступово стає більш усередненим, поверховим і менш методологічно незалежним.

Ще один важливий аспект стосується когнітивних наслідків активного використання ШІ. Психологічні та педагогічні дослідження останніх років фіксують тривожну тенденцію коли люди систематично передають алгоритмам інтелектуальні завдання, це може послаблювати критичне мислення та знижувати творчі здібності.

Тут виникає парадокс. Технологія, яка позиціонується як інструмент розширення людських можливостей, може поступово обмежувати їх, якщо використовується без рефлексії та балансу.

Особливо відчутно ці зміни проявляються в освіті. Якщо студент перекладає виконання навчальних завдань на алгоритм, він не формує необхідних компетентностей. Але проблема існує і з іншого боку, коли викладач, який постійно покладається на ШІ під час підготовки до занять, ризикує поступово втратити глибину власного розуміння предмета. У ширшій перспективі така двостороння залежність може призвести до ослаблення інституційної пам’яті науки та уповільнення наукового прогресу.

Нарешті, є ще один вимір проблеми, який стосується автентичності історичних і документальних джерел. Сучасні генеративні системи вже здатні створювати тексти, зображення, відео та аудіо, що майже бездоганно імітують будь-який стиль, епоху або авторство. У такій ситуації виникає фундаментальне питання *чи можемо ми бути впевнені у справжності джерел?* І це питання виходить далеко за межі академічної науки. Воно має пряме значення для правосуддя, державного управління та навіть для збереження культурної пам’яті й ідентичності суспільства.

Чи можемо ми вплинути на ці тенденції? І чи здатне людство використати можливості штучного інтелекту так, щоб вони справді сприяли нашому розвитку? Це

складні, але цілком закономірні запитання, які сьогодні постають перед науковцями, освітянами та суспільством загалом.

Так, людство здатне використати потенціал ШІ на свою користь. Проте цей потенціал буде реалізований не всюди і не всіма. Ймовірно, лише частина суспільства зможе по-справжньому інтегрувати ШІ як інструмент розвитку, а не як заміну власного мислення. Для цих людей ШІ стане інтелектуальним підсилювачем, допоможе швидше аналізувати інформацію, відкривати нові зв'язки між ідеями та зосереджуватися на творчих і складних завданнях.

Водночас інша частина суспільства може використати ті самі технології як спосіб уникати інтелектуальних зусиль. У такому випадку ШІ перестає бути інструментом розвитку і перетворюється на механізм поступової залежності від алгоритмів.

Саме тому ключове питання полягає не лише в самій технології, а в культурі її використання. Якщо освіта, наукові інституції та суспільні норми зможуть сформувати відповідальне ставлення до ШІ, як до допоміжного інструменту, а не заміни людського мислення, тоді технологія дійсно може стати потужним ресурсом прогресу. Але цьому потрібно вчити вже у молодших класах.

Інакше кажучи, майбутнє взаємодії людини та ШІ залежить передусім від того, чи зможе сама людина зберегти активну роль у процесі мислення, пізнання і творчості. Саме в цьому і полягає головний виклик нової цифрової епохи, яка вже настала.

Метою статті є комплексний аналіз правових та соціально-цивілізаційних наслідків створення штучного загального інтелекту (AGI), виявлення системних ризиків, що виникають у зв'язку з переходом від вузьких ШІ-систем до загального та надрозумного штучного інтелекту, а також обґрунтування необхідності формування якісно нового режиму правового управління технологіями. Для реалізації визначеної мети передбачається вирішення таких *наукових завдань*: дослідити еволюцію концепції штучного інтелекту від вузьких систем до AGI; виявити потенційні соціально-економічні наслідки AGI у сферах наукового прогресу, трансформації ринку праці та державного управління; визначити основні ризики AGI для фундаментальних прав людини, включаючи право на приватність, принцип недискримінації, свободу вираження поглядів та цілісність демократичних процесів; сформулювати рекомендації щодо правового режиму AGI, включаючи механізми юридичної відповідальності розробників і операторів, питання правосуб'єктності систем та принципи превентивного регулювання.

Аналіз сучасного стану досліджень. Наукова дискусія щодо правових і соціальних вимірів AGI перебуває на етапі активного формування та характеризується вираженою міждисциплінарністю, поєднуючи здобутки правознавства, комп'ютерних наук, етики та соціальної філософії. Попри зростаючий масив публікацій, проблема комплексного правового режиму для AGI як системної технологічної потуги залишається недостатньо розробленою.

Серед досліджень, що формують доказову базу для правового осмислення AGI, визначальне місце посідає "AI Index Report 2025" Стенфордського університету [14], який систематизує кількісні та якісні тенденції розвитку ШІ від динаміки обчислювальних потужностей до зміни бізнес-процесів та ринку праці. Окремий вимір управлінських ризиків AGI представлено у звіті "Стан майбутнього 20.0" [8], де прямо констатується, що управління AGI може стати найскладнішим викликом, з яким людство будь-коли стикалося, а неготовність до нього кваліфікується як потенційно фатальна помилка цивілізаційного масштабу. Часові горизонти появи AGI та прогнози

провідних технологічних лідерів систематизовано у матеріалах AGI Predictions Timeline [9], що дозволяє ідентифікувати практичні дедлайни для нормотворчої діяльності.

