

УДК 341.1/.8

Янишівський Михайло Мирославович

аспірант кафедри державної політики та врядування

Інституту адміністрування, державного управління та професійного розвитку

Національного університету «Львівська політехніка»

Yanishivsky Mykhailo

Graduate Student of the Department of Public Policy and Governance

Institute of Administration, Public Administration and Professional Development of

Lviv Polytechnic National University

ORCID: 0000-0002-8788-6339

Янишівський Тарас Ярославович

магістр освітньої програми "Права людини", спеціальність 081 "Право"

Українського католицького університету

Yanishivsky Taras

Master of the educational program "Human Rights", specialty 081 "Law"

Ukrainian Catholic University

ORCID: 0009-0005-6747-837X

**ПОЛІТИКА ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ШТУЧНОГО
ІНТЕЛЕКТУ: ПРОГРАМНІ ДОКУМЕНТИ, ЗАКОНОДАВСТВО ТА
ПРАКТИКА СУДУ ЄС**

**THE POLICY OF THE EUROPEAN UNION IN THE FIELD OF
ARTIFICIAL INTELLIGENCE: PROGRAM DOCUMENTS,
LEGISLATION AND PRACTICE OF THE EU COURT**

Анотація. Стаття присвячена розгляду політики Європейського Союзу (ЄС) у сфері технології штучного інтелекту (ШІ) через призму

аналізу програмних документів, чинного законодавства, проєктів нормативного регулювання на рівні ЄС та практики Суду ЄС.

Проблема формування політики ЄС у сфері ІІІ є актуальною з огляду на проривний розвиток технології ІІІ з одного боку, та необхідність імплементації європейського законодавства в процесі євроінтеграції України, з іншого боку.

Стаття розглядає ключові програмні документи ЄС щодо ІІІ, їх вплив на регулювання та стратегію розвитку цієї сфери. Згідно з ними, ЄС прагне створити людино-орієнтовану стратегію, сприяти інвестиціям, дослідженням та інноваціям, трансформації освіти та забезпечити доступ до технології ІІІ для громадян та бізнесу. Програмні документи ЄС встановлюють ключові елементи благонадійності ІІІ, такі як правомірність, етичність та надійність, а також наголошують на важливості цінностей, прав людини та прозорості. Ці документи відображають стратегічний погляд на ІІІ та закликають до постійного оновлення політики, враховуючи технологічний розвиток та соціальне середовище. З програмних документів ЄС щодо ІІІ впливають основні засади та пріоритети для майбутнього нормативного регулювання.

На сьогодні в ЄС спеціалізоване законодавство, що б безпосередньо регулювало ІІІ, відсутнє. Проте існують директиви та регламенти, які непрямо впливають на розробку та використання систем ІІІ. Наприклад, загальний регламент про захист даних (GDPR) встановлює обмеження для обробки персональних даних. Директива про авторське право на єдиному цифровому ринку впливає на розробку систем ІІІ, які працюють з авторськими матеріалами. Директива про відповідальність за продукцію встановлює відповідальність виробників за дефекти. До ІІІ також застосовуються регулювання щодо кібербезпеки.

Одночасно в ЄС проводиться активна законодавча робота з врегулювання ІІІ. Проєкт регламенту про ІІІ створює єдину юридичну базу

для ШІ в ЄС. Він, зокрема, встановлює класифікацію систем ШІ за рівнем ризику, формулює вимоги до використання ШІ, створює Раду ЄС з питань ШІ, визначає технологічно нейтральне визначення ШІ тощо. Проєкт Директиви ЄС щодо відповідальності за шкоду завдану ШІ встановлює правила щодо позадоговірної відповідальності. Такі проєкти регулювання, як Директива про безпеку машин та обладнання, Регламент про цифрові послуги, Регламент про цифрові ринки та Регламент про управління даними, також матимуть вплив на регулювання ШІ.

Попри відсутність спеціалізованого законодавства, Суд ЄС вже розглядає справи, які стосуються ШІ, особливо у сферах захисту авторських прав та персональних даних. Він визнає право на захист авторських прав для створених ШІ об'єктів і встановлює відповідальність операторів пошукових систем за обробку персональних даних. Рішення Суду ЄС створюють прецеденти, які можуть вплинути на майбутнє регулювання ШІ в ЄС.

Ключові слова: штучний інтелект, машинне навчання, Європейський Союз, цифрова стратегія ЄС, етичні стандарти штучного інтелекту, акт про штучний інтелект, політика ЄС, законодавство ЄС, Суд ЄС.

Summary. The article is devoted to the review of the policy of the European Union (EU) in the field of artificial intelligence (AI) technologies through the prism of program documents, current legislation, regulatory projects and the practice of the EU Court.

The problem of EU policy formation in the field of AI is urgent in view of the breakthrough development of AI technologies on the one hand. It requires the implementation of European legislation in the process of European integration of Ukraine.

The article examines the key program documents of the EU regarding AI, their influence on the regulation and development strategy of this area. The EU

aims to create a people-oriented strategy, promote investment, research and innovation, transform education and ensure access to AI technologies. EU policy documents set out key elements of AI trustworthiness, such as legality, ethics and trustworthiness, and emphasize the importance of values, human rights and transparency. These documents reflect a strategic view of AI and call for a continuous renewal policy, taking into account technological developments and the social environment, and reflect the main principles and priorities for future regulation of AI in the EU.

Currently, there is no specialized legislation in the EU that regulates AI. However, there are directives and regulations that indirectly affect the development and use of an AI system. For example, the General Data Protection Regulation (GDPR) sets restrictions on the processing of personal data. The Directive on Copyright in the Digital Single Market impacts the development of AI systems that work with copyrighted material. The Product Liability Directive establishes manufacturers' liability for defects. Cybersecurity rules also apply to AI. At the same time, legislative work on the regulation of AI is active. The proposal on AI Act creates a single legal framework for AI. In particular, it establishes a system of classification of AI according to the level of risk, requirements for the use of AI, creates the EU Council on AI, creates a technologically neutral definition of AI, etc. The draft Artificial Intelligence Liability Directive establishes rules on non-contractual liability. Projects such as the Machinery Directive, the Digital Services Act, the Digital Markets Act and the Data Governance Act also affect AI.

Despite the issuance of specialized legislation, the Court of Justice of the EU is already considering cases related to AI, especially in the areas of copyright and personal data protection. It recognizes the right to copyright protection for AI-generated materials and establishes the responsibility of search engine operators for the processing of personal data. The decisions of the Court of

Justice of the EU create precedents that may influence the further regulation of AI in the EU.

Key words: *artificial intelligence, machine learning, European Union, EU digital strategy, ethical standards of artificial intelligence, artificial intelligence act, EU policy, EU legislation, EU Court of Justice.*

Постановка проблеми. Штучний інтелект (далі – ШІ) вже відіграє дуже вагому роль у світі, в якому ми живемо, і його вплив продовжує зростати у різноманітних аспектах нашого життя, включаючи економіку, освіту, медицину, політику та навіть культуру. Європейський Союз (далі – ЄС) активно розробляє свій підхід до ШІ, спрямований на досягнення досконалості та благонадійності у цій сфері, підвищення дослідницької та промислової потужності, гарантуючи при цьому безпеку та права людини.