В українській науці системний аналіз ризик-ландшафту ШІ здійснено в аналітичній доповіді Центру Разумкова “Штучний інтелект — можливості, небезпеки, фактори ризику” (жовтень 2025) [3], яка є одним із перших україномовних досліджень, що розглядає ШІ комплексно у технологічному, соціальному та безпековому вимірах. У сфері протидії дезінформації на базі ШІ вагомим є дослідження Марущака, Петрова [2], присвячене досвіду України щодо національного регулювання ШІ-дезінформації у порівняльній перспективі.

Проблему гомогенізації знань та збіднення інтелектуального середовища внаслідок масового застосування генеративного ШІ досліджено у роботі Raghavan у рамках MIT GenAI program [1]. Це дослідження є важливим підґрунтям для правового осмислення епістемічних ризиків ШІ та обґрунтування регуляторних вимог до прозорості алгоритмічного ранжування контенту. Питання правосуб’єктності та відповідальності у контексті ШІ розглядається у роботі Tait, присвяченій концепції “мінімально необхідної особи” [10], що є релевантним для дискусії про межі правових фікцій стосовно AGI-систем.

У сфері нормативного регулювання центральне місце посідають матеріали, пов’язані з імплементацією AI Act [4] та аналітикою Європейського парламентського дослідницького сервісу щодо “Digital Omnibus on AI” [5] як пакету уточнень до регламенту. Принципово важливим є документ Європейської комісії про відкликання пропозиції щодо Директиви про відповідальність за ШІ [11, 12], що засвідчує зміну регуляторної стратегії ЄС і переорієнтацію на посилення відповідальності через вже чинні механізми. Міжнародний вимір регулювання представлено Блетчлійською декларацією [7, 20], Рамковою конвенцією Ради Європи [16], матеріалами ОЕСР щодо ризиків та інцидентів, пов’язаних із ШІ [17], а також Декларацією лідерів Саміту впливу ШІ у Нью-Делі (лютий 2026 року) [6]. Водночас, незважаючи на зростаючий масив досліджень, проблема комплексного правового режиму для AGI як системної технологічної потуги залишається недостатньо розробленою: більшість наявних праць зосереджена або на вузькоприкладних аспектах окремих застосувань ШІ, або на загальних етичних принципах, не переходячи до конкретних правових механізмів управління системним ризиком.

Методологічну основу дослідження становить система загальнонаукових і спеціально-правових методів пізнання. Порівняльно-правовий метод застосовується при аналізі різних підходів до регулювання ШІ європейського (AI Act, Конвенція Ради Європи), міжнародно-організаційного (ОЕСР, ЮНЕСКО) та окремих національних моделей, що дозволяє виявити спільні принципи та суттєві відмінності регуляторних рамок. Системний метод використовується для дослідження AGI як явища, що одночасно є технологічним, соціально-економічним та правовим феноменом, елементи якого перебувають у складній взаємозалежності. Прогностичний метод забезпечує аналіз часових горизонтів появи AGI та моделювання правових наслідків різних сценаріїв його розвитку. Метод критичного аналізу наукових і нормативних джерел застосовується для оцінки достатності чинних регуляторних інструментів щодо управління ризиками рівня AGI. Нарешті, формально-юридичний метод використовується при тлумаченні конкретних нормативних положень, зокрема AI Act, Рамкової конвенції Ради Європи та актів ОЕСР та при формулюванні правових рекомендацій.

Виклад основного матеріалу. Перше десятиліття XXI століття позначилось інтенсивним розвитком цифрових технологій, однак саме у 2020-х роках штучний інтелект перетворився на одну з найвпливовіших сил глобальних трансформацій. Від чат-ботів і систем розпізнавання образів до великих мовних моделей, здатних генерувати переконливий текст, зображення, програмний код і наукові гіпотези, технологічна еволюція ШІ набула безпрецедентних темпів. Цілком ймовірно, що 2026 рік стане роком переходу від систем “вузького” штучного інтелекту (Narrow AI) до моделей загального штучного інтелекту (Artificial General Intelligence, AGI). Якщо попереднє десятиліття було присвячене регулюванню конкретних алгоритмічних рішень у сфері розпізнавання обличчя чи кредитних скорингів, то контекст 2026 року вимагає осмислення систем, здатних до міждоменного навчання, каузального мислення та автономного визначення цілей. Більше того, вже зараз мова йде про гіпотетичний надрозумний штучний інтелект (SAI / Superintelligent AI / ASI), ознаками якого будуть: інтелектуальна перевага над людиною у всіх доменах; здатність до самовдосконалення (recursive self-improvement); потенційна автономність у прийнятті рішень; можливість створення нових наукових парадигм [2, 3].

2026 рік знаменним буде й у правовому вимірі саме через перехід до практичної реалізації норм Закону ЄС про ШІ (AI Act) [4]. Базова дата загального застосування AI Act 2 серпня 2026 року, водночас окремі розділи набрали чинності раніше. Паралельно інституції ЄС обговорюють “Digital Omnibus on AI” як пакет цільових змін, покликаних спростити/уточнити імплементацію AI Act [5]. А 20 лютого 2026 року ЄС схвалив Декларацію лідерів на Саміті впливу штучного інтелекту 2026 року в Нью-Делі, в якій визнається, що *“перспективи штучного інтелекту найкраще реалізуються лише тоді, коли його переваги поширюються на людство”* [6].

На наше переконання, перехід від вузького ШІ до концепції AGI є не просто технологічним, а фундаментальним цивілізаційним зрушенням. Якщо системи вузького ШІ вирішують конкретні завдання в межах визначеної предметної галузі, то AGI, за своїм теоретичним визначенням, здатний здійснювати когнітивну діяльність загального характеру, зокрема навчатися, адаптуватися, розмірковувати і діяти в непередбачуваних ситуаціях так само ефективно, як і людина або навіть перевершуючи її. Ця перспектива породжує принципово нові питання як правового, так і етичного та соціального характеру.

Вже зараз можна визначити ряд конкретних тенденцій у розвитку ШІ, які безпосередньо визначитимуть траєкторію розвитку права у цій сфері. Зокрема:

масштабування, збільшення параметрів, даних і обчислень демонструє передбачуваний зв'язок із поліпшенням якості мовних моделей; класичні емпіричні “закони масштабування” показують, що продуктивність зростає зі збільшенням model size, dataset size і compute згідно з наближеними степеневими залежностями. Із правової перспективи це важливо тому, що обчислювальний бюджет і масштаб моделі стають проксі-індикаторами потенційних ризиків, тобто можуть використовуватися як тригери додаткових обов'язків на кшталт посиленних оцінок безпеки або постачання технічної документації [7];

по-друге, зростає кількість систем, що поєднують різні модальності (текст, зображення, звук, відео). Правові наслідки проявляються у складності оцінки ризиків, адже мультимодальні системи можуть впливати не лише на інформаційні потоки, а й на фізичні процеси (наприклад у транспорті чи промисловості), що підвищує значущість норм про безпеку, прозорість та відповідальність [7];

по-третє, у 2025 році фіксується розвиток автономних AI-агентів, систем здатних самостійно планувати послідовності дій, використовувати зовнішні інструменти (веб-пошук, виконання коду, взаємодія з інтерфейсами) та рефлексувати над власними результатами. Фреймворки на кшталт AutoGPT, AgentGPT і ReAct демонструють перші кроки в напрямку автономного вирішення складних завдань. Для правового аналізу саме агентність є мостом до AGI-дискурсу, оскільки автономність, багатокрокове планування і здатність взаємодіяти з інструментами змінюють профіль відповідальності, вимоги до людського нагляду і параметри делегування рішень алгоритмам. Відповідно до виконавчого резюме звіту “Стан майбутнього 20.0” управління AGI може стати найскладнішим і найважчим управлінським викликом, із яким людство коли-небудь стикалося. Як зазначає Стюарт Рассел у розділі 3: *“Ба більше, якщо не вирішити це завдання до створення систем ЗШІ, це стало би фатальною помилкою для людської цивілізації. Ніхто не має права допустити таку помилку”*. Наразі ніщо не заважає людству допустити таку помилку. Оскільки AGI може з’явитися протягом цього десятиліття, необхідно вже зараз почати створювати національні та наднаціональні системи управління, які забезпечать керований перехід від сучасних форм ШІ до майбутніх форм AGI так, щоб його розвиток був на користь людства. Якщо ми зробимо це правильно, майбутнє цивілізації може бути справді прекрасним для всіх [8].

Проблема визначення часових горизонтів появи AGI залишається однією з найбільш дискусійних. Упродовж 2025–2026 років відбувся суттєвий зсув у бік більш ранніх прогнозів, що пов’язано зі стрімким прогресом мультимодальних моделей, автономних агентів та систем із елементами причинно-наслідкового міркування. Особливо помітними є оцінки представників технологічного сектору, які безпосередньо працюють над розробкою моделей, що наближаються до рівня загального інтелекту.

Серед найбільш оптимістичних прогнозів варто виокремити позиції керівників провідних AI-компаній. Згідно з агрегованими даними AGI Predictions Timeline (2026), Сем Альтман (OpenAI) оцінює ймовірність появи AGI у проміжку 2025-2027 років, що робить його одним із найрадикальніших прихильників швидкого настання епохи загального інтелекту. Подібної точки зору дотримується і Даріо Амодей, генеральний директор Anthropic, який у 2026 році прогнозує появу AGI вже у 2026-2027 роках, підкреслюючи, що сучасні моделі демонструють поведінку, яку раніше вважали недосяжною для вузького ШІ. До оптимістичного табору належать також ключові фігури, пов’язані з Google та Microsoft. Співзасновник Google Сергій Брін у 2026 році оцінює можливу появу AGI у діапазоні 2028-2030 років, наголошуючи на швидкому прогресі в архітектурах, здатних до узагальнення знань. Колишній CEO Google Ерік Шмідт висловлює схожий прогноз – 2028-2031 роки, підкреслюючи, що розвиток AGI є не лише технічним, а й геополітичним викликом. Мустафа Сулейман, керівник Microsoft AI та співзасновник DeepMind, у 2026 році оцінює появу AGI у межах 2028-2032 років, зазначаючи, що сучасні системи вже демонструють “зародкові форми загального міркування” [9].