ЄС, як один з найбільших глобальних гравців, вже визнав важливість цього питання та активно працює над виробленням політики та проєктів регулювання у сфері ШІ. Це охоплює розробку програмних документів, стратегій, планів, етичних принципів та стандартів, а також законів та інших форм регулювання використання ШІ в різних сферах.

Для України, яка вже має статус кандидата на членство в ЄС, і перебуває в активній фазі євроінтеграції, важливо розуміти цю політику і бути готовою до її впровадження. Це особливо важливо, оскільки регулювання ШІ належать до сфери функціонування внутрішнього ринку ЄС, а отже є виключною компетенцією ЄС. І отже українське законодавство повинно відповідати стандартам ЄС. Крім того, Україна вже розробила власну амбітну Концепцію розвитку штучного інтелекту в Україні, реалізація якої також повинна відповідати політиці та регулюванню ЄС. Це не лише допоможе Україні інтегруватися в ЄС, але і сприятиме розвитку вітчизняної індустрії, створюючи нові можливості для економічного зростання та соціального прогресу.

Таким чином, актуальність цього дослідження полягає в необхідності адаптації українського законодавства до європейських стандартів у сфері штучного інтелекту, що є важливим кроком на шляху до інтеграції України в ЄС. У цьому контексті, стаття розглядає чотири основні блоки: по-перше, це аналіз програмних документів ЄС, по-друге, аналіз чинного законодавства ЄС, що в той чи інший спосіб регулює ІІІ, по-третє, аналіз проектів спеціалізованого законодавства ЄС щодо ІІІ та, по-четверте, аналіз вже наявної практики суду ЄС щодо ІІІ.

Аналіз останніх досліджень і публікацій. Проблемі формування політики та регулювання у сфері технології ІІІ на рівні ЄС, на перший погляд, присвячена помітна кількість досліджень та публікацій. Однак їх аналіз свідчить про те, що дослідження політики ЄС у сфері ІІІ, по-перше, зазвичай, не є комплексними. Наприклад, стосуються окремих її аспектів, як-от аналіз лише програмних документів (Р. Джусто-Ханані), дослідження безпекового виміру політики (І. Радіонова) або дослідження політики ЄС щодо ІІІ в контексті самого лише публічного управління (М. Янишівський, Т. Тарасенко та В. Тарасенко). З іншого боку, в деяких публікаціях досліджується політика ЄС щодо ІІІ в ширшому контексті, як складова інших проблем, наприклад, інформаційної політики (О. Пістракевич), чи як інструмент цифровізації зовнішньоекономічної політики (В. Камишанський) або ж розглядається в контексті застосування інноваційних підходів до методології правового регулювання (О. Красівський та М. Янишівський). Політика ЄС щодо ІІІ також є предметом дослідження у працях, де розглядаються національні стратегії щодо ІІІ окремих держав членів ЄС (О. Пістракевич) або в порівнянні зі стратегіями інших глобальних гравців (І. Ульнічане). Окрема група публікацій стосується виключно проблеми нормативного регулювання, зокрема теоретичних основ регулювання ІІІ в ЄС (К. Єфремова), експериментального регулювання та перспектив правового регулювання (С. Ранчордас), етичних

проблем в контексті нормативного регулювання ШІ (М Кокельберг), регулювання ШІ у сфері медицини (А. Д. Стерн) та аналізу проєктів регулювання, наприклад, проєкту регламенту, що встановлює гармонізовані правила щодо ШІ (М. Веале та Ф. З. Боргесіус, М. Янишівський). Натомість комплексного підходу до аналізу політики ЄС у сфері ШІ, який би враховував як програмні документи, так і нормативні, в тому числі й проєкти нормативного регулювання та практику суду ЄС, у вищенаведених працях немає. По-друге, політика, регулювання та судова практика щодо ШІ у ЄС перебуває лише на стадії становлення, зокрема, з огляду на швидкий розвиток технології, тому підходи та бачення швидко змінюються, а наукові публікації можуть впродовж короткого проміжку часу ставати неактуальними та застарілими.

Формулювання цілей статті. Метою дослідження є розгляд політики Європейського Союзу у сфері технології штучного інтелекту за допомогою аналізу ключових програмних документів, чинних нормативно-правових актів, проєктів регулювання та практики суду ЄС.

Виклад основного матеріалу. Програмні документи ЄС відіграють ключову роль у формуванні політики щодо ШІ. Ці документи не мають юридичної сили в традиційному розумінні, вони не встановлюють обов'язкових норм чи регуляцій. Замість цього, вони служать орієнтирами, вказуючи напрямки, в яких ЄС прагне рухатися в контексті ШІ. **Програмні документи** визначають основні засади та пріоритети, керівні принципи та рамки для майбутнього регулювання. Вони підкреслюють стратегічний погляд ЄС на ШІ та визначають шляхи для його впровадження та використання в соціально-економічному контексті.

*Комунікація Європейської Комісії "Штучний інтелект для Європи"*¹ опублікована у квітні 2018 року, є одним і перших ключових програмних

¹ Communication from the European Commission "Artificial Intelligence for Europe"

документів у сфері ШІ в ЄС. В Комунікації наголошується, зокрема, що технологія ШІ перестала бути науковою фантастикою і стала частиною повсякденного життя, що змінює світ, суспільства та цілі індустрії. Завдяки розвитку обчислювальних потужностей, доступності даних, розвитку алгоритмів, ШІ став однією з найбільш стратегічних технологій 21 століття, тому, щоб ЄС міг бути не лише конкурентоспроможним, а й стати світовим лідером у галузі ШІ, ЄС повинен мати скоординований план щодо ШІ. Європейська Комісія (далі – ЄК) наголошує на необхідності залучати інвестиції (понад 20 млрд євро щороку), підтримувати дослідження та інновації, підтримувати так звані “центри передового досвіду”² та стимулювати їхню співпрацю між собою. Разом з тим, як зазначається в Комунікації, розвиток ШІ та пов’язана з ним трансформація ринку праці не повинна залишити “за бортом” громадян ЄС, тому необхідні належна трансформація освіти та сприяння доступу до технології ШІ малих підприємств та потенційних користувачів. Згідно з цим програмним документом, ЄС має забезпечити розвиток ШІ, заснованого на цінностях, фундаментальних правах людини, етичних принципах підзвітності та прозорості та запропонувати рамки правового регулювання [1].