Власне таким чином і обмежуються часові рамки для впровадження відповідних правових норм. Однозначно знову серед трендових проблем будуть питання правосуб’єктності ШІ. Історично правосуб’єктність ніколи не була обмежена лише природними особами. Римське право використовувало фікції, а сучасне право надає статус особи корпораціям, муніципалітетам та навіть природним об’єктам, таким як річки. Однак, як зазначають сучасні дослідники, надання статусу особи ШІ розглядається переважно як “політика уникнення відповідальності” реальними власниками [10]. Вважаємо, що правосуб’єктність AGI є передчасним і потенційно

небезпечним кроком, що може розмивати відповідальність людини за функціонування систем та знижувати рівень захисту прав людини. Натомість на нашу думку слід розвивати концепцію “AGI як об’єкта підвищеної правової уваги”, тобто системи, що не є суб’єктом, але вимагає спеціального правового режиму.

Цікавим є той факт, що у Робочій програмі Європейської Комісії на 2025 рік було офіційно відкликано пропозицію щодо Директиви про відповідальність за штучний інтелект [11], що засвідчує зміну регуляторної стратегії ЄС у сфері ШІ. У документі Комісія прямо зазначає, що не бачить “жодної передбачуваної можливості досягнення політичної згоди” щодо цього акта, а тому вважає за доцільне переглянути підхід до регулювання відповідальності за шкоду, спричинену системами ШІ. Такий крок свідчить про перехід від спроби створити окремих горизонтальний інструмент до більш прагматичної моделі, орієнтованої на емпіричну категоризацію ризиків та посилення відповідальності розробників і постачальників через уже чинні механізми, зокрема через імплементацію AI Act. Проте це також може свідчити й про тиску з боку галузевих лобістів, які розглядають будь-які правила відповідальності як екзистенційну загрозу своїм бізнес-моделям [12]. Така зміна підходу може мати значний вплив на формування європейської моделі регулювання ШІ, зміщуючи акцент на доказову базу, технічні стандарти та суворіші вимоги до розробників високоризикових систем.

Якщо брати до уваги концепції технологічної сингулярності Вернора Віджі і Рейя Курцвейла, то правові системи зобов’язані передбачати механізми запобіжного управління, які здатні функціонувати в умовах гранично стрімких технологічних змін. Вже сьогодні системи на кшталт AlphaFold 3 (результат співпраці Google DeepMind та Isomorphic Labs) вирішують задачі прогнозування структури білків, що ще кілька десятиліть тому вважалися принципово недоступними для комп’ютерів [13]. AGI, за прогнозами, міг би одночасно аналізувати десятки тисяч наукових статей, виявляти несподівані зв’язки між різними галузями знань і пропонувати нові теоретичні рамки. Відкриття нових матеріалів, зокрема суперпровідників, катализаторів, метаматеріалів, фармацевтичних речовин вже зараз відбувається за допомогою ШІ-асистованого скринінгу. AGI міг би вивести цей процес на рівень справжньої автономної наукової творчості. Наслідки для енергетики (термоядерний синтез, ефективні сонячні батареї), медицини (персоналізована терапія) та промисловості (нові технологічні процеси) важко переоцінити.

У сфері медицини AGI відкриває перспективи для принципово нових підходів: від раннього виявлення раку на основі аналізу геномних даних до прискореної розробки вакцин і персоналізованих терапевтичних протоколів. Симуляція клінічних випробувань дозволила б скоротити час розробки нових ліків з 10-15 до 2-3 років.

Автоматизація інтелектуальної праці є, мабуть, найбільш обговорюваним соціально-економічним наслідком AGI. На відміну від попередніх хвиль автоматизації, що торкалися переважно рутинної фізичної праці, AGI загрожує витісненням із ринку праці юристів, лікарів, журналістів, аналітиків, архітекторів та представників інших когнітивних професій.

За даними звіту аналітиків Стенфордського університету, масове використання вузьких систем уже відображається у зміні бізнес-процесів. Швидке зростання частки організацій, що застосовують ШІ, свідчить про зсув до “AI-enabled” продуктивності та конкуренції. Також зазначається, що штучний інтелект підвищує продуктивність праці та в більшості випадків допомагає скоротити розрив у кваліфікації серед працівників [14]. Згідно із цим звітом ШІ перестав бути допоміжним інструментом і почав відігравати роль “активного учасника” і лікувального процесу. Поява біомедичних

фундаційних моделей, навчених на масивах даних, що за масштабом не поступаються тим, на яких навчалися чат-боти, дозволила створювати інструменти для діагностики рідкісних хвороб та виробництва окремих ліків.

На початку 2026 року OpenAI оголосила про ChatGPT for Health, позиціонуючи мовну модель загального призначення як інструмент для отримання інформації, пов'язаної зі здоров'ям, та взаємодії з пацієнтами. Штат Юта став першим штатом, який дозволяє мешканцям поновлювати свої ліки онлайн через комерційну платформу штучного інтелекту без необхідності попередньо спілкуватися з лікарями. OpenEvidence, платформа медичних доказів на базі штучного інтелекту, розроблена переважно для клініцистів та медичних працівників, стала домінуючим гравцем у прийнятті рішень у місцях надання медичної допомоги, підкреслюючи той факт, що лікарі часто обходять традиційні IT-контролери, щоб використовувати ШІ в клінічній допомозі [15].

Використання ШІ-систем для підтримки або автоматизації адміністративних рішень активно застосовується у сферах розподілу соціальної допомоги, прогнозування правопорушень та оцінки кредитоспроможності. AGI міг би вивести цей процес на якісно інший рівень, беручи на себе управлінські функції у масштабах цілих міністерств або державних програм.

Прогнозування політики за допомогою AGI передбачає моделювання наслідків законодавчих змін, бюджетних рішень та регуляторних заходів з урахуванням складних системних взаємозалежностей. Такі інструменти могли б підвищити якість державних рішень, проте одночасно породжують серйозні ризики: непрозорість алгоритмічного мислення, акумулювання влади у руках тих, хто контролює системи, та ерозія демократичної підзвітності.

Концепція “цифрових держав”, де AGI інтегрований у інфраструктуру реєстрів, судових систем, систем безпеки та охорони здоров'я, відкриває перспективи ефективнішого та більш рівномірного надання публічних послуг. Однак реалізація цієї перспективи, на наше переконання, потребує надійних правових механізмів, що гарантують підзвітність, оскарження рішень та захист від системних збоїв.

Коли ми говоримо про AGI у правовому контексті, важливо дивитися на ризики ширше, ніж просто на “побічні ефекти технології”. Вважаємо, що мова йде про можливий перерозподіл влади між державою, великими компаніями та окремими людьми. І це вже питання конституційного масштабу. Тому юридична дискусія зосереджується на кількох ключових темах: хто контролює ці системи, хто несе відповідальність за їхні рішення, наскільки концентруються ресурси, і як при цьому зберегти фундаментальні права людини.

У цьому контексті особливої важливості набуває проблема, яка полягає в тому, що сучасні великі моделі, а тим більше потенційні AGI-системи, потребують колосальних обчислювальних потужностей і величезних масивів даних. Через це реальні можливості розробки та контролю таких технологій можуть опинитися в руках дуже вузького кола держав і корпорацій.

Для права це означає нові виклики. Потрібні механізми прозорості, нагляду та антимонопольного контролю, які не дозволять технологічним гігантам фактично перебрати на себе регуляторні функції. Інакше може виникнути ситуація, коли монополія на обчислювальні ресурси й дані фактично визначатиме правила гри для всіх інших.

З юридичної точки зору важливо, щоб система регулювання ШІ прямо охоплювала ключові права людини. Серед них зокрема право на приватність і захист персональних

даних, принцип рівності та недискримінації, захист демократичних процесів і доступ до ефективних механізмів правового захисту. У міжнародному праві ці принципи вже почали закріплюватися. Наприклад, відповідна конвенція Ради Європи визначає мету регулювання як забезпечення того, щоб розробка й використання ШІ протягом усього його життєвого циклу були сумісними з правами людини, демократією та верховенством права. Документ також підкреслює важливість прозорості, нагляду, підзвітності, недискримінації та захисту приватності, а також передбачає доступні й ефективні засоби правового захисту [16].

Ще один важливий аспект полягає у формуванні політики на основі реальних даних. Організація економічного співробітництва та розвитку (ОЕСР) підкреслює необхідність створення доказової бази для регулювання ШІ. Один із ключових інструментів тут систематичний моніторинг інцидентів та небезпечних випадків, пов'язаних із використанням ШІ [17].

Для систем рівня AGI це набуває ще більшого значення. Чим вищий рівень автономії технології, тим важливішими стають оперативний нагляд, стандартизований механізм повідомлення про інциденти та обов'язковий аналіз таких випадків після їх виникнення. Саме такі механізми дозволяють виявляти повторювані ризики й формувати ефективну політику безпеки. Ми маємо також враховувати, що вже зафіксовані численні випадки алгоритмічної дискримінації у кредитуванні, найманні на роботу та медичній діагностиці. AGI, навчений на упередженому соціальному досвіді людства, ризикує відтворювати та посилювати наявні нерівності у безпрецедентних масштабах, охоплюючи всі сфери суспільного життя одночасно. Наприклад уже зафіксовано задокументовані випадки алгоритмічної дискримінації. У сфері найму одним із найвідоміших прикладів став позов *Mobley v. Workday* (2024), у якому позивачі стверджують, що алгоритмічна система *Workday* систематично відхиляла кандидатів за ознаками раси, віку та інвалідності, що стало підставою для першого у США групового позову проти AI-рекрутингової платформи [18].

Вважаємо, що ключовою правовою проблемою AGI є небезпека втрати ефективного людського контролю. Автономність системи, що характеризується здатністю самостійно переслідувати цілі в довгостроковій перспективі, може призвести до ситуацій, у яких рішення AGI не лише виходять за межі людського розуміння, а й завдають шкоди інтересам окремих осіб або суспільства загалом. Складність алгоритмічних рішень, прийнятих AGI-системами, суттєво ускладнює їхній правовий аналіз. Якщо сьогодні суд може вимагати від розробника пояснити, чому система відмовила у кредиті або поставила відповідний діагноз, то у разі AGI-систем з трильйонами параметрів і складними ланцюгами міркувань такі пояснення можуть бути принципово недоступними навіть для авторів системи.