*Керівні принципи з етики для благонадійного ШІ*³ опубліковані у квітні 2019 року визначили 3 ключові елементи благонадійності ШІ: (1) правомірність (дотримання усіх законів та регулювань); (2) етичність (забезпечення етичних принципів та цінностей); (3) надійність (як технічну, так і соціальну, оскільки навіть з благими цілями системи ШІ можуть завдавати ненавмисної шкоди). Лише одночасна наявність всіх 3 елементів забезпечує благонадійність ШІ. Документ складається з 3 розділів і зосереджуються на етичності та надійності, практично не торкаючись правомірності, оскільки комплексного правового регулювання ШІ в ЄС ще

² Centres of excellence

³ Ethics guidelines for trustworthy AI

і досі не існує (станом на липень 2023 року). Перший розділ ідентифікує етичні принципи та відповідні цінності, що мають враховуватися при розробці та впровадженні ІІІ: повага до автономії людини, запобігання завданню шкоди, справедливість та зрозумілість. Також особлива увага звертається на ситуації, де залучені вразливі групи: діти, особи з інвалідністю, групи, що історично перебували у менш вигідному становищі, споживачі, працівники тощо. Документ пропонує вживати адекватні заходи для пом'якшення ризиків ІІІ щодо демократії, верховенства права, справедливого розподілу благ та "людського розуму".

Другий розділ описує 7 ключових вимог до розробки та впровадження ІІІ: (1) людське посередництво та нагляд; (2) технічна надійність та безпека; (3) конфіденційність та управління даними; (4) прозорість; (5) різноманіття, недискримінація та справедливість; (6) довкільний та суспільний добробут; 7) підзвітність [2, с. 2]. Третій розділ містить конкретний, але невичерпний список критеріїв оцінки надійного ІІІ, спрямований на реалізацію вимог, викладених у другому розділі, який потрібно адаптовувати до конкретного випадку використання системи ІІІ.

Важливим є те, що самі автори визначають документ як "відправну точку" в дискусії щодо благонадійного ІІІ та не мають на меті замінити будь-яку форму поточної чи майбутньої політики та регулювання, чи стримувати їх впровадження. Це "живий" документ, який потрібно переглядати та оновлювати з часом, щоб забезпечити постійну актуальність у міру розвитку технологій, суспільства та знань [2, с. 3].

Біла книга зі штучного інтелекту: європейський підхід до досконалості та довіри (далі – Біла книга)⁴ опублікована ЄК у лютому 2020 року, є комплексним документом, який описує підхід ЄС до ІІІ, зосереджуючись на сприянні "досконалості та довіри" до технології ІІІ.

⁴ White Paper on Artificial Intelligence: A European approach to excellence and trust

Передовсім Біла стверджує, що технологія ІІІ має надзвичайний потенціал вдосконалити різноманітні аспекти життя: охорону здоров'я, сільське господарство, пом'якшення наслідків зміни клімату, виробництва товарів тощо. З іншого боку, визнаючи ризики, які несе в собі технологія, ЄК наголошує на важливості "благонадійності"⁵ цифрових технологій та закликає опиратися на європейські цінності, використовувати регуляторний та інвестиційно-орієнтований підходи [3, с. 1], оскільки ЄС відстає в обсягах інвестицій від інших регіонів світу [3, с. 4] та поважати права громадян ЄС та під час розробки та впровадження ІІІ в ЄС [3, с. 2].

Відповідно основними блоками Білої книги є, по-перше, політичні рамки⁶ для узгодження зусиль публічної влади на європейському, національному та регіональному рівнях задля створення "екосистеми досконалості"⁷ [3, с. 3]. Щоб побудувати таку екосистему, що зможе ефективно підтримувати розвиток та впровадження ІІІ в економіці та публічному управлінні ЄС, Біла книга визначає ряд кроків на різних рівнях [3, с. 5], що включають роботу з державами-членами, зосередження зусиль дослідницької та інноваційної спільноти, залучення інвестицій [3, с. 6] По-друге, це ключові елементи майбутньої нормативно-правової бази для побудови "екосистеми довіри"⁸. Також документ окреслює сильні сторони ЄС у галузі ІІІ, такі як вже наявні дослідницькі центри, інноваційні стартапи, досягнення в робототехніці та такі конкурентоспроможні сектори виробництва та послуг, як автомобілебудування, охорона здоров'я, енергетика, фінанси, сільське господарство [3, с. 3].

Білу книгу супроводжує також *Звіт про наслідки штучного інтелекту, Інтернету речей і робототехніки для безпеки та відповідальності*, який оцінює вплив ІІІ, Інтернету речей і робототехніки

⁵ Trustworthiness

⁶ Policy framework

⁷ "Ecosystem of excellence"

⁸ "Ecosystem of trust"

на наявні сфери законодавства ЄС щодо безпеки продукції та відповідальності. Звіт акцентує на потребі полегшити тягар доказування, встановлений національними законами, для справ про компенсацію через дії ІІІ. Звіт також дійшов важливих висновків, що поточне законодавство про безпеку продукції містить ряд прогалин, які необхідно усунути, а масштаби та сукупний вплив викликів ІІІ можуть ускладнити надання компенсації жертвам у всіх випадках, коли це може бути виправдано [4].

Важливою є опублікована у 2021 ЄК *Комунікація «Сприяння європейському підходу до штучного інтелекту»*⁹, що містить в додатку *Переглянутий скоординований план щодо штучного інтелекту* (далі – Скоординований план) 2021 року¹⁰. Вперше опублікований у 2018 році Скоординований план є спільним зобов'язанням ЄК та держав-членів працювати разом, щоб максимізувати потенціал ЄС у сфері ІІІ для конкуренції на глобальному рівні. Перегляд Скоординованого плану у 2021 пропонує набір спільних дій для ЄК та держав-членів, щоб досягти глобального лідерства ЄС у сфері благонадійного ІІІ і пропонує 3 ключові дії: прискорити інвестиції; повно та своєчасно впроваджувати політику щодо ІІІ, а також узгоджувати її для розв'язання глобальних проблем.

Документ пропонує 4 ключові набори пропозицій для ЄС та держав-членів: (1) створення сприятливих умов для розробки та впровадження ІІІ в ЄС; (2) перетворення ЄС в середовище, де "досконалість" процвітає як у дослідницьких центрах, так і на ринку; (3) забезпечення того, щоб ІІІ "працював для людей і був силою добра в суспільстві"; (4) отримання ЄС стратегічного лідерства у ключових за впливом секторах. Документ також містить графіки ключових дій та аналіз національних стратегій та інвестицій у ІІІ. Важливо, що Скоординований план не стосується розробки та використання ІІІ у воєнних цілях [5].

⁹ Fostering a European approach to Artificial Intelligence

¹⁰ Coordinated Plan on Artificial Intelligence 2021 Review

Аналіз програмних документів ЄС вказує на стратегічний підхід до ІІІ, з акцентом на людино-орієнтованість, інвестиції, інновації, освіту та доступ до технології. Вони визначають ключові принципи благонадійності ІІІ, вимоги до його розробки та впровадження. ЄС визнає необхідність постійного оновлення цих документів та активізації зусиль у сфері інвестицій. Ці документи відіграють важливу роль у формуванні майбутнього регулювання ІІІ, що є також важливо для держав, які прагнуть до інтеграції з ЄС, включаючи Україну.

На сьогодні в ЄС не існує специфічного регулювання, яке було би прямо спрямоване на ІІІ. Однак, існує ряд **законодавчих актів** (регламенти та директиви), які непрямо регулюють цю сферу, встановлюючи важливі принципи та норми в таких областях, як захист даних, інтелектуальна власність, відповідальність за продукцію та кібербезпека. Ці документи формують правовий фундамент, на якому базується використання та регулювання ІІІ в ЄС.

*Загальний регламент про захист даних*¹¹ (далі – GDPR) та ІІІ тісно пов'язані, оскільки ІІІ часто використовується для обробки персональних даних. GDPR встановлює правила та обмеження щодо того, як можна використовувати та обробляти персональні дані. Ці принципи застосовуються до всіх систем ІІІ, які обробляють персональні дані в межах ЄС, незалежно від місцезнаходження такої системи. Важливо розуміти, що основна технологія, яка на сьогодні лежить в основі ІІІ – це машинне навчання, для якого велика кількість даних, зокрема і тих, що є персональними, є життєвонеобхідною.

Основні принципи щодо персональних даних встановлених GDPR наведені в статтях 4, 5, 7 та 8. Так, обробка даних повинна відбуватися законно, справедливо та прозоро, з дотриманням принципу мінімізації

¹¹ General Data Protection Regulation (GDPR)

даних. Дані, зібрані для конкретних цілей, не можуть оброблятися для інших цілей без додаткової згоди. Також важливою є гарантія точності персональних даних та негайного виправлення неточностей. GDPR встановлює обмеження зберігання, згідно з якими персональні дані повинні зберігатися не довше, ніж це необхідно, а також вимагає забезпечувати належну безпеку даних (захист від несанкціонованого або незаконного оброблення, а також від випадкової втрати, знищення або пошкодження). Також ШІ, який займається профілюванням, повинен дотримуватися положень GDPR щодо отримання явної згоди від осіб перед обробкою їх даних. Особливу увагу GDPR приділяє обробці даних дітей, для якої встановлені спеціальні умови [6].

GDPR, хоч і не згадує ШІ прямо, проте встановлює правила щодо "автоматизованої обробки даних", що часто є функцією програм оснащених ШІ. Згідно з GDPR, суб'єкти даних мають право відмовитися від рішень, які були прийняті на основі автоматизованої обробки даних, особливо якщо ці рішення розглядають їх "особисті характеристики" та мають значні наслідки. Наприклад, це може стосуватися ситуацій, коли на основі автоматизованої обробки даних приймаються рішення про надання кредиту або працевлаштування. Проте GDPR також визначає обставини, при яких автоматизована обробка даних є прийнятною: (1) коли це вимагається законодавством ЄС або держави-члена ЄС, наприклад, для виконання спеціальних завдань, таких як моніторинг, боротьба проти шахрайства та уникнення сплати податків; (2) коли автоматизована обробка даних необхідна для укладення або виконання договору; (3) коли суб'єкт даних надав свою явну згоду на таку обробку.

Проте навіть у випадках, коли автоматизована обробка допустима, необхідно дотримуватися певних гарантій: (1) надання повної інформації суб'єкту даних про процес обробки і його право на втручання людини; (2) можливість для суб'єкта даних висловити свою думку і обговорити рішення,

що було прийнято на основі автоматизованої обробки; (3) обов'язок забезпечити обґрунтування рішення, що було прийнято після автоматизованої обробки; (4) право суб'єкта даних на оскарження такого рішення. Всі ці гарантії мають на меті забезпечити, що автоматизована обробка даних використовується належно та з повагою до особистих прав і свобод суб'єктів даних [6; 7, с. 6-7].

*Директива про авторське право на єдиному цифровому ринку*¹² 2019 року безпосередньо не регулює ІІІ, але встановлює правила, які можуть впливати на те, як системи ІІІ розробляються та використовуються в контексті об'єктів, захищених авторським правом. Це, зокрема, стосується таких сфер як (1) інтелектуальний аналіз тексту та даних (TDM); (2) використання матеріалів, захищених авторським правом; (3) фільтрування вмісту.

Так, по-перше, директива передбачає обов'язковий виняток для аналізу тексту та даних, методу, який часто використовується в ІІІ для машинного навчання. Це дозволяє системам ІІІ аналізувати захищений авторським правом вміст для аналізу даних, не порушуючи закони про авторське право. По-друге, системам ІІІ самим часто доводиться використовувати великі обсяги даних і вивчати їх, деякі з яких можуть бути захищені авторським правом. Директива містить вказівки щодо використання матеріалів, захищених авторським правом, на платформах для обміну контентом в Інтернеті. Це опосередковано впливає на те, як навчаються та використовуються системи ІІІ, оскільки їм може знадобитися дотримуватися цих вказівок при використанні захищеного авторським правом вмісту для навчання та аналізу даних. А з іншого боку, саме системи ІІІ можна використовувати для моніторингу та фільтрації вмісту, щоб запобігти порушенням авторських прав [8].

¹² Directive on Copyright in the Digital Single Market

*Директива про відповідальність за продукцію*¹³ від 1985 року гармонізує закони держав-членів щодо відповідальності виробників за шкоду, спричинену дефектною продукцією. Згідно з директивою, виробники несуть відповідальність за шкоду, спричинену дефектами їхньої продукції. Поняття "дефект" полягає в тому, що продукт не забезпечує безпеки, на яку особа має право розраховувати (стаття 6). Термін "виробник" визначається широко і включає виробника готової продукції, виробника сировини або будь-яку особу, яка шляхом розміщення свого імені, товарного знака чи іншого відмітного елемента на продукті представляє себе його виробником (стаття 3) [9]. Але застосування директиви до ШІ викликає проблеми, оскільки вони з часом навчаються та адаптуються, що може розмити ідентифікацію "виробника" та точне визначення "дефекту", якщо проблема виникає після того, як система ШІ еволюціонувала після випуску. Так у вищезгаданому *Звіті про наслідки штучного інтелекту, Інтернету речей і робототехніки для безпеки та відповідальності* визнається, що чинне законодавство ЄС про безпеку продукції прямо не розглядає нові виклики та ризики цих нових технологій. Однак у ньому також зазначається, що це не означає, що воно не застосовуватиметься до продуктів, які містять ці технології [4].

*Директива про заходи для високого спільного рівня кібербезпеки в Союзі*¹⁴ або так звана Директива NIS2 також не згадує ШІ, але має наслідки для систем ШІ. Директива вимагає від організацій у певних секторах вживати заходів для підвищення рівня кібербезпеки. Наприклад, якщо система ШІ використовується для керування мережею або інформаційною системою, то ця система повинна бути захищена відповідно до вимог Директиви NIS2. Крім того, фокус директиви на таких сферах, як управління вразливістю та кібергігієна, також може стосуватися систем ШІ, оскільки ці

¹³ Product Liability Directive

¹⁴ Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

системи можуть мати вразливості, якими потрібно керувати, і вимагають належної кібергігієни [10; 11].

*Акт про кібербезпеку*¹⁵ встановлює рамки ЄС для сертифікації продуктів, послуг і процесів інформаційно-комунікаційних технологій (далі – ІКТ) з кібербезпеки. Акт може застосовуватися до систем ШІ, які використовуються як частина продуктів, послуг або процесів ІКТ, оскільки ці системи ШІ є частиною ландшафту ІКТ в ЄС [12; 13].