Можемо констатувати, що свобода вираження поглядів зазнає подвійного ризику. З одного боку, AGI-системи, здатні до гіперперсоналізованої генерації контенту, можуть використовуватися для маніпулятивних кампаній і дезінформації нового рівня складності. З іншого боку, автоматизована модерація контенту за допомогою AGI може призводити до систематичного подавлення законних висловлювань, що не відповідають тренувальним уявленням системи про “допустиме”.

Крім того, демократичні процеси також є вразливими перед AGI-системами, здатними до цілеспрямованого мікротаргетингу виборців, фабрикації достовірних дипфейків та управління інформаційним порядком денним. Вибори, референдуми, парламентські дебати, всі ці інститути демократії залежать від здатності громадян

приймати раціональні рішення на підставі достовірної інформації і AGI може радикально підірвати цю основу.

Підсумовуючи наше дослідження, акцентуємо увагу на ряді тривожних маркерів, які не слід випускати із поля зору. Якщо подивитися на те, як змінювалися уявлення про безпеку ШІ в провідних технологічних організаціях, можна побачити досить тривожну тенденцію. Вона має пряме значення для права та майбутнього регулювання ШІ. На початку серйозної дискусії про ризики ШІ, приблизно у 2015 році, поняття безпеки охоплювало значно ширший горизонт. Йшлося не лише про окремі технічні проблеми, а про можливу втрату контролю над системами, здатними перевершити людський інтелект. Іншими словами, безпека тоді розумілася як захист людства від потенційних наслідків появи надпотужного суперінтелекту.

Однак уже до 2020 року фокус почав помітно змінюватися. Дискусія дедалі частіше концентрувалася на більш вузьких питаннях, шкідливому контенті, помилках моделей або операційних ризиках конкретних систем. Ці проблеми справді важливі, але вони значно звужують початкове розуміння того, що означає “безпека ШІ”.

До 2025 року у публічному дискурсі частини великих технологічних компаній поняття безпеки іноді зводиться майже виключно до юридичної відповідальності за певні категорії контенту. Така еволюція виглядає не просто зміною термінів або технічної мови. Вона радше свідчить про глибший процес: поступове зміщення фокусу від глобальної відповідальності до управління корпоративними ризиками.

Інакше кажучи, первісна ідея відповідального розвитку ШІ поступово поступається комерційній логіці. Безпека починає трактуватися не як захист фундаментальних інтересів людства, а як спосіб мінімізувати репутаційні втрати чи судові ризики для компаній. Особливу тривогу викликає те, що це звуження відбулося паралельно з безпрецедентним зростанням технологічних можливостей.

Ця тенденція також ставить під сумнів ефективність саморегулювання індустрії. Галузь, яка спочатку декларувала відповідальність перед людством, під тиском конкуренції, інвестицій та швидких технологічних циклів демонструє труднощі у підтриманні власних нормативних стандартів. У такій ситуації держави та міжнародна спільнота навряд чи можуть і надалі покладатися лише на добровільні принципи або корпоративні хартії.

Особливо це актуально на тлі наближення горизонту AGI. У таких умовах головний нормативний висновок полягає в необхідності якісно нового підходу до правового регулювання. Йдеться про перехід від фрагментарного контролю окремих застосувань вузького ШІ до системного управління технологічною потужністю як такою. Сучасні *frontier models*, системи загального призначення (*general-purpose AI*) та автономні агентні архітектури є принципово новим об’єктом регулювання. Їхня відмінність полягає не лише в тому, що вони виконують певні функції краще за попередні системи. Значно важливіше те, що вони мають системний потенціал впливу, тобто здатність трансформувати цілі сфери суспільного життя.

З огляду на окреслені проблеми, на глобальному рівні дискусія про регулювання AGI зосередилась навколо кількох ключових питань [19]. *По-перше*, щодо міжнародних стандартів безпеки, учасники Блетчлійської декларації країн-учасниць Саміту з безпеки штучного інтелекту (2023) та її наступники сформулювали першу спільну позицію провідних держав щодо ризиків “прикордонних” ШІ-систем та необхідності координованого підходу до оцінки їхньої безпеки. Однак декларативний характер цих домовленостей поки що не перетворився на обов’язкові механізми [20].

По-друге, обговорюється питання ліцензування потужних AI-моделей у частині чи повинні компанії, що розробляють системи з обчисленням понад певний поріг, проходити обов'язкову сертифікацію безпеки аналогічно до ядерних об'єктів або фармацевтичних препаратів? Такі пропозиції, висловлені зокрема Центром з управління ШІ, знаходять підтримку в частині дослідницького співтовариства, проте зіштовхуються з опором технологічної індустрії [21].

По-третє, обговорюється ідея глобального наглядового органу, свого роду "МАГАТЕ для ШІ". Такий орган міг би здійснювати моніторинг найпотужніших ШІ-систем, встановлювати стандарти їхньої оцінки та слугувати форумом для координації між державами у надзвичайних ситуаціях, пов'язаних із ШІ. Ця ідея залишається суперечливою з огляду на складнощі суверенітету та верифікації.