Станом на липень 2023 року ЄС не має спеціалізованого законодавства для регулювання ШІ. Однак, наявні директиви та регламенти, такі як GDPR, *Директива про авторське право на єдиному цифровому ринку*, *Директива про відповідальність за продукцію* та *акти про кібербезпеку* вже впливають на розробку та використання систем ШІ в ЄС в таких сферах як обробка персональних даних, захист авторських прав, відповідальність за продукцію та кібербезпека.

Натомість в ЄС наразі активно обговорюються на офіційному рівні **проєкти регулювання ШІ**, які мають на меті встановити чіткі правила та стандарти для ШІ. Основними серед них є *проєкт Регламенту, що встановлює гармонізовані правила щодо штучного інтелекту* та *проєкт Директиви щодо відповідальності за штучний інтелект*.

*Проєкт Регламенту, що встановлює гармонізовані правила щодо штучного інтелекту*¹⁶ (далі – Акт про ШІ) був розроблений з метою впровадження першої єдиної юридичної бази для регулювання ШІ в межах ЄС. Акт про ШІ пропонує поділ систем ШІ на групи відповідно до потенційного ризику, який вони можуть створювати для користувачів та суспільства: неприпустимий ризик, високий ризик, обмежений ризик та мінімальний ризик.

¹⁵ Cybersecurity act

¹⁶ Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)

Системи ШІ, що мають неприпустимий ризик, представляють безпосередню загрозу для безпеки, життя та прав людей і повинні бути заборонені. Це стосується систем, що використовуються для соціального оцінювання, а також систем, що в режимі реального часу здійснюють дистанційну біометричну ідентифікацію і використовуються для моніторингу у публічних місцях.

Системи ШІ, які використовуються у сферах критичної інфраструктури, освіти, зайнятості, ключових державних та приватних послуг, правоохоронних органах, міграційних службах та судових органах, визнаються, згідно з проєктом, системами з високим ризиком. Ці системи повинні відповідати строгим вимогам, перш ніж їх можна буде виводити на ринок. Вимоги включають оцінку ризику і способи його зниження, високу якість використовуваних даних, прозорість, людський контроль та безпеку.

Системи ШІ з обмеженим ризиком, такі як чатботи, підпадають під вимоги прозорості: користувачам має бути чітко зрозуміло, що вони спілкуються з машинною системою, а не з людиною. Більшість систем ШІ, які вважаються системами з мінімальним ризиком або без ризику, можуть використовуватися без юридичних обмежень.

Акт про ШІ також передбачає утворення спеціальної Ради ЄС з питань ШІ, до складу якої входитимуть представники всіх держав-членів, для допомоги в імплементації регулювань і запровадження штрафів за порушення. Штрафи для компаній, які не дотримуються цих вимог, можуть досягати 6% від їхнього глобального обороту або 30 мільйонів євро, в залежності від того, яка сума є вищою.

Зважаючи на дуже стрімкий розвиток технологій і ринку, проєкт регламенту вводить технологічно нейтральне визначення ШІ. Так, акт про ШІ визначає систему ШІ як "програмне забезпечення, розроблене за допомогою одного або декількох методів і підходів, що вказані в Додатку I (до проєкту регламенту), яке може генерувати результати (наприклад,

контент, прогнози, рекомендації або рішення) щодо певного набору цілей, визначених людиною, впливаючи на середовище, з яким воно взаємодіє" [14; 15, с. 175-176].

Наразі, проєкт регламенту обговорюється в комітетах Європейського Парламенту. Так, 11 травня 2023 року Комітет у справах внутрішнього ринку та Комітет у справах громадянських свобод схвалили проєкт переговорного мандату стосовно проєкту регламенту. Члени Європейського Парламенту запропонували:

1) Ввести заборони на агресивне і дискримінаційне використання систем ШІ, таких як системи дистанційної біометричної ідентифікації в режимі реального часу в громадських місцях, прогнозування для поліції, системи розпізнавання емоцій для правоохоронних цілей, неконтрольоване вилучення біометричних даних з соціальних мереж або відео з камер спостереження для створення баз даних для ідентифікації;

2) Розширити класифікацію систем ШІ з високим ризиком, включаючи вплив на здоров'я людей, безпеку, основні права або довкілля, вплив на виборців у політичних кампаніях і системи рекомендацій, які використовуються великими соціальними платформами;

3) Встановити обов'язки для постачальників великих генеративних моделей, таких як ChatGPT, щодо додаткових вимог прозорості, таких як надання інформації про те, що контент був створений штучним інтелектом, запобігання створенню незаконного контенту і публікації об'єктів, захищених авторським правом, що використовуються для навчання;

4) Запропонувати конкретні кроки для розвитку інновацій в галузі ШІ, такі як винятки для наукових досліджень і компонентів ШІ, що надаються з відкритими ліцензіями, створення спеціальних контрольованих середовищ для тестування ШІ під контролем державних органів, а також розширення прав громадян на подачу скарг на системи ШІ, отримання пояснень рішень,

які суттєво впливають на їх права і засновані на системах високого ризику [16; 15, с. 176].

Також у вересні 2022 року ЄК запропонувала *проект Директиви щодо відповідальності завданої штучним інтелектом*¹⁷, маючи на меті покращити функціонування внутрішнього ринку шляхом встановлення єдиних правил щодо певних аспектів позадоговірної цивільної відповідальності за заподіяну шкоду із залученням систем ШІ. Директива пропонує гармонізувати правила для подання позовів в тих питаннях, які не покриваються іншими директивами про відповідальність. Це, наприклад, порушення конфіденційності або збитки, спричинені проблемами безпеки захисту персональних даних. Найбільш суттєвою зміною стане спрощена процедура отримання компенсації за збитки, завдані діяльністю ШІ, таких як дискримінація при наймі на роботу. Очікується, що Директива значно полегшить діяльність бізнесу, який зможе впроваджувати заходи безпеки та регулювання ШІ, щоб запобігати притягнення їх до відповідальності [17, с. 2].

Крім цих двох ключових документів, є також ряд додаткових ініціатив, які впливають на ШІ, зокрема у сферах безпеки машин та обладнання, цифрових послуг, цифрових ринків та щодо управління даними.

*Директива щодо безпеки машин та обладнання*¹⁸ – це директива ЄС, що забезпечує єдиний рівень безпеки для машин, що продаються в ЄС. Наразі ця директива проходить процес перегляду, відомий як REFIT¹⁹, щоб адаптувати законодавство до швидкого розвитку технологій, зокрема ШІ. У відповідь на інтеграцію технологій ШІ у різні типи машин предмет регулювання Директиви буде розширений на ШІ та робототехніку. Також

¹⁷ Artificial Intelligence Liability Directive

¹⁸ Machinery Directive

¹⁹ Regulatory Fitness and Performance programme

передбачаються зміни, що мають на меті усунення нових ризиків пов'язаних з ШІ, який забезпечує автономну роботу обладнання, адже це може ускладнити прогнозування та контроль дій обладнання [18].

Також вплив на регулювання ШІ будуть мати *проект Регламенту про цифрові послуги*²⁰ спрямований на створення безпечнішого цифрового простору, де захищені фундаментальні права користувачів цифрових послуг, *проект Регламенту про цифрові ринки*²¹, що націлений запобігти зловживанням великих онлайн-платформ зі значним мережевим впливом [19] та *проект Регламенту про управління даними*²², що повною мірою буде застосовуватися з вересня 2023 року і має на меті сприяти доступності даних для використання завдяки підвищенню довіри до посередників даних і посилення механізмів обміну даними в ЄС [20].

Вищенаведені ініціативи показують, що ЄС активно працює над встановленням чіткого регулювання ШІ, що враховує різні аспекти його використання та впливу на суспільство, зокрема, визначення ризиків та класифікацію технологій залежно від ступеня ризику з встановленням різних вимог до функціонування таких систем, створення спеціальних органів, регулювання питання відповідальності за шкоду завдану ШІ, використання ШІ під час надання цифрових послуг, та на єдиному цифровому ринку, в контексті управління даними тощо.

Досліджуючи політику ЄС в будь-якому питанні, не варто забувати, що в ЄС існує й судова гілка влади, функції якої виконує **Суд Європейського Союзу** (далі — Суд ЄС), що займається інтерпретацією законодавства ЄС у випадках, коли національні суди країн-членів ЄС мають сумніви щодо того, як в конкретних справах застосувати норми, прописані в директивах та регламентах ЄС. Всупереч факту, що наразі в ЄС відсутнє

²⁰ Digital Services Act

²¹ Digital markets act

²² European Data Governance Act

спеціалізоване законодавство щодо ШІ, Суд ЄС протягом багатьох років роботи, особливо в останні роки, виносив рішення у справах, які стосувалися ШІ та потребували відповідного тлумачення актів ЄС. Найчастіше ці питання виникали у справах, що стосувалися захисту права інтелектуальної власності та захисту персональних даних.

В контексті захисту інтелектуальної власності ці рішення безпосередньо не стосуються творів, створених ШІ, але демонструють основний підхід Суду ЄС до оцінки захищеності творів і можуть використовуватися як настанова для оцінки творів, створених ШІ у майбутніх рішеннях. Однією із таких справ є справа C-5/08 (*Infopaq International A/S v Danske Dagblades Forening*) 2009 року. У цій справі Суд ЄС постановив, що уривки тексту можуть бути захищені авторським правом, якщо вони є "власним інтелектуальним твором" автора. Це рішення актуальне в контексті творів, створених ШІ, оскільки воно показує, що навіть менші уривки тексту або компоненти творів, створених ШІ, можуть мати право на захист авторських прав, якщо вони становлять власну інтелектуальну творчість автора [21]. Незадовго після цієї справи, у 2011 році, Суд ЄС у справі C-145/10 (*Eva-Maria Painer v Standard Verlags GmbH*) конкретизував, що твір можна вважати особистим інтелектуальним твором, якщо він відображає "свободу творчості" автора і, таким чином, є "власним інтелектуальним твором" [22]. Також важливим є відносно недавнє рішення у справі C-516/17 (*Spiegel Online GmbH v. Volker Beck*), видане 29 липня 2019. В цьому рішенні Суд ЄС постановив, що використання захищених авторським правом творів системами ШІ в контексті аналізу тексту та даних може вважатися дозволеним використанням [23].

З цих рішень можна зробити висновок, що Суд ЄС поки що доволі відкрито ставиться до використання ШІ для генерування нових творів. Однак, варто пам'ятати, що всі ці рішення були винесені до недавнього

прориву у сфері машинного навчання²³, зокрема до створення Chat GPT, що значно розширило розуміння того, як ШІ може використовуватися для креативної діяльності.

Іншою сферою, де ШІ не залишився без уваги Суду ЄС, є захист персональних даних. Ще у 2014 році широкого розголосу набула справа C-131/12 (*Google Spain v AEPD and Mario Costeja González*). У рішенні в цій справі Суд визнав, що оператори пошукових систем несуть відповідальність за обробку персональних даних і що суб'єкти даних мають "право бути забутими"²⁴). Це також має наслідки для пошукових систем на базі ШІ та їхніх зобов'язань щодо захисту даних, оскільки алгоритми пошукових систем повинні бути достатньо "розумними", щоб розпізнавати всю інформацію, яку необхідно видалити [24].

Е 2018 році Суд ЄС виніс рішення у справі C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*). Суд ЄС встановив, що адміністратор фан-сторінки у Facebook несе солідарну з платформою відповідальність за обробку даних відвідувачів сторінки. Це рішення можна використати, щоб навести вагомий аргумент, що цільова реклама передбачає спільний контроль рекламодавців із платформами чи іншими постачальниками рекламних технологій, які допомагають їм націлювати свої оголошення на користувачів. Відповідно до логіки Суду ЄС, якщо рекламодавець використовує будь-який сервіс, який збирає дані про користувачів, щоб націлити на них рекламу, рекламодавець робить внесок в обробку персональних даних, оскільки використовує інструмент, для якого дані були зібрані [25].

Однією з останніх справ, де питання захисту персональних даних перетинається зі ШІ, є справа C-817/19 (*Ligue des droits humains v Conseil des ministres*). Справа стосувалася Директиви ЄС від 27 квітня 2016 про

²³ Machine learning

²⁴ Right to be forgotten

використання даних запису реєстрації пасажирів для запобігання, виявлення, розслідування та переслідування терористичних та тяжких злочинів. Відповідно до цієї директиви, працівники поліції та судових органів мають право доступу до даних пасажирів, які прилітають у країни ЄС чи відлітають з них. У деяких випадках це також дозволяє збирати дані про пасажирів на рейсах в межах ЄС. Окрім того, що Суд ЄС постановив встановити певні обмеження, щоб збір даних не порушував законодавство ЄС, він також заборонив використання системи машинного навчання²⁵ ШІ для збору та обробки даних про пасажирів авіакомпаній [26]. Важливість цього рішення важко переоцінити, адже вперше орган ЄС виніс рішення, яке настільки напругу стосувалося б долі ШІ у ЄС. Заборона використання систем машинного навчання створює прецедент, який може бути використаний у майбутніх справах щодо ШІ.

Як видно з рішень Суду ЄС, питання ШІ ще не поставало перед Судом повною мірою. В останні кілька десятиліть питання ШІ виникало у справах Суду, що стосуються захисту права інтелектуальної власності та захисту персональних даних. Тільки за декілька останніх років з'явилися справи, які напругу вплинули на регулювання ШІ. Ці рішення показують, що регулювання ШІ в ЄС буде тільки посилюватися та отримувати нові обмеження. Особливо важливо слідкувати за майбутніми рішеннями Суду ЄС стосовно систем машинного навчання, оскільки в разі розширення обмежень на їх використання в ЄС можуть виникнути серйозні проблеми із впровадженням цієї революційної технології.