На нашу думку, найбільш практично значущим правовим питанням у контексті AGI на даний час є визначення суб'єкта юридичної відповідальності за шкоду, заподіяну системою. Власне це те питання, яке явним, очевидним і можливим для правової інтерпретації. Традиційні концепції деліктної відповідальності передбачають наявність вини, причинно-наслідкового зв'язку та суб'єкта, здатного нести відповідальність. AGI, що діє автономно і непередбачувано, ускладнює застосування кожного з цих елементів.

Відповідальність розробників є однією з можливих моделей. Розробник AGI несе відповідальність за шкоду, спричинену системою, незалежно від наявності вини, за аналогією з відповідальністю виробника за дефектну продукцію. Директива ЄС про відповідальність за ШІ частково рухається в цьому напрямку, встановлюючи презумпцію причинного зв'язку для систем ШІ, що не відповідають стандартам AI Act. Проте механізм відповідальності не є достатнім для систем, що здатні навчатися і змінювати свою поведінку після виходу на ринок.

Відповідальність операторів систем, осіб або організацій, що використовують AGI, є другою можливою моделлю. Ця концепція ставить знак рівності між AGI і складним інструментом, що потребує ліцензованого оператора. За аналогією з пілотуванням літака або ядерною енергетикою, оператор AGI міг би нести відповідальність за шкоду, **якщо не вжив усіх необхідних заходів безпеки**. Однак якщо AGI функціонує автономно і його дії виходять за межі того, що оператор міг передбачити, ця модель також виявляється недостатньою.

Практичним рішенням може бути і гібридний підхід у рамках якого розробники несуть відповідальність за відповідність системи стандартам безпеки на момент виходу на ринок; оператори за належне використання та налаштування системи; держава за достатність регуляторної рамки.

Висновки. З урахуванням проведеного дослідження. Можемо виокремити ряд принципово важливих аспектів, які потребують особливої правової уваги.

По-перше, AGI є не лише технологічним, а й цивілізаційним явищем, що потребує комплексного осмислення в правовій, етичній і соціальній площинах. Еволюція від вузького ШІ до систем, здатних до загального когнітивного функціонування, є якісним стрибком, що ставить під сумнів ефективність правових режимів, розроблених для попередніх поколінь технологій.

По-друге, необхідність раннього правового регулювання AGI є очевидною і не залежить від точних прогнозів щодо строків його появи. Досвід регулювання Інтернету, соціальних мереж та криптовалют переконливо засвідчило, що коли правові рамки формуються постфактум, суспільство зазнає значних збитків, що могли б бути попереджені. Превентивне законодавство, що встановлює вимоги до розробки, тестування і впровадження потужних ШІ-систем, є не гальмом для інновацій, а

необхідною умовою їхнього відповідального розвитку. Діалог між правниками, технологіями та представниками громадянського суспільства повинен розпочатися зараз, до того, як AGI перетвориться на реальність.

По-третє, пріоритет захисту прав людини у цифрову епоху є системоутворюючим принципом, навколо якого повинне будуватися правове регулювання AGI. Приватність, недискримінація, свобода слова, доступ до правосуддя та демократичне самовизначення є не технічними вимогами, а фундаментальними цінностями, що не підлягають компромісу навіть заради максимізації ефективності або ж конкурентних переваг. Будь-яка правова рамка регулювання AGI, що не ставить захист цих прав на чільне місце, є неприйнятною.

По-четверте, правова наука ще не виробила вичерпних відповідей на питання відповідальності за шкоду від AGI та правосуб'єктності таких систем. Поточний консенсус схиляється до гібридної моделі відповідальності розробників і операторів при збереженні AGI виключно як об'єкта, а не суб'єкта права. Однак ці рішення потребують постійного перегляду в міру розвитку технологій і накопичення практики.

По-п'яте, глобальний характер AGI вимагає глобальної координації правового регулювання. Фрагментація правового простору між юрисдикціями не лише знижує ефективність захисту прав, а й створює умови для “регуляторного арбітражу”, переміщення розробки AGI в юрисдикції з найменш суворим контролем. Такі міжнародні механізми як Принципи ОЕСР щодо штучного інтелекту, Рекомендація ЮНЕСКО щодо етики штучного інтелекту, Конвенція Ради Європи та потенційні угоди у форматі G7/G20 є необхідними, але недостатніми. Потрібен більш масштабний крок у напрямку юридично обов'язкового глобального договору про регулювання потужних ШІ-систем.

Перспективними напрямками подальших досліджень є розробка конкретних правових механізмів верифікації дотримання стандартів безпеки AGI; дослідження питань юрисдикції та застосовного права до AGI-систем, що функціонують у транскордонних контекстах; аналіз правових наслідків розробки AGI для сфери праці та соціального захисту; вивчення можливостей використання самого ШІ для вдосконалення правового регулювання (так зване “RegTech for AGI”); а також дослідженням специфічного українського виміру регулювання AGI в контексті євроінтеграції та цифрової трансформації держави.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Список використаних джерел

1. Raghavan M. Measuring and Mitigating Homogenization in Generative AI. Massachusetts Institute of Technology URL: https://genai.mit.edu/measuring-and-mitigating-homogenization-in-generative-ai/?utm_source=copilot.com
2. Marushchak A, Petrov S., Khoperiya A. Countering AI-powered disinformation through national regulation: learning from the case of Ukraine. *Front. Artif. Intell.*, 07.01.2025 URL: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1474034/full?utm_source=copilot.com
3. Пищуліна О. Штучний інтелект – можливості, небезпеки, фактори ризику. Центр Разумкова. Жовтень 2025. URL: <https://razumkov.org.ua/images/2025/10/10/2025-AI.pdf>
4. The EU Artificial Intelligence Act. Up-to-date developments and analyses of the EU AI Act. URL: <https://artificialintelligenceact.eu/>

5. Digital Omnibus on AI. European Parliamentary Research Service. 2026 URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782651/EPRS_BRI%282026%29782651_EN.pdf
6. European Union endorses Leaders' Declaration at AI Summit in India. European Commission. 20.02.2026 URL: <https://digital-strategy.ec.europa.eu/en/news/european-union-endorses-leaders-declaration-ai-summit-india>
7. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. GOV.UK 13.02.2025 URL: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>
8. Офіційний стислий виклад звіту «Стан майбутнього 20.0». URL: <https://www.millennium-project.org/wp-content/uploads/2026/02/Ukrainian-Executive-Summary.pdf>
9. When Will AGI Arrive? URL: https://theagiclock.com/?utm_source=copilot.com
10. Izak Tait MVP: The Minimal Viable Person. Preprints.org. 20.05.2025 URL: <https://www.preprints.org/manuscript/202505.1625>
11. Liability Rules for Artificial Intelligence. URL: https://commission.europa.eu/topics/business-and-industry/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en
12. Andrews C. European Commission withdraws AI Liability Directive from consideration. IAPP. 12.02.2025 URL: https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration?utm_source=copilot.com
13. How does AlphaFold Server work? URL: <https://alphafoldserver.com/welcome>
14. The 2025 AI Index Report. Stanford University URL: <https://hai.stanford.edu/ai-index/2025-ai-index-report>
15. Handler R. Clinical AI Has Boomed. Stanford Medicine. 15.01.2026 URL: <https://medicine.stanford.edu/news/current-news/standard-news/clinical-ai-has-boomed.html>
16. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law URL: <https://rm.coe.int/1680afae3c>
17. AI risks and incidents. OECD URL: <https://www.oecd.org/en/topics/sub-issues/ai-risks-and-incident.html>
18. Tyman A. Mobley v. Workday: Court Holds AI Service Providers Could Be Directly Liable for Employment Discrimination Under “Agent” Theory. Seyfarth. 19.06.2024 URL: <https://www.seyfarth.com/news-insights/mobley-v-workday-court-holds-ai-service-providers-could-be-directly-liable-for-employment-discrimination-under-agent-theory.html>
19. Деякі фрагменти цього тексту згенеровані за допомогою ChatGPT та Claude.
20. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 URL: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>
21. The Center for AI Safety (CAIS) is on a mission to reduce societal-scale risks from artificial intelligence. 2024 Impact Report URL: <https://safe.ai/work/impact-report/2024>

Олександр Дмитрович Довгань

доктор юридичних наук, професор, Заслужений діяч науки і техніки України
радник при дирекції Державної наукової установи «Інститут інформації, безпеки і права
Національної академії правових наук України».

04053, Україна, м. Київ, пров. Несторівський, 4

email: dod16.67@ukr.net

Тарас Юрійович Ткачук

доктор юридичних наук, професор

учений секретар наукової лабораторії (наукової установи) Українського науково-
дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
03113, Україна, м. Київ, вул. Миколи Василенка, 3

email: tarast25@gmail.com

Oleksandr D. Dovhan

Doctor of Law, Professor, Honored Worker of Science and Technology of Ukraine

Advisor to the Directorate of the State Scientific Institution "Institute of Information, Security
and Law of the National Academy of Legal Sciences of Ukraine"

4 Nestorivskyi Lane, Kyiv, 04053, Ukraine

email: dod16.67@ukr.net

Taras Yu. Tkachuk

Doctor of Law, Professor

Scientific Secretary of the Research Laboratory (Research Institution) of the Ukrainian
Research Institute of Special Equipment and Forensic Expertise of the Security Service of
Ukraine

3 Mykoly Vasylenka Street, Kyiv, 03113, Ukraine

email: tarast25@gmail.com

Рекомендоване цитування: Довгань О.Д., Ткачук Т.Ю. Artificial General Intelligence: новий етап глобальної правової дискусії. *Інформація і право*. № 1(56)/2026. 2026. С. 67-81. [https://doi.org/10.37750/2616-6798.2026.1\(56\).357246](https://doi.org/10.37750/2616-6798.2026.1(56).357246)

Suggested Citation: Dovhan O., Tkachuk T. (2026) Artificial General Intelligence: a New Chapter in the Global Legal Discourse. *Information and Law*. 1(56)/2026. 67-81. [https://doi.org/10.37750/2616-6798.2026.1\(56\).357246](https://doi.org/10.37750/2616-6798.2026.1(56).357246)

Дата надходження статті до редакції: 18.03.2026 р.

Дата прийняття статті до друку після рецензування: 29.03.2026 р.

Дата публікації (оприлюднення): 01.04.2026 р.