Висновки і перспективи подальших досліджень. Ми розглянули такі ключові програмні документи ЄС щодо ШІ: Комунікація ЄК "Штучний інтелект для Європи", Керівні принципи з етики для благонадійного ШІ, Біла книга зі штучного інтелекту: європейський підхід до досконалості та

²⁵ Machine learning systems

довіри, Звіт про наслідки штучного інтелекту, Інтернету речей і робототехніки для безпеки та відповідальності», Звіт про наслідки штучного інтелекту, Інтернету речей і робототехніки для безпеки та відповідальності, Комунікація «Сприяння європейському підходу до штучного інтелекту»

Аналіз цих програмних документів демонструє визначену стратегію ЄС щодо сфери ШІ. ЄС визначає свою стратегію як людино-орієнтовану, з акцентом на залучення інвестицій, підтримці досліджень та інновацій, трансформації освіти та сприяння доступу до технології ШІ бізнесу та громадян. Програмні документи ЄС, хоча і не мають юридичної сили в традиційному розумінні, встановлюють основні засади та пріоритети, керівні принципи та рамки для майбутнього регулювання. Вони підкреслюють важливість цінностей, прав людини, етичних принципів підзвітності та прозорості та визначають ключові елементи благонадійності ШІ, включаючи правомірність, етичність та надійність.

ЄС, однак, відстає в обсягах інвестицій від інших регіонів світу, що підкреслює необхідність активізації зусиль у цій сфері. Програмні документи ЄС визначають ключові елементи майбутньої нормативно-правової бази для побудови "екосистеми довіри" та "екосистеми досконалості", а також визнають необхідність усунення прогалин в поточному законодавстві.

Програмні документи ЄС відображають стратегічний погляд на ШІ, визначаючи шляхи для його впровадження та використання в соціально-економічному контексті. Вони підкреслюють важливість постійного перегляду та оновлення політики, щоб забезпечити її актуальність у міру розвитку технологій, соціального середовища та наших знань. Це підкреслює важливість активного слідкування за цими документами та адаптації до їх вимог для країн, які прагнуть до інтеграції з ЄС, включаючи Україну.

Сьогодні в ЄС не існує спеціалізованого законодавства, яке б безпосередньо регулювало сферу ШІ. Втім, є ряд директив та регламентів, які непрямо впливають на розробку та використання систем ШІ:

(1) *Загальний регламент про захист даних (GDPR)* встановлює строгі правила та обмеження для обробки персональних даних, які безпосередньо впливають на системи ШІ, що використовують ці дані.

(2) *Директива про авторське право на єдиному цифровому ринку* встановлює правила, які впливають на розробку та використання систем ШІ в контексті об'єктів, захищених авторським правом.

(3) *Директива про відповідальність за продукцію* встановлює відповідальність виробників за шкоду, спричинену дефектами в продуктах, зокрема, систем ШІ.

(4) *Директива про заходи для високого спільного рівня кібербезпеки в ЄС та Акт про кібербезпеку* встановлюють вимоги до кібербезпеки, які мають значний вплив на розробку та використання систем ШІ.

З іншого боку, в ЄС ведеться активна законотворча робота щодо нормативного врегулювання ШІ. Йдеться, зокрема, про *проект Регламенту ЄС, що встановлює гармонізовані правила щодо штучного інтелекту та проект Директиви щодо відповідальності завданої штучним інтелектом*.

Проект Регламенту ЄС встановлює гармонізовані правила щодо штучного інтелекту, має на меті створити єдину юридичну базу для регулювання ШІ в ЄС. Він пропонує класифікацію систем ШІ за рівнем ризику, встановлює вимоги до їх використання, передбачає створення Ради ЄС з питань ШІ для контролю за дотриманням регуляторів і вводить технологічно нейтральне визначення ШІ. Останні пропозиції щодо зміни проекту регламенту включають заборону агресивного та дискримінаційного використання систем ШІ, розширення класифікації систем ШІ з високим ризиком, встановлення обов'язків для постачальників великих генеративних моделей, та розробку конкретних кроків для розвитку інновацій в галузі ШІ.

Проект Директиви ЄС щодо відповідальності за штучний інтелект має на меті встановити єдині правила для позадоговірної цивільної відповідальності за шкоду, спричинену системами ШІ, спрощуючи процедуру отримання компенсації та допомагаючи компаніям впроваджувати відповідні заходи безпеки та регулювання.

Важливими також є законодавчі пропозиції, які мають опосередкований вплив на розробку та використання ШІ. Це, зокрема, пропозиції змін до Директиви щодо безпеки машин та обладнання, проєкт Регламенту про цифрові послуги, проєкт Регламенту про цифрові ринки та проєкт Регламенту про управління даними.

Аналізуючи політику ЄС щодо ШІ, важливо також враховувати роль Суду ЄС, який інтерпретує законодавство ЄС і вирішує спори, пов'язані з ШІ. Попри відсутність спеціалізованого законодавства, що регулює ШІ, Суд ЄС вже розглядав декілька справ, пов'язаних зі ШІ в контексті захисту права інтелектуальної власності та захисту персональних даних.

Суд ЄС визнав, що навіть невеликі уривки тексту або компоненти творів, створених ШІ, можуть мати право на захист авторських прав, якщо вони відображають власну інтелектуальну творчість автора, що дає юридичну впевненість для розробників ШІ, але вимагає обережності у використанні захищених авторським правом матеріалів. У контексті захисту персональних даних, Суд ЄС постановив, що оператори пошукових систем, що використовують ШІ, несуть відповідальність за обробку персональних даних і що суб'єкти даних мають "право бути забутими". Також рішенням Суду ЄС було заборонено використання систем ШІ для збору та обробки даних про пасажирів авіакомпаній. Це рішення створює прецедент, який може вплинути на майбутнє регулювання ШІ в ЄС.

Література

1. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe. COM/2018/237 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (дата звернення: 18.07.2023)
2. Shaping Europe's digital future. "Ethics Guidelines for Trustworthy AI," April 8, 2019. URL: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (дата звернення: 18.07.2023)
3. European Commission. "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust". COM(2020) 65 final. URL: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (дата звернення: 18.07.2023)
4. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. COM/2020/64 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064> (дата звернення: 18.07.2023)
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence. COM/2021/205 final. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2021%3A205%3AFIN> (ДАТА звернення: 18.07.2023)
6. Commission, European Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

- persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). European Commission (2016). URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679> (дата звернення: 18.07.2023)
7. Янишівський М. М., Красівський О.Я. Обчислювальне право: сумісність із правами людини та законодавче регулювання. *Науковий вісник. "ДЕМОКРАТИЧНЕ ВРЯДУВАННЯ"*. Львів, 2021. Вип. 1(27). URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2022/jan/26350/239197-tekststatti-551113-1-10-20210915.pdf> (дата звернення: 18.07.2023)
 8. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance). URL: <http://data.europa.eu/eli/dir/2019/790/oj> (дата звернення: 18.07.2023)
 9. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. URL: <http://data.europa.eu/eli/dir/1985/374/oj> (дата звернення: 18.07.2023)
 10. The NIS 2 Directive. *Веб-сайт Cyber Risk GmbH*. URL: <https://www.nis-2-directive.com/> (дата звернення: 18.07.2023)
 11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: <http://data.europa.eu/eli/dir/2022/2555/oj> (дата звернення: 18.07.2023)

12. The EU Cybersecurity Act. Веб-сайт Європейської комісії. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act> (дата звернення: 18.07.2023)
13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: <http://data.europa.eu/eli/reg/2019/881/oj> (дата звернення: 18.07.2023)
14. Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206> (дата звернення: 18.07.2023)
15. Янишівський М. М. Регулювання використання технології штучного інтелекту в Європейському Союзі: проєкт акту про штучний інтелект. doi: <https://doi.org/10.36059/978-966-397-315-9-43> (дата звернення: 18.07.2023)
16. AI Act: a step closer to the first rules on Artificial Intelligence. *Веб-сайт Європейського Парламенту.* URL: <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> (дата звернення: 18.07.2023)
17. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). URL: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf (дата звернення: 18.07.2023)

18. Internal Market, Industry, Entrepreneurship and SMEs - Machinery. Веб-сайт Європейської комісії. URL: https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/machinery_en (дата звернення: 18.07.2023)
19. The Digital Markets Act: ensuring fair and open digital markets. Веб-сайт Європейської комісії. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (дата звернення: 18.07.2023)
20. European Data Governance Act. Веб-сайт Європейської комісії. URL: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act> (дата звернення: 18.07.2023)
21. Judgment of the Court (Fourth Chamber) of 16 July 2009. Infopaq International A/S v Danske Dagblades Forening. Case C-5/08. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=72482&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=439753> (дата звернення: 18.07.2023)
22. Judgment of the Court (Third Chamber) of 1 December 2011. Eva-Maria Painer v Standard VerlagsGmbH and Others. Case C-145/10. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0145> (дата звернення: 18.07.2023)
23. Judgment of the Court (Grand Chamber) of 29 July 2019. Spiegel Online GmbH v Volker Beck. Case C-516/17. URL: <https://curia.europa.eu/juris/document/document.jsf%3Bjsessionid=DBDA-AA3440CF75684D01BB6D8C849913?text=&docid=216543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=437457> (дата звернення: 18.07.2023)
24. Judgment of the Court (Grand Chamber) of 13 May 2014. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario

Costeja González. Case C-131/12. URL:

[https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065
&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=44
0207](https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=440207) (дата звернення: 18.07.2023)

25. Judgment of the Court (Grand Chamber) of 5 June 2018. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case C-210/16. URL:
[https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543
&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=43
8990](https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=438990) (дата звернення: 18.07.2023)

26. Judgment of the Court (Grand Chamber) of 21 June 2022. Ligue des droits humains v Conseil des ministres. C-817/19. URL:
[https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282
&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=44
0636](https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=440636) (дата звернення: 18.07.2023)

References

1. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe. COM/2018/237 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (Accessed: 18.07.2023)
2. Shaping Europe's digital future. "Ethics Guidelines for Trustworthy AI," April 8, 2019. URL: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (Accessed: 18.07.2023)
3. European Commission. "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust,". COM(2020) 65 final. URL: <https://commission.europa.eu/publications/white-paper-artificial->

intelligence-european-approach-excellence-and-trust_en (Accessed: 18.07.2023)

4. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. COM/2020/64 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064> (Accessed: 18.07.2023)
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence. COM/2021/205 final. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2021%3A205%3AFIN> (Accessed: 18.07.2023)
6. Commission, European Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). European Commission (2016). URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679> (Accessed: 18.07.2023)
7. Yanyshivskyi M. M., Krasivskyi O.Ia. Obchysliuvalne pravo: sumisnist iz pravamy liudyny ta zakonodavche rehuliuвання. Naukovyi visnyk. "DEMOKRATYCHNE VRIADUVANNIA". Lviv, 2021. Vyp. 1(27) URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2022/jan/26350/239197-tekststatti-551113-1-10-20210915.pdf> (Accessed: 18.07.2023)
8. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA

- relevance.). URL: <http://data.europa.eu/eli/dir/2019/790/oj> (Accessed: 18.07.2023)
9. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. URL: <http://data.europa.eu/eli/dir/1985/374/oj> (Accessed: 18.07.2023)
 10. The NIS 2 Directive. *Cyber Risk GmbH website*. URL: <https://www.nis-2-directive.com/> (Accessed: 18.07.2023)
 11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: <http://data.europa.eu/eli/dir/2022/2555/oj> (Accessed: 18.07.2023)
 12. The EU Cybersecurity Act. *European Commission website*. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act> (Accessed: 18.07.2023)
 13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: <http://data.europa.eu/eli/reg/2019/881/oj> (Accessed: 18.07.2023)
 14. Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206> (Accessed: 18.07.2023)

15. Yanyshivskiy M. M. Rehuliuвання vykorystannia tekhnolohii shtuchnoho intelektu v Yevropeiskomu Soiuzi: Proiekt aktu pro shtuchnyi intelekt. doi: <https://doi.org/10.36059/978-966-397-315-9-43> (Accessed: 18.07.2023)
16. AI Act: a step closer to the first rules on Artificial Intelligence. *European Parliament website*. URL: <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> (Accessed: 18.07.2023)
17. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). URL: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf (Accessed: 18.07.2023)
18. Internal Market, Industry, Entrepreneurship and SMEs - Machinery. *European Commission website*. URL: https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/machinery_en (Accessed: 18.07.2023)
19. The Digital Markets Act: ensuring fair and open digital markets. *European Commission website*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (Accessed: 18.07.2023)
20. European Data Governance Act. *European Commission website*. URL: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act> (Accessed: 18.07.2023)
21. Judgment of the Court (Fourth Chamber) of 16 July 2009. Infopaq International A/S v Danske Dagblades Forening. Case C-5/08. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=72482&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=439753> (Accessed: 18.07.2023)
22. Judgment of the Court (Third Chamber) of 1 December 2011. Eva-Maria Painer v Standard VerlagsGmbH and Others. Case C-145/10. URL:

<https://eur-lex.europa.eu/legal->

[content/EN/TXT/?uri=CELEX%3A62010CJ0145](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0145) (Accessed: 18.07.2023)

23. Judgment of the Court (Grand Chamber) of 29 July 2019. Spiegel Online GmbH v Volker Beck. Case C-516/17. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=216543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=437457> (Accessed: 18.07.2023)
24. Judgment of the Court (Grand Chamber) of 13 May 2014. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Case C-131/12. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=440207> (Accessed: 18.07.2023)
25. Judgment of the Court (Grand Chamber) of 5 June 2018. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case C-210/16. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=438990> (Accessed: 18.07.2023)
26. Judgment of the Court (Grand Chamber) of 21 June 2022. Ligue des droits humains v Conseil des ministres. C-817/19. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=440636> (Accessed: 18.07.2023)